Multi-channel ranging system for the localization of wireless connected objects in low power wide aea networks : From modeling to field trials

Florian Wolf

Doctoral Thesis

Université de Limoges

University of Limoges

Doctoral School n°610 of Sciences and Engineering on Systems, Mathematics and Informatics (SISMI)

French National Centre for Scientific Research (CNRS), XLIM, Joint Research Unit (UMR) 7252

Thesis in fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY OF THE UNIVERSITY OF LIMOGES

Specialty: **Information Technology Sciences and Engineering**
Electronics on Radio Frequencies, Photonics and Systems

Presented by

Florian WOLF

Multi-Channel Ranging System for the Localization of Wireless Connected Objects in Low Power Wide Area Networks: from Modeling to Field Trials

Thesis directed by **Jean-Pierre Cances** and supervised by **Sébastien de Rivaz** and **François Dehmas**

In cooperation with **CEA-Leti**

Thesis presented on June 11th, 2020, in presence of the following jury:

Prof. Bernard TOURANCHEAU	Professor at the University Grenoble Alpes	Chairman
Prof. Gerard J. M. JANSSEN	Professor at Delft University of Technology	Reviewer
Prof. Maarten WEYN	Professor at the University of Antwerp	Reviewer
Prof. Elena-Simona LOHAN	Professor at Tampere University	Examiner
Prof. Laurent CLAVIER	Professor at the University of Lille	Examiner
Prof. Jean-Pierre CANCES	Professor at the University of Limoges	Thesis Director
Dr. Sébastien DE RIVAZ	Research engineer, PhD at CEA-Leti	Thesis Supervisor
Mr. François DEHMAS	Research engineer at CEA-Leti	Thesis Supervisor
Mr. Olivier SELLER	Research engineer at Semtech	Invitee

Thèse de Doctorat

Université de Limoges

Université de Limoges

École Doctorale n°610 des Sciences et Ingénierie des Systèmes, Mathématiques, Informatique (SISMI)

Centre National de la Recherche Scientifique (CNRS), XLIM, Unité Mixte de Recherche (UMR) 7252

Thèse pour obtenir le grade de

DOCTEUR DE L'UNIVERSITÉ DE LIMOGES

Spécialité : **Sciences et Ingénierie pour l'Information**
Électronique des Hautes Fréquences, Photonique et Systèmes

Présentée par

Florian WOLF

Système de Mesure Multicanaux de Distances pour la Localisation des Objets Connectés dans les Réseaux Longue Portée et Basse Consommation: de la Modélisation jusqu'aux Tests Terrain

Thèse dirigée par **Jean-Pierre Cances** et codirigée par **Sébastien de Rivaz** et **François Dehmas**

En coopération avec le **CEA-Leti**

Thèse soutenue le 11 juin 2020, en présence du jury composé de :

Pr. Bernard TOURANCHEAU	Professeur à l'Université Grenoble Alpes	Président
Pr. Gerard J. M. JANSSEN	Professeur à l'Université de Delft	Rapporteur
Pr. Maarten WEYN	Professeur à l'Université d'Anvers	Rapporteur
Pr. Elena-Simona LOHAN	Professeure à l'Université de Tampere	Examinatrice
Pr. Laurent CLAVIER	Professeur à l'Université de Lille	Examinateur
Pr. Jean-Pierre CANCES	Professeur à l'Université de Limoges	Directeur de Thèse
Dr. Sébastien DE RIVAZ	Docteur-ingénieur de recherche au CEA-Leti	Encadrant
M. François DEHMAS	Ingénieur-chercheur au CEA-Leti	Encadrant
M. Olivier SELLER	Ingénieur de recherche à Semtech	Invité

Acknowledgments

With this first page, I wish to thank all those who I was learning from and working with over more than three years, as well as I like to acknowledge all those who contributed to the success of this thesis.

Firstly, I thank the members of the jury for having accepted to judge on this work and for the scientific and technical discussions during the defense. In particular, I like to thank Professor Tourancheau for chairing the oral presentation and his future-oriented vision on the topic, Professor Janssen and Professor Weyn for having reviewed in detail this thesis, Professor Lohan and Professor Clavier for their examination and Mister Seller for his industrial view on the contributions.

Je souhaite remercier Monsieur Clermidy et Monsieur Ktenas, chefs du Service Technologies Sans Fils (STSF) du Département Intégration Systèmes (DSYS) au CEA-Leti, de m'avoir donné cette opportunité de travailler sur ce sujet très intéressant, innovant et dans l'air du temps, ainsi que pour leur support pour participer aux conférences. Je remercie également Monsieur Berg, chef du Laboratoire Communication des Objets Intelligents (LCOI), pour son intérêt dans ce travail, son regard très critique et constructif, ainsi que sa communication efficace et directe. En plus, je souhaite remercier toutes les équipes du STSF et au-delà, pour les échanges techniques variés. En particulier : Jean-Baptiste, Xavier, Jérémy, David I, Patrick, Bernard, Jean-Michel, David II, Marc, Manuel, Nicolas, Lionel, Julien et Serge pour leurs supports, leurs conseils et leurs appuis dans la phase d'implémentation et d'expérimentation. Sans eux, la réalisation d'un démonstrateur matériel aurait été impossible ! Merci à Yoann pour ce modèle de manuscrit de thèse. Merci à Sylvie et Valérian pour leurs efforts et leur engagement d'intégrer mes résultats dans des projets internationaux et de donner par conséquence une suite à ces travaux de thèse. Un merci spécial à Patricia et Sandrine pour leur assistance administrative, l'organisation des diverses missions liées à ce travail, ainsi que pour la préparation logistique de la soutenance de thèse. Un grand merci à mes collègues de bureau, Benoît et Christophe. C'était un plaisir de les côtoyer pendant plus de trois ans. Le mélange des sphères académiques et industrielles qu'ils incarnent crée une atmosphère professionnelle très enrichissante pour un jeune doctorant. Je souhaite également remercier Mohamed pour son esprit de coopération, sa motivation et ses idées, ce que nous a amené à une étude et publication commune. Merci également à Kévin pour son investissement dans la réalisation d'une étude comparative et la prise en main du démonstrateur matériel.

Enfin, je remercie le Professeur Cances de l'université de Limoges et du XLIM qui a dirigé cette thèse. Merci pour sa guidance et son suivi à distance, ses conseils précieux pour la rédaction des publications scientifiques et du manuscrit de thèse. Merci également pour les différentes occasions qui m'ont permis de venir à Limoges pour pouvoir apprendre le VHDL au sein des équipes du XLIM et de participer aux séminaires scientifiques.

Finalement, un très, très grand merci à Sébastien et François pour leur encadrement au cours de cette thèse. Merci pour leur guidance et leur disponibilité quotidienne. Merci à Sébastien pour sa créativité et son esprit visionnaire, essayant toujours de sortir de la manière habituelle de penser qui m'a appris une approche essentielle à l'innovation. Merci à François pour sa rigueur et son soin pour les détails, qui m'a beaucoup aidé à résoudre les problèmes techniques de façon systématique. Merci à eux pour leur grande confiance dans toutes mes idées, mes décisions et mes actions techniques et non-techniques. Cette autonomie et cette liberté m'ont toujours motivé à vouloir prendre en main les choses et mener à bien ce projet de thèse.

Thank you for the support! *Merci pour le soutien!* *Vielen Dank für die Unterstützung!*

Abstract

The Internet of Things (IoT) is an enabler to new applications, such as smart metering and environmental monitoring, intended to address current and future societal and ecological challenges. Things, possibly mobile or in distant locations, require wireless connectivity for data collection and remote control. Low Power Wide Area (LPWA) networks provide city-scale long-range, narrowband radio transmissions respecting the energy constraints of battery-powered low-cost objects.

Being capable to localize these objects will add value to their data, enables tracking applications and is therefore a demanded and recent research topic. Precise and accurate radio signal delay based positioning without integrating additional hardware but taking advantage of intrinsic wireless communication signals is appealing in terms of device complexity, cost and energy consumption. However, radio localization within LPWA networks is challenging due to narrowband transmissions, resulting in a lack of delay precision as well as due to radio propagation channels, which degrade the accuracy of location estimates.

This work addresses both challenges by investigating a multi-channel ranging system for LPWA networks. Coherently combining multiple sequentially transmitted narrowband signals on different radio channels improves delay estimation precision and allows resolving multipath channels for refined positioning accuracy. This scheme, based on instantaneous narrowband signals, conserves the LPWA long-range feature and is hence compatible with LPWA networks. A detailed signal model considering hardware imperfections as well as the required protocol exchanges for time, frequency and phase synchronization is developed. Based on this model, the requirements on radio transceiver architectures regarding the necessary phase coherence for multi-channel ranging are discussed. Lower bounds on the ranging precision are derived for both, free-space and multipath propagation channels, illustrating the improved precision compared to narrowband single channel ranging. Numerical simulations of radio signals for the two-way multi-channel ranging protocol illustrate that the performance of developed range estimators attains the theoretical precision bound and pave the way towards implementation. A flexible Software Defined Radio (SDR) based demonstrator is implemented to validate simulation results. Field trials in real urban outdoor environments are in accordance with simulation results and prove how scalable multi-channel ranging, in combination with advanced signal processing methods, will be an enabler towards precise and accurate localization in LPWA networks.

Keywords: Internet of Things (IoT); Low Power Wide Area (LPWA); Radio localization; Ranging; Frequency hopping; Phase of Arrival (PoA); Coherent processing; Narrow-Band IoT (NB-IoT), LoRa, Sigfox

Résumé

L'Internet des objets (IoT, pour Internet of Things, en anglais) ouvre la porte vers la réalisation de nouvelles applications, telles que les compteurs intelligents et le suivi environnemental, destinées à adresser nos défis sociétaux et écologiques actuels et futurs. Les objets, possiblement mobiles ou distants, nécessitent une connectivité sans fil pour la centralisation des données et le contrôle à distance. Les réseaux longue portée et basse consommation (LPWA, pour Low Power Wide Area, en anglais) offrent des transmissions radio bande étroite avec une couverture à l'échelle typique d'une ville, tout en respectant les contraintes de consommation énergétique bas coût des objets.

Intégrer la possibilité de localiser ces objets ajouterait de la valeur à leurs données et permettrait leur suivi géographique. Voilà pourquoi c'est un domaine de recherche très actif actuellement. L'utilisation du temps de propagation des signaux radio de communication, sans intégration supplémentaire de modules matériels dédiés à la localisation, est une approche très intéressante pour la complexité, la consommation et le coût des objets. Néanmoins la radio localisation dans les réseaux LPWA pose des défis liés d'une part aux transmissions à bande étroite qui n'offrent pas une résolution temporelle suffisante et d'autre part aux canaux de propagation qui peuvent introduire des biais sur les estimées de position.

Cette thèse adresse ces défis en étudiant un système de mesure multicanaux de distance pour les réseaux LPWA. La combinaison cohérente des signaux bande étroite transmis séquentiellement sur des canaux différents améliore la précision d'estimation des temps de propagation et permet de résoudre en partie les multi-trajets pour une meilleure précision de localisation. Cette technique basée sur les signaux à bande instantanée étroite conserve la capacité longue portée des transmissions et reste compatible avec les réseaux LPWA. Un modèle détaillé prenant en compte les imperfections matérielles ainsi que les besoins protocolaires pour la synchronisation en temps, fréquence et phase est développé. Basé sur ce modèle, les variantes des architectures des émetteurs-récepteurs radios et leurs impacts sur la cohérence de phase pour l'estimation multicanaux de distance sont discutés. Les limites théoriques de précision sont dérivées pour la propagation en espace libre et dans des canaux de propagation multi-trajets, illustrant l'amélioration de précision possible entre l'approche multicanaux et l'approche monocanal pour l'estimation de distance. Des estimateurs de distance sont développés et appliqués aux signaux radio simulés afin de montrer que leurs performances atteignent les limites théoriques. Ces résultats de simulation sont validés avec des expérimentations menées avec un démonstrateur implémenté avec une radio logicielle (SDR, pour Software Defined Radio, en anglais). Les tests terrains réalisés en environnement urbain permettent de confirmer l'apport d'un système d'estimation multicanaux de distance, en combinaison avec du traitement de signal avancé, pour fournir une fonctionnalité de localisation intrinsèque et précise pour les réseaux LPWA.

Mots clés: Internet des objets (IoT); Réseaux longue portée et basse consommation (LPWA); Radio localisation; Estimation de distance; Sauts de fréquence; Phase d'arrivée (PoA); Traitement cohérent; Narrow-Band IoT (NB-IoT), LoRa, Sigfox

Publications

Patents

- **"Ranging Method for a LPWA Network and Associated Position Estimation Method"**
  "Méthode d'Estimation de Distance dans un Réseau LPWA et Méthode d'Estimation de Position Associée"
  Florian Wolf, Mohamed Sana, Sébastien de Rivaz and François Dehmas
  French patent application filed on 13^{th} *September 2019. Application N° 1910164.*
- **"Ranging Method for a LPWA Network and Associated Position Estimation Method"**
  "Méthode d'Estimation de Distance dans un Réseau LPWA et Méthode d'Estimation de Position Associée"
  Florian Wolf, Sébastien de Rivaz, François Dehmas and Jean-Pierre Cances
  French patent application filed on 13^{th} *September 2019. Application N° 1910165.*
- **"Phase Difference of Arrival Positioning Method for a Wireless Connected Object in a LPWA Network"**
  "Méthode de Localisation d'un Objet Connecté par Différences de Phase d'Arrivée dans un Réseau LPWA"
  Florian Wolf, Sébastien de Rivaz and François Dehmas
  French patent application filed on 13^{th} *May 2020. Application N° 2004730.*

International Journal Communications

- **"Precise Localization in Narrowband LPWA Networks based on Phase Difference of Arrivals"**
  Florian Wolf, Sébastien de Rivaz, François Dehmas and Jean-Pierre Cances
  To be submitted, 2020.

International Conference Communications

- **"Improved Multi-Channel Ranging Precision Bound for Narrowband LPWAN in Multipath Scenarios"**
  Florian Wolf, Christophe Villien, Sébastien de Rivaz, François Dehmas and Jean-Pierre Cances
  2018 IEEE Wireless Communications and Networking Conference (WCNC), Barcelona, Spain, 2018.
- **"Coherent Multi-Channel Ranging for Narrowband LPWAN: Simulation and Experimentation Results"**
  Florian Wolf, Jean-Baptiste Doré, Xavier Popon, Sébastien de Rivaz, François Dehmas and Jean-Pierre Cances
  2018 IEEE 15^{th} *Workshop on Positioning, Navigation and Communications (WPNC)*, Bremen, Germany, 2018.
- **"Benchmarking of Narrowband LPWA Physical Layer Ranging Technologies"**
  Florian Wolf, Kévin Le Déroff, Sébastien de Rivaz, Nicolas Deparis, François Dehmas and Jean-Pierre Cances
  2019 IEEE 16^{th} *Workshop on Positioning, Navigation and Communications (WPNC)*, Bremen, Germany, 2019.
- **"Comparison of Multi-Channel Ranging Algorithms for Narrowband LPWA Network Localization"**
  Florian Wolf, Mohamed Sana, Sébastien de Rivaz, François Dehmas and Jean-Pierre Cances
  2019 The 5^{th} *International Symposium on Ubiquitous Networking (UNet)*, Limoges, France, 2019.
- **"Accurate Narrowband LPWA Ranging: Principles, Performance in AWGN and Multipath Channels"**
  Florian Wolf, Sébastien de Rivaz, François Dehmas, Valérian Mannoni, Vincent Berg and Jean-Pierre Cances
  2020 IEEE 29^{th} *European Conference on Networks and Communications (EuCNC)*, Dubrovnik, Croatia, 2020.

Posters

- **"Multi-Channel Ranging for Low Power Wide Area Networks"**
  Florian Wolf, Sébastien de Rivaz, François Dehmas and Jean-Pierre Cances
  2019 XLIM 9^{th} *PhD Student Poster Workshop of the University of Limoges*, Limoges, France, 2019.

Awards

Best Paper Award

- **"Coherent Multi-Channel Ranging for Narrowband LPWAN: Simulation and Experimentation Results"**
  Florian Wolf, Jean-Baptiste Doré, Xavier Popon, Sébastien de Rivaz, François Dehmas and Jean-Pierre Cances
  2018 IEEE 15^{th} *Workshop on Positioning, Navigation and Communications (WPNC)*, Bremen, Germany, 2018.

Best Paper Award

- **"Comparison of Multi-Channel Ranging Algorithms for Narrowband LPWA Network Localization"**
  Florian Wolf, Mohamed Sana, Sébastien de Rivaz, François Dehmas and Jean-Pierre Cances
  2019 The 5^{th} *International Symposium on Ubiquitous Networking (UNet)*, Limoges, France, 2019.

Best Student Paper Award

- **"Accurate Narrowband LPWA Ranging: Principles, Performance in AWGN and Multipath Channels"**
  Florian Wolf, Sébastien de Rivaz, François Dehmas, Valérian Mannoni, Vincent Berg and Jean-Pierre Cances
  2020 IEEE 29^{th} *European Conference on Networks and Communications (EuCNC)*, Dubrovnik, Croatia, 2020.

Projects

The work of this thesis has partially contributed to the following projects with participation of CEA-Leti.

French Agence Nationale de la Recherche (ANR) Project Application

- **"Eco-responsible IoT Network Conception dedicated to Environmental Surveillance"**
  "Conception Éco-responsable de Réseaux IoT dédiés au Suivi de l'Environnement (CERISE)"

  - *Generic ANR project call 2019, rejected*
    Véronique Perrot-Bernardet (ENSAM)
    Sébastien De Rivaz (CEA-Leti)
    Jean-Pierre Cances (XLIM)
    Olivier Berder (IRISA)
  - *Generic ANR project call 2020, rejected*
    Véronique Perrot-Bernardet (ENSAM)
    Sébastien De Rivaz (CEA-Leti)
    Jean-Pierre Cances (XLIM)
    Olivier Berder (IRISA)
    Olivier Seller (Semtech)

  Position estimation of devices dedicated to environmental surveillance and monitoring is crucial to geo-reference data, which increases its value. Considering an eco-responsible design and realization of monitoring devices is of high importance if mass fabrication and device exposure to nature are envisaged.

  Promising results on the positioning technique obtained in this thesis partially motivated the joint project application which aims at addressing current climatic, ecological and societal challenges.

European Union's Horizon 2020 Research and Innovation Project

- **"5G HEalth AquacultuRe and Transport validation trials (5G-HEART)"**
  H2020-ICT-2018-2020, ICT-19-2019
  5G-HEART project (grant agreement N° 857034)
  Advanced 5G validation trials across multiple vertical industries
  https://5g-ppp.eu/5g-heart, http://5gheart.org

  This project considers amongst others, applications such as the localization of patients with geo-location enabled vital-sign patches. LPWA networks are considered providing indoor and long-range coverage as well as long battery life times.

  The research on precise multi-channel ranging carried out in the thesis partially contributed to this project.

Contents

List of Figures

List of Tables

List of Acronyms

2G · Second Generation
3GPP · 3rd Generation Partnership Project
4G · Fourth Generation
5G · Fifth Generation
ADC · Analog to Digital Converter
AGC · Automatic Gain Control
ALOHA · Additive Links On-line Hawaii Area
AoA · Angle of Arrival
APC · Adaptive Power Control
AP · Access Point
ARM · Advanced RISC Machine
AWGN · Additive White Gaussian Noise
AXI · Advanced eXtensible Interface
BPSK · Binary Phase Shift Keying
BSSID · Basic Service Set Identifier
CDF · Cumulative Distribution Function
CDMA · Code Division Multiple Access
CEPT · European Conference of Postal and Telecommunications Administrations
CFO · Carrier Frequency Offset
CIR · Channel Impulse Response
CNN · Convolutional Neural Network
CORDIC · Coordinate Rotation Digital Computer
COST 259 · European Co-Operation in the field of Scientific and Technical research 259
CPLD · Complex Programmable Logic Device
CRC · Cyclic Redundancy Check
CRLB · Cramer Rao Lower Bound
CRONEN · Coherent Ranging On Narrowband Enabled Networks
CSS · Chirp Spread Spectrum
CW · Continuous Wave
DAC · Digital to Analog Converter
DBPSK · Differential Binary Phase Shift Keying
DMA · Direct Memory Access
DNN · Deep Neural Network
DoA · Direction of Arrival
DPDoA · Double Difference Phase Difference of Arrival
DSSS · Direct Sequence Spread Spectrum
EC-GSM · Extended Coverage GSM
EIRP · Effective Isotropic Radiated Power
EMC · Electromagnetic Compatibility
eMTC · enhanced Machine Type Communication
EPA · Extended Pedestrian A
ERP · Effective Radiated Power
ESPRIT · Estimation of Signal Parameters via Rotational Invariance Technique
ETSI · European Telecommunications Standards Institute
ETU · Extended Typical Urban
FCC · Federal Communications Commission
FDD · Frequency Division Duplex
FDMA · Frequency Division Multiple Access
FEC · Forward Error Correction
FEM · Front End Module
FFT · Fast Fourier Transform
FIFO · First In, First Out
FIM · Fisher Information Matrix
FIR · Finite Impulse Response
FPGA · Field Programmable Gate Array
FSK · Frequency Shift Keying
GDOP · Geometric Dilution of Precision
GNSS · Global Navigation Satellite System
GPIO · General Purpose Input Output
GPS · Global Positioning System
GSM · Global System for Mobile Communications
HTx · Hilly terrain
IDFT · Inverse Discrete Fourier Transform
IEEE · Institute of Electrical and Electronics Engineers

IF · Intermediate Frequency
IoT · Internet of Things
ISM · Industrial, Scientific and Medical
ITU · International Telecommunication Union
JM · Jacobian Matrix
kNN · k-Nearest Neighbors
LBT · Listen Before Talk
LIDAR · Light Detection and Ranging
LNA · Low Noise Amplifier
LoRaWAN · Long-Range Wide Area Network
LoS · Line of Sight
LO · Local Oscillator
LPWA · Low Power Wide Area
LTE · Long Term Evolution
LUT · Look-Up Table
M2M · Machine to Machine
MAC · Medium Access Control
MATLAB · MATrix LABoratory
M-DNN · Mixed Data Trained DNN
MIMO · Multiple Input Multiple Output
ML · Maximum Likelihood
MUSIC · Multiple Signal Classification
NB-IoT · Narrow-Band IoT
NLoS · None Line of Sight
OFDMA · Orthogonal Frequency Division Multiple Access
OFDM · Orthogonal Frequency Division Multiplexing
PAPR · Peak to Average Power Ratio
PA · Power Amplifier
PCI · Peripheral Component Interconnect
PDoA · Phase Difference of Arrival
PEB · Position Error Bound
PLG · Programmable Logic Gate
PLL · Phase-Locked Loop
PoA · Phase of Arrival
PoF · Phase of Flight
PPS · Pulse Per Second
PRS · Positioning Reference Signal
PSD · Power Spectral Density
PSK · Phase Shift Keying
PowDoA · Power Difference of Arrival
QoS · Quality of Service
QPSK · Quadrature Phase Shift Keying
RADAR · Radio Detection and Ranging
RAM · Random Access Memory
Rax · Rural area
R-DNN · Real Data Trained DNN
ReLU · Rectifier Linear Unit
RFID · Radio Frequency Identification
RF · Radio Frequency
RISC · Reduced Instruction Set Computing
RMS · Root Mean Square
RSSD · Received Signal Strength Difference
RSSI · Received Signal Strength Indicator
RTK-GPS · Real-Time Kinematic GPS
RX · Receiver
SC-FDMA · Single Carrier FDMA
S-DNN · Synthetic Data Trained DNN
SDR · Software Defined Radio
SD · Secure Digital
SFD · Start of Frame Delimiter
SFO · Sampling Frequency Offset
SF-RADAR · Step Frequency RADAR
SGD · Stochastic Gradient Descent
SLAM · Simultaneous Localization and Mapping
SNR · Signal to Noise Ratio
SoC · System on Chip
SPI · Serial Peripheral Interface
SRD · Short-Range Device
SVD · Singular Value Decomposition
SX1280 · LoRa 2.4 GHz SX1280
TDoA · Time Difference of Arrival
ToA · Time of Arrival
ToD · Time of Departure
ToF · Time of Flight
Tux · Typical urban
TX · Transmitter
UMTS · Universal Mobile Telecommunication System
UNB · Ultra-Narrow Band
UWB · Ultra-Wide Band
VCTCXO · Voltage Controlled Temperature Compensated Crystal Oscillator
VHDL · Very High Speed Integrated Circuit Hardware Description Language
WiFi · "Wireless Fidelity"
ZC · Zadoff-Chu
ZZLB · Ziv Zakai Lower Bound

List of Symbols

Math operators.

$\lvert\cdot\rvert$	Absolute value.
$\arg\{\cdot\}$	Angle/argument of complex value.
$\arg\max_q \{g(q)\}$	Argument of the maximum of $g(q)$.
$\arg\min_q \{g(q)\}$	Argument of the minimum of $g(q)$.
I_k	Modified k^{th}-order Bessel function of first kind.
$\lceil\cdot\rceil$	Ceiling.
$(\cdot)^*$	Complex conjugate.
$*$	Convolution.
$\cos(\cdot)$	Cosine.
$\text{cov}\{\cdot\}$	Covariance.
$\Omega_{r,s}$	Cross correlation between signals r and s.
$\tilde{\Omega}_{r,s}$	Normalized cross correlation between signals r and s.
$\delta(\cdot)$	Dirac function.
$\text{diag}\{\cdot\}$	Diagonal matrix.
$\mathbb{E}_q[g(q)] = \int_{\infty}^{\infty} qg(q)dq$	Expectation.
$\widehat{(\cdot)}$	Estimated value.
$\forall q$	For all q.
$\nabla(\cdot)$	Gradient operator.
$\mathcal{I}\{\cdot\}$	Imaginary part.
$[e,q)$	Interval with closed border, including e and open border, excluding q.
j	$j \cdot j = -1$.
$\max_q \{g(q)\}$	Maximum of $g(q)$.
$\overline{(\cdot)}$	Mean value.
$\text{mean}_q \{g(q)\}$	Mean of $g(q)$.
$\text{median}_q \{g(q)\}$	Median of $g(q)$.
$\min_q \{g(q)\}$	Minimum of $g(q)$.
$\lVert\cdot\rVert_2$	L_2-norm.
$\mathcal{N}\left(\mu,\sigma^2\right)$	Normal distribution with mean μ and variance σ^2.
$\frac{\partial g(q)}{\partial q}$	Partial derivative of $g(q)$.
$p(e\lvert q)$	Probability distribution function of e for a given q.
$Q(\cdot)$	Gaussian error function.
$\mathcal{R}\{\cdot\}$	Real part.
$\Pi_T(t)$	Rectangular window of length T.
$\sin(\cdot)$	Sine.
$\tan(\cdot)$	Tangent.
$\text{trace}\{\cdot\}$	Trace of a matrix.
$(\cdot)^{\text{T}}$	Transpose.
$(\cdot)^{\text{unit}}$	Variable in *unit*.
$\text{Var}\{\cdot\}$	Variance.
$(\cdot)^{[X]}$	Entity belonging to node X.
$(\cdot)^{[X,Y]}$	Entity considering a transmission from node X to node Y.

Number sets.

$\mathbb{C}$	Set of complex numbers.
$\mathbb{R}$	Set of real numbers.
$\mathbb{Z}$	Set of integer numbers.

Symbols.

A	Signal amplitude.
$\mathcal{A}$	Parameter for CRLB.
A_c	Complex amplitude at channel c.
$\boldsymbol{a}$	Acceleration vector.
α_c	Multipath channel amplitude at channel c.
a_p	Complex amplitude of the p-th multipath component.
a'_p	Complex amplitude of the p-th multipath component, integrating path delay phase rotation at the carrier frequency.
$A_{\mathbf{V}}$	Variable attenuation.
az	Azimuth angle.
B	Bandwidth (instantaneous).
$\mathcal{B}_{\text{DNN}}$	Mini-batch.
$\mathcal{B}$	Parameter for CRLB.
B_{coh}	Cannel coherence bandwidth.
B_{d}	Doppler spread.
β	Path amplitude ratio.
b_i	Building i.
B_{m}	Measurement bandwidth.
B_{res}	Resolution bandwidth.
B_{RMS}	RMS-bandwidth.
B_{virt}	Virtual bandwidth.
C	Number of channels.

c	Channel index.
c^0	LoRa base chirp.
c_0	Speed of Light.
$\boldsymbol{\mathcal{X}}$	Imaging matrix.
$\boldsymbol{\chi}$	Imaging vector.
c_{sound}	Speed of Sound.
C_{st}	Constant summarizing constant terms in Friis law.
C_{st0}	Friis attenuation at distance d_0.
D	Spacing of antenna array element/laser beams.
$\mathcal{D}$	DNN training dataset.
d	Distance.
Δd	Distance difference.
$\Delta\alpha_c$	Multipath channel amplitude at channel c relative to a center channel.
$\Delta\Delta d$	Double difference distance.
$\Delta\Delta\phi_{\text{A}}$	Double Difference Phase of Arrival.
$\Delta\Delta T_{\text{A}}$	Double Time Difference of Arrival.
$\Delta d_{u,i,k}$	Distance difference between node with unknown position and anchor i and anchor k.
$\Delta\lambda_{\text{w}}$	Virtual wavelength.
$\Delta\phi_{\text{A}}$	Phase Difference of Arrival.
$\Delta\varphi_c$	Multipath channel phase at channel c relative to a center channel.
$\Delta\phi_{\text{R}}$	Redefinition of local oscillator phase difference for CRLB formulation.
$\Delta\tilde{\phi}_{\text{R}}$	Phase difference of local oscillator initial phases.
ΔR	Range resolution.
δ_{T}	Time dilatation.
ΔT_{A}	Time Difference of Arrival.
$\Delta\tau$	Delay difference.
Δf	Equidistant multi-channel frequency spacing.
δ_f	Time invariant relative frequency offset.
δf	Offset frequency from the nominal oscillator frequency.
δ_f^+	1+ time invariant relative frequency offset, $\delta_f^+ = 1 + \delta_f$.
δ'_f	Time variant relative frequency drift.
$d_{i,0}$	Distance between anchor i and anchor 0.
$\widehat{d}_{\cdot\,\text{BR}}$	Estimated distance without biased measurements (bias removed).
$\widehat{d}_{\text{PoF}}$	Estimated multi-channel PoF distance.
$\widehat{d}_{\text{PoF,CIR-calib}}$	Estimated multi-channel PoF CIR bias calibrated distance.
$\widehat{d}_{\text{PoF,CIR-first}}$	Estimated multi-channel PoF CIR first path distance.
$\widehat{d}_{\text{PoF,CIR-max}}$	Estimated multi-channel PoF CIR maximum amplitude distance.
$\widehat{d}_{\text{PoF,DNN}}$	Estimated multi-channel PoF DNN determined distance.
$\widehat{d}_{\text{PoF,M-DNN}}$	Estimated multi-channel PoF M-DNN determined distance.
$\widehat{d}_{\text{PoF,MUSIC}}$	Estimated multi-channel PoF MUSIC determined distance.
$\widehat{d}_{\text{PoF,S-DNN}}$	Estimated multi-channel PoF S-DNN determined distance.
$\widehat{d}_{\text{PoF,Slope}}$	Estimated multi-channel PoF slope distance.
$\widehat{d}_{\cdot\,\text{IPq}}$	Estimated distance on q-times interpolated received signals.
$\widehat{d}_{\cdot\,\text{Sq}}$	Estimated distance smoothed over q successive independent measurements.
$\widehat{d}_{\text{ToF}}$	Estimated single channel ToF distance.
$\widehat{d}_{\text{ToF,MC-mean}}$	Estimated multi-channel mean ToF distance.
$\widehat{d}_{\text{ToF,MC-median}}$	Estimated multi-channel median ToF distance.
d_{max}	Maximum distance covered in the field trial.
$d_{u,i}$	Distance between node with unknown position and anchor i.
$\boldsymbol{d}$	Estimated distance vector.
$\mathcal{E}$	Average power gain of the delay profile/a multipath component.
E_{b}	Energy of one bit.
ϵ	Error.
$\epsilon_{\widehat{d}}$	Range estimation error.
$\epsilon_{\widehat{\delta}_f}$	Relative frequency estimation error.
ϵ_{rms}	RMS error.
$\epsilon_{T_{\text{Samp}}}$	Sampling resolution error.
E_{S}	Energy of a symbol.
$E_{\text{S,ranging}}$	Energy of a ranging symbol.
η	Spectral efficiency.
$\mathcal{F}$	Frequency offset search space.
F	Sample data size.
f	Frequency.
f_c	Channel frequency at channel c.
f_{d}	Doppler frequency.
f_{Samp}	Sampling frequency.
$f_{\text{Samp,BB}}$	Baseband sampling frequency.
$f_{\text{Samp,IF}}$	IF sampling frequency.
f_{w}	Carrier frequency.
f'_{ξ^i}	Instantaneous frequency of a LoRa down-chirp.

f_{ξ^i}	Instantaneous frequency of a LoRa up-chirp.
$\mathbf{\Gamma}$	Hankel matrix.
γ_{a_H}	High time threshold.
γ_{a_L}	Low time threshold.
γ_first	First path power threshold.
γ_L	Path loss exponent.
$\gamma_{\tau_\mathrm{max}}$	Minimum power for the maximum excess delay path.
$\mathrm{GDoP_c}$	Circular Geometric Dilution of Precision.
$\mathrm{GDoP_h}$	Hyperbolic Geometric Dilution of Precision.
g_k	Complex gain of antenna element k.
G_r	Antenna gain at receiver side.
g_R	Complex radio transceiver hardware gain.
G_t	Antenna gain at transmitter side.
$g^{\boldsymbol{w}}$	Regression function.
H	Channel transfer function.
h	Channel impulse response.
h_b	Base station antenna height.
$\tilde{H}_c$	Short form for $H^{[1,2]}_{\mathrm{PoF},c}$.
h_m	Mobile node antenna height.
h_max	Amplitude of strongest multipath component.
$\widehat{H}_{\mathrm{PoA}_c}$	Estimated one-way channel transfer function at channel c.
h_PoA	One-way channel impulse response.
$\widehat{H}_{\mathrm{PoF}_c}$	Estimated two-way channel transfer function at channel c.
h_PoF	Two-way channel impulse response.
I	Fischer information.
$\boldsymbol{I}$	Fischer information matrix.
J	Jacobian.
$\boldsymbol{J}$	Jacobian matrix.
K	Number of samples/symbols.
k	Sample/symbol index.
K_A	Number of antenna array elements.
κ_τ	Delay profile Kurtosis.
k_B	Constant of Boltzmann.
K_BS	Number of anchors/base stations.
K_code	Code length.
K_IDFT	IDFT length.
K_preamble	Number of preamble symbols.
K_ranging	Number of ranging symbols.
$K_\mathrm{resolution}$	IQ bit resolution.
K_S	Number of samples in waveform s_0.
L	Link budget.
$\mathcal{L}$	Loss function.
λ_w	Carrier wavelength.
L_Γ	Hankel matrix dimension.
L_path	Path loss.
$\mathcal{L}_\mathrm{single-side}$	Single-side phase noise spectrum.
M	Symbol alphabet size.
m	Number of bits per symbol.
$\mathcal{M}_i$	Location solving metric i.
μ	Mean.
μ_I	Mean in-phase value.
μ_Q	Mean quadrature value.
$\tilde{\boldsymbol{N}}$	Noise vector on two-way channel transfer function estimate.
N	Noise signal spectrum.
n	Noise signal.
N_0	Noise spectral density.
$\tilde{N}_c$	Noise on two-way channel transfer function estimate on channel c.
n_Channel	Shadowing and small-scale fading effect on received power.
N_F	Noise figure.
n_Range	Range estimation noise.
$\boldsymbol{n}_\mathrm{Range}$	Range estimation noise vector.
n_RSSI	RSSI estimation noise.
O	Number of performed measurements.
ω_D	Doppler direction finder rotation speed.
$\Omega_{H,H}$	Spaced-time, spaced-frequency correlation function.
$\Omega_{h,h}$	CIR autocorrelation function, multipath intensity profile, delay power profile.
P	Number of multipath components.
p	Multipath component index.
p_A	Amplitude probability distribution.
PEB	Position error bound.
l	Integer phase ambiguity.
ϕ	Phase.
ϕ_A	Phase of Arrival.
$\phi_{\mathrm{A}c}$	Phase of Arrival at channel c.
φ_c	Multipath channel phase at channel c.
ϕ_g	Gaussian phase noise.
ϕ_PN	Phase noise.
ϕ_PoF	Phase of Flight.
$\phi_{\mathrm{PoF}c}$	Phase of Flight at channel c.
ϕ_R	Local oscillator initial phase.
$\phi_{\mathrm{R}c}$	Local oscillator initial phase at channel c.
$\tilde{\phi}_{\mathrm{R}\,c}$	Local oscillator initial phase at channel c integrating clock offset, drift and phase noise.
ϕ_w	Wiener phase noise.
p_i	Propagation path i.
P_min	Error probability of optimum decision rule.
P_n	Noise power.
pol	Polar angle.
P_r	Power at the receiver side.

P_{req}	Receiver sensitivity.
PSD	Power spectral density.
ψ_τ	NLoS proportionality factor.
P_{t}	Power at the transmitter side.
R	Observation.
R	Data rate.
r	Time signal on the receiver side.
r_{ADC}	ADC input signal.
r_c	Final baseband received signal on channel c.
R_{D}	Doppler direction finder radius.
R_{first}	First path distance search space.
$R_{\text{Fresnel},k}$	k^{th} Fresnel zone radius.
ρ	DNN learning rate.
r_{IF}	IF signal on the receiver side.
R_{max}	Maximum unambiguous range.
r_{R}	RF receive signal.
$\boldsymbol{R}$	Observation vector.
s	Time signal on the transmitter side.
S_0	Transmit signal spectrum.
s_0	Transmit signal.
S_D	Doppler power spectrum.
s_{DAC}	DAC output signal.
r_Δ	Difference time signal.
s_{IF}	IF signal on the transmitter side.
σ	Standard deviation.
σ_{Allan}	Allan standard deviation.
σ_{Channel}	Standard deviation of the shadowing and small-scale fading effect on received power.
$\Sigma\Delta\phi_{\text{R}}$	Sum-difference of initial oscillator phases.
σ_g	Gaussian phase noise standard deviation.
σ_{Range}	Standard deviation of the range estimation error.
$\boldsymbol{\sigma}_{\text{Range}}$	Standard deviation vector of the range estimation error.
σ_{RSSI}	Standard deviation of the RSSI estimation noise.
$\boldsymbol{\Sigma}_{\boldsymbol{R}}$	Observation noise covariance matrix.
σ_τ	Delay spread.
$\boldsymbol{\Sigma}_{\boldsymbol{\theta}}$	Prior information on unknown estimation parameter.
σ_w	Wiener phase noise standard deviation.
$\Sigma_{\boldsymbol{R}}$	Observation noise variance.
s_{LO}	Local oscillator signal.
s_{LoRa}	LoRa signal.
SNR	Signal to noise ratio.
$S_{\phi_{\text{PN}}}$	Phase noise power spectral density.
s_{PSK}	Pulse shaped PSK signal.
s_{R}	RF transmit signal.
r_Σ	Sum time signal.

T	Time duration.
$\mathcal{T}$	Time of Arrival search space.
t_0	Time offset.
t_{A}	Time of Arrival.
T_{air}	Time on air.
$\overline{\tau}$	Mean delay.
τ	Delay.
$\overline{\tau}_e$	Mean excess delay.
$\tau_{h_{\text{max}}}$	Delay of the strongest multipath component.
τ_{max}	Maximum excess delay.
τ_p	Propagation delay of the p-th multipath component.
τ_{RMS}	RMS delay.
T_{b}	Time of one bit.
T_{beam}	Beam dwell time.
T_{coh}	Channel coherence time.
t_{D}	Time of Departure.
Temp	Temperature.
t_{H}	High time.
θ	Unknown estimation parameter.
$\Theta_{i,k}$	Angle spanned by the vectors $\boldsymbol{x}_i$ and $\boldsymbol{x}_k$.
$\boldsymbol{\theta}$	Unknown estimation parameter vector.
t_{L}	Low time.
T_{local}	Time in local time scale.
T_{m}	Multipath spread.
T_{packet}	Time of one packet.
T_{preamble}	Time of one preamble.
T_{pulse}	Time of one pulse.
T_{ranging}	Time of one ranging signal transmission.
T_{real}	Time in global/real time scale.
$T_{\text{resolution}}$	Time resolution.
T_{response}	Node response time between reception and transmission.
t_{rise}	Rise time of amplitude delay profile.
T_{S}	Time of one symbol.
T_{Samp}	Time of one sample.
T_{ToF}	Time of Flight.
T_{turn}	Time of one beam rotation.
T_{w}	Time of one carrier cycle.
$\boldsymbol{U}_{\text{N}}$	Noise subspace U.
$\boldsymbol{U}_{\text{S}}$	Signal subspace U.
$\boldsymbol{u}$	Reference direction/antenna broadside.
$\boldsymbol{v}_0$	Initial velocity vector.
$\boldsymbol{V}_{\text{N}}$	Noise subspace V.
$\boldsymbol{V}_{\text{S}}$	Signal subspace V.
$\boldsymbol{w}$	Network weights.
w_i	Location solver weight i.
$W_{i,k}$	Area spanned by the vectors $\boldsymbol{x}_i$ and $\boldsymbol{x}_k$ for GDOP interpretation.
$\boldsymbol{X}$	Anchor placement matrix.
$\boldsymbol{x}$	Coordinate vector.

x	x coordinate.
$\boldsymbol{x}_0$	Initial position.
ζ	Complex symbol/LoRa chirp.
x_i	x-coordinate of anchor i.
x_k	x-coordinate of anchor k.
$\dot{\boldsymbol{x}}$	Velocity vector.
$\ddot{\boldsymbol{x}}$	Acceleration vector.
x_u	x-coordinate of node with unknown position.
$\boldsymbol{x}_u$	Coordinate vector of node with unknown position.
$\mathcal{Y}$	Imaging function.
y	y coordinate.
y_i	y-coordinate of anchor i.
y_k	y-coordinate of anchor k.
y_u	y-coordinate of node with unknown position.
Z	System impedance.
z	z coordinate.
ζ_{opt}	Threshold for LoS/NLoS classification.
z_i	z-coordinate of anchor i.
z_k	z-coordinate of anchor k.
z_u	z-coordinate of node with unknown position.

Introduction

Wireless communication is a constantly evolving field of research and development, which profoundly changes everyday life. With the experimental discovery of electromagnetic waves by Heinrich Hertz in 1886 and the first long-range wireless transmissions performed by Guglielmo Marconi in 1895 a new era of communication began. Later followed by the introduction of cellular mobile services and their worldwide standardization with the Global System for Mobile Communications (GSM), wireless communication and data transfer was made available to everyone. Together with the invention of the Internet, global communication, exchange and trade were revolutionized and in return boost growth and development of new wireless communication standards. Nowadays, the Second Generation (2G) to the Fourth Generation (4G) of mobile communication increase available data rate, connectivity, coverage and offer more services, bringing communication closer to the user [Var12].

Currently, the Fifth Generation (5G) of mobile communication is about to be developed. Besides ever improved quality of service for the user, the 5G will also be an enabler for inter-machine communication [NGM15]. Generally called Internet of Things (IoT), the concept aims at connecting everyday-life objects to the Internet, allowing user or machine interaction with these devices. Many of these objects, especially the mobile ones, such as temperature sensors, air quality monitors or object tracking devices, have to be energy autonomous and require wireless communication over possibly long ranges [RKS17]. Therefore, long-range, asynchronous wireless connectivity, together with low power and low-cost mass market solutions are part of the key enablers for the IoT.

Wireless technologies addressing these requirements are called Low Power Wide Area (LPWA) networks. Achieving long-range connectivity is a major challenge for these networks as transmit power is limited for energy consumption and radio spectrum regulations reasons. Available LPWA technologies include proprietary industrial solutions as well as standardized technologies being part of the 5G. Two approaches are used to attain low levels of receiver sensitivity for long-range communication: narrow bandwidth or low spectral efficiency modulation schemes [Rot17]. In both cases, data rate is traded against sensitivity, which is convenient as LPWA devices primarily have payloads of only a few bytes to transmit. Besides the long-range communication capability, LPWA systems and applications show a growing demand for geo-referencing and localizing objects and the data they produce [Eff].

Requirements on LPWA positioning vary in the demanded accuracy, availability, complexity and depend on each application. A majority of LPWA devices will be Global Navigation Satellite System (GNSS) denied due to energy consumption constrains or signal unavailability. Instead, LPWA signals transmitted for communication can be used with radio signal based localization methods in order to determine device position. Subsequently, system complexity, energy consumption and cost are kept at a minimum. Radio transmissions are altered in amplitude, time, frequency and phase by the wireless propagation channel. Relating these signal alteration to device position, allows location estimation based on measurements of radio signal changes.

This thesis investigates the feasibility and a proof of concept implementation of a localization method within LPWA networks. The studied approach achieves both, accurate and precise ranging as well as fulfilling long-range low-cost and low-power requirements. Time of Arrival (ToA) techniques which deduce inter-device range from the propagation delay do not provide the required precision due to narrowband LPWA signals. Assuming narrowband transmissions as an inevitable system constraint, multi-channel ranging techniques potentially offer improved temporal resolution for precise ranging. This signal phase based approach coherently combines multiple sequentially measured narrowband channel estimations on different frequencies in order to virtually increase bandwidth and so ranging performances. Multi-channel ranging has been widely adopted in various contexts, i.e. [PSSV09a; VKK16; SRW18]. However, its application to LPWA long-range transmissions yet remains open and is the aim of the present thesis. This work studies attainable precision under different propagation conditions, necessary requirements on transceiver architectures and oscillator specifications to achieve phase based multi-channel ranging with low-cost LPWA devices. Extensive study by theoretical models, numerical simulation, experimental validation and field trials demonstrate the potential of the solution.

Review of the Chapter Contents

The **first chapter** introduces the principles of wireless communication in LPWA networks. It further motivates why LPWA networks benefit or require a positioning function. Key performance indicators for localization techniques are discussed and a detailed overview on radio signal based localization techniques and the underlying metrics are presented. Existing LPWA technologies are reviewed regarding available positioning functions and new positioning techniques are given.

In the **second chapter** a focus on challenges for LPWA radio localization is made. These are categorized into system limitations such as limited bandwidth to achieve long-range communication and network topology. Secondly, hardware impairments including oscillator frequency offset and their impact on radio signal based localization are studied. The third category of challenges is related to the propagation channel. Various metrics characterizing the radio channel are defined and their significance for precise and accurate positioning is studied.

Based on the literature review from the first chapter and the dressed challenges, the arising research questions and the scope of the thesis are motivated.

The **third chapter** derives the signal model for multi-channel ranging based on a general radio transceiver architecture including a numerical Intermediate Frequency (IF) mixing stage. The signal model is then adapted to two-way ranging and the resulting requirements for the transceiver architecture are discussed. Theoretical CRLBs on the ranging precision are derived based on the presented signal model. Preliminary numerical simulations are used to validate the proposed ranging algorithms.

The development and implementation of a multi-channel transceiver testbed for experimentations and outdoor field trials is presented in the **fourth chapter**. Ranging performances are evaluated through both numerical simulations and experimentations in an Additive White Gaussian Noise (AWGN) channel. Hardware impairments such as clock frequency offset are investigated. Simulations with an European Telecommunications Standards Institute (ETSI) multipath channel model are used to predict ranging performances in multipath channels. Outdoor field trials are performed to benchmark ranging precision and accuracy under real urban propagation conditions. The comparison to an industrial LPWA ranging solution is given. Performances impeded by multipath propagation are improved through a bias mitigation, outlier detection and elimination scheme.

The **fifth chapter** proposes advanced range estimation algorithms for multi-channel ranging in order to improve the accuracy under real multipath propagation. A high-resolution Multiple Signal Classification (MUSIC) based range estimator and a learning based Deep Neural Network (DNN) approach are compared to the initial Inverse Discrete Fourier Transform (IDFT) based range estimator. Algorithms are compared on simulated data and on real field trial measurements.

1

Localization for LPWA Networks

"It is of great advantage to the student of any subject to read the original memoirs on that subject, for science is always most completely assimilated when it is in the nascent state..."

— James Clerk Maxwell (1831 – 1879)

Chapter contents

This chapter motivates the need for a positioning functionality for Low Power Wide Area (LPWA) networks and states some typical use cases. In the following, the basic principles of communication within these networks are introduced and existing LPWA solutions and standards are presented. Further, an overview on radio based localization techniques and the underlying metrics is given. Finally, LPWA positioning solutions and emerging candidates are reviewed.

1.1 Philosophy of LPWA Networks

Since the early days of wireless communication, research and development focuses on how the quality of service for users can be improved. The standardization of global mobile communication services has focused much on increasing data rate, reliability and coverage during the last generations (Second Generation to Fourth Generation). With the advent of the Fifth Generation (5G) of mobile wireless communications not only user to user communication but also inter-machine communications are in the focus of study [Pal+16]. This concept, called Internet of Things (IoT) aims to connecting everyday-life objects to the Internet, allowing interaction with users or other machines and objects. A majority of these objects is either mobile or dispatched on large areas, requiring wireless communication. Wireless technologies addressing these requirements are called and grouped as LPWA networks.

Typical applications for LPWA networks include water metering or smoke detectors, where information on consumption or a possible fire alert is transmitted wirelessly to providers or fire fighters respectively. Other applications, where the need for georeferenced data is manifest, are environmental or animal behavior monitoring, parcel tracking or forest fire detection.

During the Second Generation (2G) to Fourth Generation (4G) of wireless communication an increasing number of users became connected. Studies forecast that the 5G will provide a massive access to connected objects [NGM15]. The data as such, *e.g.* the temperature recording of a single sensor in the mountains has little value, however it becomes meaningful for a large number of distributed sensors. Especially when the data is georeferenced [Eff], it can serve *e.g.* to detect the risk of avalanches.

Location information can simplify network deployment as illustrated by the application of forest fire detection, where wireless nodes comprising temperature and gas sensors can be dropped out of an airplane [TKL11]. Once distributed on the zone of interest, the nodes automatically locate themselves, avoiding a manual *place and note the position* procedure. Geo-located alerts enable efficient fire fighter intervention.

Passing information efficiently and rapidly from source to destination is crucial to all communication systems. The process of routing information from source to destination has to consider the quality of the transmission channel. This process can be aided by positioning knowledge of neighboring nodes, which then can serve strategies that optimize data transfer *e.g.* by geographical routing [BP17].

Besides technical challenges, which come along the advent of IoT solutions, societal and ethical questions have to be addressed as well. Smart metering applications, aiming at the reduction of water or electrical energy consumption, face the paradox of consuming resources in order to save resources. The upgrading of existing meters to enable wireless access consumes resources (*e.g.* installation, hardware), however it aims at real-time consumption monitoring to save water or electrical energy.

Concepts on data ownership, privacy and security of the data transmitted by the huge amount of possibly locatable things have to be reviewed. Particularly when data is traded in business, offering control and power [Lia+18].

Wireless connected sensor nodes used in wide area monitoring for environmental studies, use rare natural resources and increase electronic and electromagnetic pollution, i.e. rare earth metals and Electromagnetic Compatibility (EMC). The whole lifecycle, comprising design, development, production, usage and recycling needs to be sustainable by following an eco-responsible approach [Uni; LRV11].

1.2 Long-Range Communication

1.2.1 Requirements

Communication technologies designated for LPWA use cases typically meet the following requirements [RKS17]:

- Low-complexity radio transceiver architectures.
- Low-cost devices due to a massive deployment and integration into consumer connected objects.

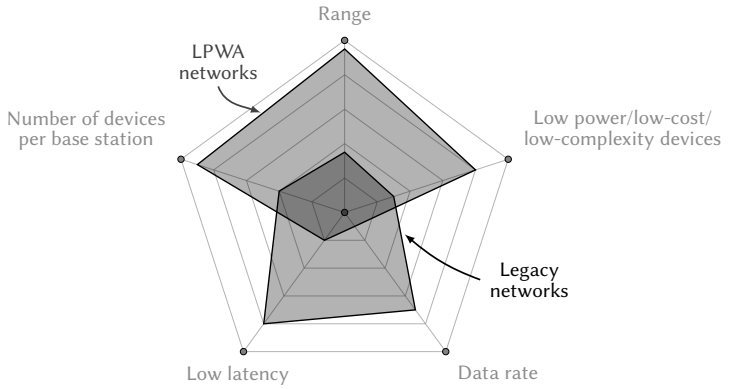


FIGURE 1.1 – *Requirements for legacy mobile communication networks and LPWA networks, according to [Rot17].*

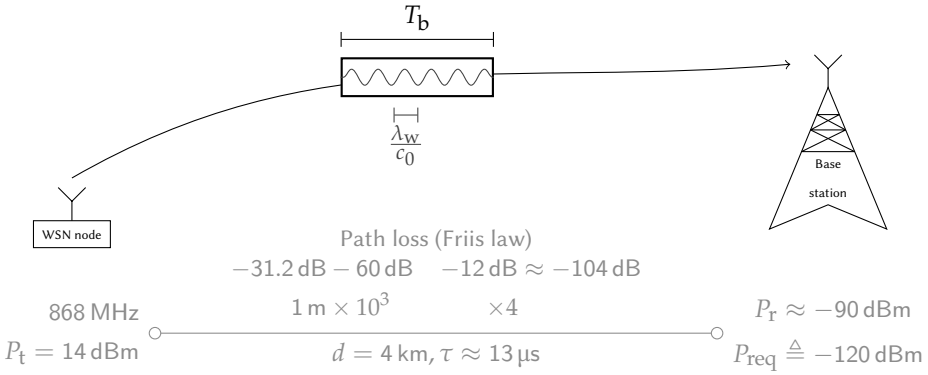


FIGURE 1.2 – *Typical link budget for a transmission between a node and a base station, considering the SRD* 868 MHz *band, Friis law and a* 4 km *distance in a LPWA network.*

- Low-power consumption for autonomous battery powered operation over several years without space for large batteries and the possibility for their replacement if devices are *e.g.* sealed.
- Low-payload size communication as most objects only transmit a few sensor values.
- Long-range communication capability to cover large areas with sparse base station density.

These requirements are not met by legacy mobile communication technologies, which provide low latency and high data rate communication at a trade-off of massive access, complexity, cost, power consumption and communication range as depicted in Figure 1.1.

1.2.1.1 Principles of Communication

In order to explain the strategies to achieve long-range communication, basic principles of communication are explained according to [Rot17].

Considering a wireless sensor node transmitting data to a base station as illustrated in Figure 1.2, average transmit power P_t and average received power P_r can be linked to the range d between node and base station by the Friis formula [Fri46] for Line of Sight (LoS) communication

$$P_r = P_t G_t G_r \left(\frac{\lambda_w}{4\pi d}\right)^2, \tag{1.1}$$

with transmit G_t and receive G_r antenna gain and wavelength λ_w. Assuming wavelength and antenna gains to be fixed, power and range are linked as follows $P_r = C_{st} P_t / d^2$.

For achieving long-range communication, either transmission power needs to be increased or receivers must be capable of receiving at low levels of received power. Choosing arbitrary high levels of transmit power conflicts with the requirement for low-power consumption and radio regulation. Hence, focus lies on methods for lowering the minimum required received power in order to enable long-range communication.

The receiver disposes of the bit energy defined by the received signal power P_r and the bit duration T_b. The energy available to achieve demodulation and information extraction is given by

$$E_\mathrm{b} = P_\mathrm{r} T_\mathrm{b} = \frac{P_\mathrm{r}}{R}, \tag{1.2}$$

with data rate $R = 1/T_\mathrm{b}$.

In addition, electronic systems experience thermal noise [Loy99]. For a receiver bandwidth B, the thermal noise power is given by

$$P_\mathrm{n} = N_0 B = k_\mathrm{B} \mathrm{Temp} B, \tag{1.3}$$

with noise spectral density N_0, which is proportional to the Boltzmann constant k_B (equal to $1.3806 \cdot 10^{-23}$ Joules $\cdot$ K^{-1}) and ambient system temperature Temp in Kelvin.

At the receiver side the Signal to Noise Ratio (SNR) is defined by

$$SNR = \frac{P_\mathrm{r}}{P_\mathrm{n}} = \frac{E_\mathrm{b} R}{N_0 B}. \tag{1.4}$$

In order to achieve communication with a specified level of error, a minimum Signal to Noise Ratio SNR_min is required which can be linked to a required minimal received power, called receiver sensitivity

$$P_\mathrm{req} = SNR_\mathrm{min} N_0 B. \tag{1.5}$$

As technically usual and in order to deal with very small and large values at the same time, quantities are expressed on a logarithmic scale. The measure in decibels (dB) is defined as 10 times the base-10 logarithm. Received power can be given in decibels by

$$\left(P_\mathrm{req}\right)^\mathrm{dBm} = \left(SNR_\mathrm{min}\right)^\mathrm{dB} + \left(10 \log_{10}\left(N_0 \cdot 10^3\right)\right)^\mathrm{dBm} + \left(10 \log_{10}\left(B\right)\right)^\mathrm{dB}. \tag{1.6}$$

Due to imperfect receivers, which add a supplementary noise, the minimum required received power is rewritten with the noise figure N_F

$$\left(P_\mathrm{req}\right)^\mathrm{dBm} = \left(SNR_\mathrm{min}\right)^\mathrm{dB} + \left(10 \log_{10}\left(N_0 \cdot 10^3\right)\right)^\mathrm{dBm} + \left(10 \log_{10}\left(B\right)\right)^\mathrm{dB} + \left(N_\mathrm{F}\right)^\mathrm{dB}. \tag{1.7}$$

Typical receiver architectures [Loy99] achieve noise figures between 1 dB and 15 dB and $10 \log_{10}\left(N_0 \cdot 10^3\right)$ is taken equal to -174 dBm/Hz at Temp $\simeq 290$ K ($\simeq 17$ °C).

Considering (1.4), the SNR can be rewritten as

$$SNR = \frac{E_\mathrm{b}}{N_0} \eta, \tag{1.8}$$

where $\eta = R/B$ defines the spectral efficiency.

Finally, the minimum required received power can be rewritten with (1.7) and (1.8) as

$$\begin{aligned} \left(P_\mathrm{req}\right)^\mathrm{dBm} &= \left(\frac{E_\mathrm{b}}{N_0}\right)_\mathrm{req}^\mathrm{dB} + 10 \log_{10}\left(\eta\right) + 10 \log_{10}\left(N_0 \cdot 10^3\right) + 10 \log_{10}\left(B\right) + \left(N_\mathrm{F}\right)^\mathrm{dB} \\ &= \left(\frac{E_\mathrm{b}}{N_0}\right)_\mathrm{req}^\mathrm{dB} + 10 \log_{10}\left(N_0 \cdot 10^3\right) + 10 \log_{10}\left(R\right) + \left(N_\mathrm{F}\right)^\mathrm{dB}. \end{aligned} \tag{1.9}$$

Long-range communication can be achieved by maximizing the link budget defined by

$$\left(L\right)^\mathrm{dB} = \left(P_\mathrm{t}\right)^\mathrm{dBm} - \left(P_\mathrm{req}\right)^\mathrm{dBm}. \tag{1.10}$$

While transmit power is limited due to legislation, three possible strategies exist in order to attain low levels of receiver sensitivity:

- Decrease required bit energy to noise spectral power ratio $\left(E_\mathrm{b}/N_0\right)_\mathrm{req}$.
- Decrease spectral noise density N_0 or the noise figure N_F.
- Decrease data rate R.

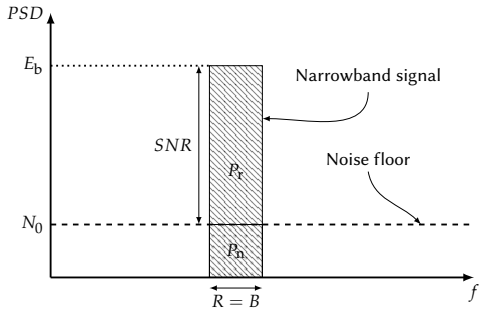
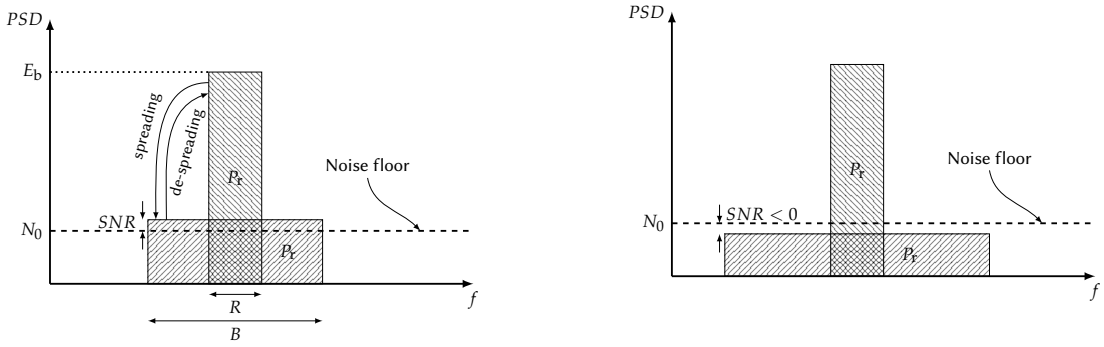


FIGURE 1.3 – *PSD for narrowband transmission, minimizing the noise power P_n through maximum spectral efficiency $\eta = 1$.*



(a) *Signal above noise floor N_0.* (b) *Signal below noise floor N_0.*

FIGURE 1.4 – *PSD for spread spectrum modulation, lowering spectral efficiency η.*

Designing transmission techniques that achieve specified error levels at a lower bit energy to noise spectral power ratio allows optimizing receiver sensitivity [Rot17]. However, due to the fundamental limits of channel capacity introduced by Claude Shannon [Sha48], bit energy to noise spectral power ratio cannot be arbitrary lowered as the theoretical limit lies at $(E_b/N_0)^{dB}_{lim} = -1.59\,dB$. Lowering spectral noise density N_0 or the noise figure N_F requires optimizing the receiver hardware or decreasing the ambient temperature of the receiver, which is impractical in LPWA scenarios. Remaining the possibility to attain arbitrary low levels of receiver sensitivity by sufficiently decreasing data rate R.

Two approaches, both resulting in low levels of receiver sensitivity by lowering data rate are possible. Narrowband transmission techniques on the one hand and low spectral efficiency approaches on the other are equivalent concerning receiver sensitivity, however each offers different advantages and inconveniences [Las14; Sem15].

1.2.1.2 Narrowband Transmission

Firstly, applying narrowband transmission techniques lowers the amount of captured ambient thermal noise and hence reduces the required minimum received power as depicted in Figure 1.3. In consequence, signals are well localized in frequency domain. This suffers the inconvenience that very accurate and stable oscillators are needed as small carrier frequency offsets induce the loss of the signal. Furthermore, in-band interference may equally lead to a missed reception.

1.2.1.3 Low Spectral Efficiency Transmission

Secondly, spectral efficiency η can be reduced while keeping a convenient bandwidth. The simplest approach to lowering spectral efficiency is the repetition of the message to transmit. Techniques that are more complex apply direct sequence spreading codes, frequency hopping or chirped waveforms [Pro01], resulting in a spectrum as depicted in Figure 1.4. In all low spectral efficiency methods, the signal duration is increased, as it is the case also with narrowband transmissions.

For further reading focusing on the aspects of optimized and flexible physical layers for LPWA refer to [Rot17].

1.2.2 Existing Technologies

In the following, a short overview on existing LPWA radio technologies is given. The principles of the physical layer, Medium Access Control (MAC) protocol specificities and available eco-systems are presented for each technology.

Sigfox and LoRa technologies are proprietary LPWA technologies operating in the license free Short-Range Device (SRD) bands of the radio spectrum, whereas Narrow-Band IoT (NB-IoT) is part of the Long Term Evolution (LTE) standard and hence using the assigned frequency bands.

1.2.2.1 Sigfox

Sigfox is a network service provider for long-range low-power communication dedicated to IoT applications [Sig]. Sigfox mainly deploys the network infrastructure including base stations and servers, and offers the services for operating connected devices over the network. Different Sigfox network compatible radio modules from various chip manufacturers [STM16; Tex16] as well as research prototype transceivers [Lac+17] exist.

The proprietary Sigfox physical layer achieves low levels of receiver sensitivity through the approach of narrowband and Ultra-Narrow Band (UNB) radio signals. Differential Binary Phase Shift Keying (DBPSK) and Frequency Shift Keying (FSK) modulation schemes with bit rates between 100 bps and 600 bps are employed.

In general, a Phase Shift Keying (PSK) modulator maps m bits to the alphabet of $M = 2^m$ symbols $\left\{\xi^0, \ldots, \xi^{M-1}\right\}$. Before symbol shaping, the transmit waveform for the modulated symbol set $\{\xi_0, \ldots, \xi_{K-1}\}$ is given by

$$s_{\mathrm{PSK}}(t) = \sum_{k=0}^{K-1} \xi_k \, s_{\mathrm{pulse}}\left(t - kT_{\mathrm{S}}\right), \tag{1.11}$$

with pulse shape s_{pulse}. Table 1.1 lists the receiver sensitivity for Sigfox compliant communication.

For the purpose of synchronization, a preamble of 4 bytes and a Start of Frame Delimiter (SFD) of 2 bytes are transmitted. Payload lengths up to 12 bytes are supported. For bit error detection, a Cyclic Redundancy Check (CRC) is employed. Together with the data fields for device identification and authentication a packet has the total length of 26 bytes. Furthermore, a packet is repeated on three different carrier frequencies to ensure correct reception through frequency diversity. Frequencies for the repetitions are predefined and known to the wireless node and the base station. As a result, the total time-on-air for a Sigfox compatible packet with a maximum payload length and a 100 bps bit rate without the three repetitions is

$$T_{\mathrm{air}} = 26 \cdot 8 \cdot T_{\mathrm{b}} = 2.08\,\mathrm{s}. \tag{1.12}$$

Due to the duty cycle limitations imposed on the license free SRD bands [CEP18] (typically 1% for the SRD 868 MHz band), communication is limited to 140 packets per day.

Another issue with UNB communication is Carrier Frequency Offset (CFO). Considering a 100 Hz bit rate Binary Phase Shift Keying (BPSK) transmission, a relative frequency offset of 1 ppm equal to 868 Hz at 868 MHz carrier frequency results in the signal being out of the receiver filter. This difficulty is addressed on the protocol level as explained in the following.

The Sigfox proprietary communication mainly addresses asymmetric network topologies with low capacity wireless nodes and less restricted base stations. In order to combat CFO, the wireless node always initiates transmissions. Access to the radio spectrum is granted through a random, Additive Links On-line Hawaii Area (ALOHA)-like access technique [Sig; Abr70]. Base stations are continuously scanning the whole frequency band and are capable of receiving wireless packets possibly shifted in frequency due to CFO. If a downlink message (acknowledge or other) is required, the base station responds after a predefined period following the uplink communication when the node opens a reception window. In order to ensure that the downlink packet is within the receive filter of the wireless node, the base station sends its message at the beforehand estimated uplink carrier frequency, which is possibly different from the nominal defined channel frequency. Due to the long transmission duration in the order of seconds, CFO time variations are still critical. Typical low-cost oscillators may exhibit frequency drifts of 50 Hz/s, which is equal to $\approx$ 50 ppb (see Chapter 2.2.1). Consequently, half of the downlink transmission lies outside the receiver filter. In order to be robust against CFO variations and to keep complexity of the receiver architecture at a minimum, three receiver paths search for the downlink message in parallel. One receiver is tuned to the uplink frequency and two to an offset of $\pm$50 Hz, allowing a decision on the best match [Lac+17]. Requiring always an uplink message to initiate the communication is certainly a restriction to certain applications, however this avoids the node to listen periodically for downlink messages by opening a reception window. Hence, the reception part of the node can remain in a low-power consumption sleep mode unless a downlink acknowledge after an uplink message is desired.

1.2.2.2 LoRa

The proprietary LoRa (Long-Range) communication technology has been developed and patented [Sel16] by Cycleo, which has been taken over by Semtech. The latter is commercializing multiple versions of the radio modem chip, including node and base station architectures [Sem16; Sem17b]. LoRa based services are offered by various providers.

Semtech offers radio chips in both, the SRD 868 MHz band [Sem16] as well as for the ISM 2.4 GHz band [Sem17b]. While the principles of the physical layer apply to both, available parametrization differs and hence attainable receiver sensitivity. The SRD 868 MHz band version offers long-range due to low bandwidths whereas the 2.4 GHz chip offers a ranging function and higher data rates at the trade-off of degraded sensitivity. The following description of the physical layer applies to both versions and the MAC is explained based on the historical, already widely spread SRD 868 MHz band version. Relevant details for the 2.4 GHz chip are reviewed in the context of localization in Chapter 1.6.1.2 and Chapter 4.3.1.3.

In contrast to the Sigfox technology, LoRa attains low levels of receiver sensitivity through low spectral efficiency modulation techniques. The waveform is based on the so-called Zadoff-Chu (ZC) sequences [FZH62; Chu72], mapping m bits to the alphabet of $M = 2^m$ symbols $\left\{\xi^0, \ldots, \xi^{M-1}\right\}$, where symbol time T_S and signal bandwidth B are linked by

$$T_S = \frac{2^m}{B} = \frac{M}{B}. \tag{1.13}$$

Bit rate of the m bit symbol is given by

$$R = \frac{m}{T_S} = B\frac{m}{2^m}, \tag{1.14}$$

resulting in the spectral efficiency

$$\eta = \frac{R}{B} = \frac{m}{2^m}. \tag{1.15}$$

The transmit waveform for the symbol set $\{\xi_0, \ldots, \xi_{K-1}\}$, is given by

$$s_{\text{LoRa}}(t) = \sum_{k=0}^{K-1} e^{j2\pi\left(f_{\xi_k}(t-kT_S)\right)\cdot(t-kT_S)}. \tag{1.16}$$

The symbol ξ^i of the alphabet has a up-chirped waveform with an instantaneous frequency linearly varying in the interval $[-B/2, B/2]$

$$f_{\xi^i}(t) = -\frac{B}{2} + B\left(\frac{t}{T_S} - \frac{i}{M}\right) + \begin{cases} B, & t \in \left[0, \frac{i}{M}T_S\right) \\ 0, & t \in \left[\frac{i}{M}T_S, T_S\right) \end{cases}. \tag{1.17}$$

Every symbol has also a complementary down-chirped waveform with instantaneous frequency $f'_{\xi^i}(t) = -f_{\xi^i}(t)$.

Demodulation starts by "de-chirping" the received signal, sampled at Nyquist frequency, with the complementary basis chirp ξ^0. After "de-chirping", a signal of constant frequency is obtained

$$f_i = f_{\xi^i}(t) + f'_{\xi^0}(t) = -B\frac{i}{M} + \begin{cases} 0, & i \in \left[0, \frac{M}{2}\right] \\ B, & i \in \left[\frac{M}{2}+1, M-1\right] \end{cases}. \tag{1.18}$$

Performing a Fast Fourier Transform (FFT) on the constant frequency signal results in a peak at frequency f_i, from which the symbol data can be extracted.

The physical layer is highly flexible and scalable due to this modulation technique, allowing to choose between the two extremes of high data rate and low levels of receiver sensitivity, which is listed in Table 1.1.

For bit error detection, a CRC and for bit error correction, Forward Error Correction (FEC) techniques are utilized. Time synchronization is achieved by transmitting a preamble of predefined chirps that are used to align the symbol frames at the receiving side accordingly. A 125 kHz bandwidth, a low spectral efficiency with $m = 12$ and a coding rate of 4/5 result in the packet duration $T_{\text{air}} = 925.7$ ms for a 6 symbol preamble and a payload of 12 bytes [Sem16].

CFO is less critical due to wider bandwidths compared to UNB communication. For the LoRa physical layer, CFO results in the whole chirp sequence being shifted in frequency domain on the transmitter side. As on the receiver side, baseband signals are sampled at Nyquist frequency, spectral aliasing occurs. Consequently, CFO shifted chirps appear as time delayed chirps. As a result, time and frequency synchronization are performed jointly and inherently when synchronizing to a preamble. This type of frequency estimation is limited by the receive filter bandwidth, which is designed as trade-off between tolerating CFO shifted signals and blocking out-of-band signals.

Another property of ZC sequences is their orthogonality for different alphabet lengths M [Chu72]. This allows sharing the same radio spectrum resource (in time and frequency) for simultaneous transmissions, where users can be separated through alphabets of different length.

Due to the flexibility of the physical layer and the inherent robustness against CFO, symmetric communication is possible. This gives rise to classical star topologies with multiple wireless nodes connected to a base station, mesh networks with inter-node communication and mixtures of both approaches to optimize network throughput, coverage and battery lifetime [OSMD18].

While the LoRa technology offers the possibility to develop application specific custom MAC protocols, an industrial consortium, called LoRa Alliance [LoR18], drives standardization for the interoperability of devices. This Long-Range Wide Area Network (LoRaWAN) standard is designed for bi-directional star topologies and addresses different data rates, security and applications by dividing nodes into three classes (A, B, C), ranging from lowest power to lowest latency [LoR18]. Uplink messages are send in an ALOHA-type spectrum access while downlink is possible in defined reception windows after the uplink message (class A). Periodic, beacon aligned downlink reception windows (class B) or continuous half-duplex reception (class C) allows reducing base station to node latency at the expense of power consumption. The throughput and scalability of LoRaWAN-based LPWA networks is studied in [GR17].

Multiple mobile communication providers offer LPWA services based on LoRa technology and LoRaWAN [Obj; Act]. In parallel, the open source project *The Things Network* [The], allows joining the public LoRaWAN network with both nodes and by deploying base stations.

1.2.2.3 Narrow-Band IoT

The LTE standard developed by the 3rd Generation Partnership Project (3GPP) working group and commonly referred to as Fourth Generation (4G) of mobile communication aims to provide higher performance to the user. Since the Release 12 (2015), besides improving performance, the standard also provides low data rate, low-complexity and low-power operation modes [3GP15]. These standard compliant modes lead to the Machine to Machine (M2M) communication solutions called NB-IoT, Extended Coverage GSM (EC-GSM) and enhanced Machine Type Communication (eMTC) in the Release 13 [3GP16].

In the NB-IoT standard, the downlink uses one LTE resource block with a frame duration of 10 ms and a 180 kHz bandwidth. This Orthogonal Frequency Division Multiple Access (OFDMA) resource block is split into 12 subcarriers with a 15 kHz spacing. In uplink, multi-tone Single Carrier FDMA (SC-FDMA) and single tone modulations are used. Sensitivity can be improved by lowering spectral efficiency through repeating the preamble up to 128 times (see Table 1.1). Transmit power is limited to 20 dBm and 23 dBm to reduce power consumption.

In downlink, OFDMA is used for flexible time/frequency resource allocation. The uplink employs SC-FDMA to relax the time and frequency synchronization of different users and to limit the Peak to Average Power Ratio (PAPR) in order to relax Power Amplifier (PA) requirements.

As NB-IoT is part of the LTE standard, transmissions are part of the cellular network. Users of the NB-IoT standard hence need to subscribe to a telecommunications service provider to use the NB-IoT connectivity in the licensed frequency spectrum.

1.2.2.4 IEEE 802.15.4k

The Institute of Electrical and Electronics Engineers (IEEE) provides the IEEE 802.15.4k as LPWA specific amendment to the IEEE 802.15.4 standard, offering extended coverage through lower levels of receiver sensitivity [IEE13].

The standard specifies both Direct Sequence Spread Spectrum (DSSS) and FSK physical layers, whereby the DSSS specification provides a link budget up to 145 dBm compared to 94 dBm for FSK.

The DSSS physical layer defines a preamble with up to 4 bytes, a SFD and a payload of maximum 32 bytes. Error correction is achieved by FEC techniques. The bits are spread with a Gold code of length $2^{4\ldots15} = 16\ldots32768$ and then BPSK or Quadrature Phase Shift Keying (QPSK) modulated with chip rates between 200 kchip/s and 1000 kchip/s. The minimum transmit power is fixed at -3 dBm, leading to the minimum link budget of 145 dB with a receiver sensitivity of -148 dBm at a bit rate of 6 bit/s, corresponding to minimum chip rate and maximum spreading code length for maximum coverage.

The IEEE 802.15.4k is mainly designed for a star network topology. Synchronous and asynchronous operation as well as a beacon-enabled mode are defined.

	Modulation	R	B	η	P_{req}	$(P_{\text{t}})_{\text{max}}$	L	**Band**	**MAC**
Unit	n/a	$bits{\cdot}s^{-1}$	Hz	$bits{\cdot}s^{-1}{\cdot}Hz^{-1}$	dBm	dBm	dB	MHz	n/a
Sigfox [Sig]	DBPSK	100	100	1	−144	20	158	SRD 868	▪ Star ▪ ALOHA ▪ max. payload 12 bytes ▪ UL: 140 packets per day ▪ DL: 4 packets per day
Lora 868 [Sem16]	CSS	183	125000	$1.5 \cdot 10^{-3}$	−147	14	161	SRD 868	▪ Star/Mesh ▪ ALOHA ▪ Full bi-directional ▪ DL: window, beacon, continuous
Lora 2400 [Sem17b]	CSS	595	203000	$2.9 \cdot 10^{-3}$	−141	14	156	SRD 2400	▪ Star/Mesh ▪ ALOHA ▪ Full bi-directional
NB-IoT DL [3GP16]	QPSK	234	180000	$1.3 \cdot 10^{-3}$	−146	23	170	Licensed	▪ Star ▪ SC-FDMA/OFDMA
NB-IoT UL [3GP16]	BPSK	9	3700	$2.4 \cdot 10^{-3}$	−163	23	187	Licensed	▪ Star ▪ SC-FDMA/OFDMA
Ingenu-RPMA [Ing]	DSSS	61	1000000	$6.1 \cdot 10^{-5}$	−150	20	170	ISM 2400	▪ Star/Tree ▪ CDMA, slotted
Weightless-N [Wei]	DBPSK	30	200	0.15	−150	20	170	SRD 868	▪ Star ▪ ALOHA
IEEE 802.11.4k [IEE13]	DSSS	6	200000	$3 \cdot 10^{-5}$	−160	-3	157	SRD 868, 2400	▪ Star ▪ ALOHA

TABLE 1.1 – *LPWA technologies with key system and performance parameters for maximized communication range.*

1.2.2.5 Overview on LPWA Technologies and Standards

Besides the most prominent LPWA technologies and standards (LoRa, Sigfox, NB-IoT, IEEE 802.15.4k) several others such as [Ing; Wei] exist. Table 1.1 gives a non-exhaustive lists on LPWA technologies with key system and performance parameters. Receiver sensitivity is calculated from (1.9), neglecting the noise figure N_{F} and taking $(E_{\text{b}}/N_0)^{\text{dB}}_{\text{req}}$ from [Rot17].

1.3 Terminology for Localization

Localization describes the process of determining the place or position of an object or subject (see Table 1.2). A position is always relative with respect to a reference system. Defining the position on the earth can be done

lo·ca·tion [ləʊˈkeɪʃən] a particular place, especially in relation to other areas, buildings etc.
lo·cate [ləʊˈkeɪt] to find the exact position of something
lo·cal·iza·tion [ləʊkəlaɪˈzeɪʃən] process of determining the location of a device
po·si·tion [pəˈzɪʃən] the place where someone or something is, especially in relation to other objects and places
po·si·tion [pəˈzɪʃənɪŋ] process of a device, determining its position

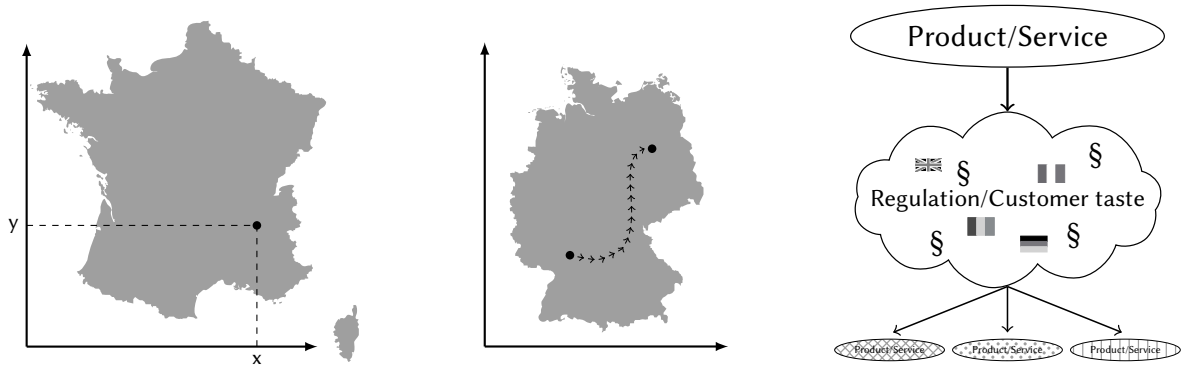
TABLE 1.2 – *Word definitions for Localization from [Lon19].*

through the coordinates latitude, longitude and altitude above sea level, compared to localization within a building, where floor and room numbers allow unambiguous localization. Hence, positioning and geo-referencing describe the process of obtaining the location or position. These terms are used interchangeable throughout this thesis.

However, sometimes a distinction is made between positioning and localization. Whereby positioning describes the process of determining the position of oneself, i.e. a device estimates its own position. Localization is this context entitles the location estimation of a device by the reference system, i.e. the infrastructure.

In technical language, localization has also the meaning of adapting and customizing a product or service to suite specific requirements for certain locations/regions such as regulation or customer taste. Unless otherwise stated, this definition of the word localization is not used in the scope of this thesis.

Navigation is the process of guiding a user or object towards a target, possibly on a predefined route. This is achieved by continuously iterating over the steps of first localizing and secondly providing instructions to follow a



(a) *Positioning/Geolocalization.* (b) *Navigation.* (c) *Regional product/service adaptation.*

FIGURE 1.5 – *Terminology for localization.*

route or to attain the target. Therefore localization is required for navigation and the type, quality and constraints of localization are linked to those of navigation. Figure 1.5 illustrates the different word definitions.

1.4 Radio Localization Performance Indicators

Localization performance indicators are used to qualitatively and quantitatively compare different positioning techniques and to judge on their suitability for a given scenario and application. The main indicators are accuracy and precision, availability, complexity and the protocol to acquire the necessary measurements as well as power consumption. These indicators will be introduced in the following and used throughout the thesis to compare the investigated localization methods and techniques from the state of the art.

1.4.1 Accuracy and Precision

Providing the location of a user or an object is the result of an estimation process. In general, estimation is based on the observation of a measurable quantity and a system model, which describes the link between this quantity and the wanted final quantity. For example, an electronic temperature sensor provides a voltage varying with temperature. A dedicated model is used to translate voltage to temperature, possibly integrating former temperature estimates and the fact that temperature changes follow a certain dynamic, which *e.g.* excludes arbitrary abrupt variations. The estimated value $\hat{x}$ possibly differs from the real value x, due to measurement noise and imperfections in the observation process.

In order to characterize and quantify the error on a set of K estimated values $\{\hat{x}_0 \dots \hat{x}_{K-1}\}$ for the set of real values $\{x_0 \dots x_{K-1}\}$ the following error metrics are used

Error	ϵ_k		$= \hat{x}_k - x_k,$	(1.19a)
Mean error/Bias (*Accuracy*)	$\mu_\epsilon = \mathbb{E}_1\{\epsilon_k\}$		$\approx \frac{1}{K}\sum_{k=0}^{K-1} \epsilon_k,$	(1.19b)
Variance (*Precision*)	$\sigma_\epsilon^2 = \mathbb{E}_1\left\{(\epsilon_k - \mu_\epsilon)^2\right\}$	$= \mathbb{E}_1\left\{\epsilon_k^2\right\} - \mathbb{E}_1^2\{\epsilon_k\} = \mathbb{E}_1\left\{\epsilon_k^2\right\} - \mu_\epsilon^2$	$\approx \frac{1}{K}\sum_{k=0}^{K-1} (\epsilon_k - \mu_\epsilon)^2,$	(1.19c)
RMS error	$\epsilon_{\text{RMS}} = \sqrt{\mathbb{E}_1\left\{\epsilon_k^2\right\}}$	$= \sqrt{\sigma_\epsilon^2 + \mu_\epsilon^2}$	$\approx \sqrt{\frac{1}{K}\sum_{k=0}^{K-1} \epsilon_k^2}.$	(1.19d)

Precision *Accuracy*

Estimation theory [VT04] provides different approaches to formulate the estimation problem and the observation model, which will be introduced in Chapter 3.2. All methods aim at extracting the maximum information from the available observations to obtain the most accurate and precise estimate possible. Accuracy and precision of estimation with respect to the real value are depicted in Figure 1.6. Accuracy takes into account biases, such as offsets and systematic errors, while precision is a measure for the statistical spread around the estimation mean.

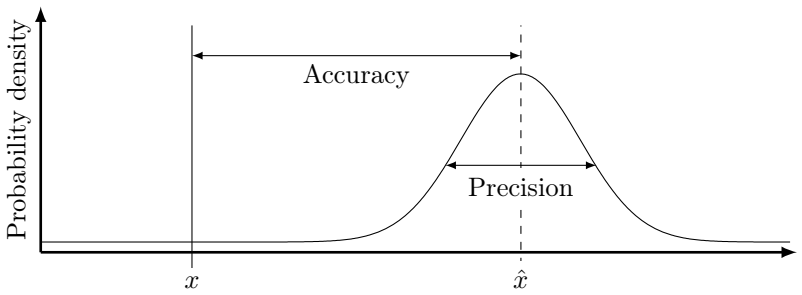


FIGURE 1.6 – *Accuracy and precision of an estimate $\hat{x}$ with respect to the real value x.*

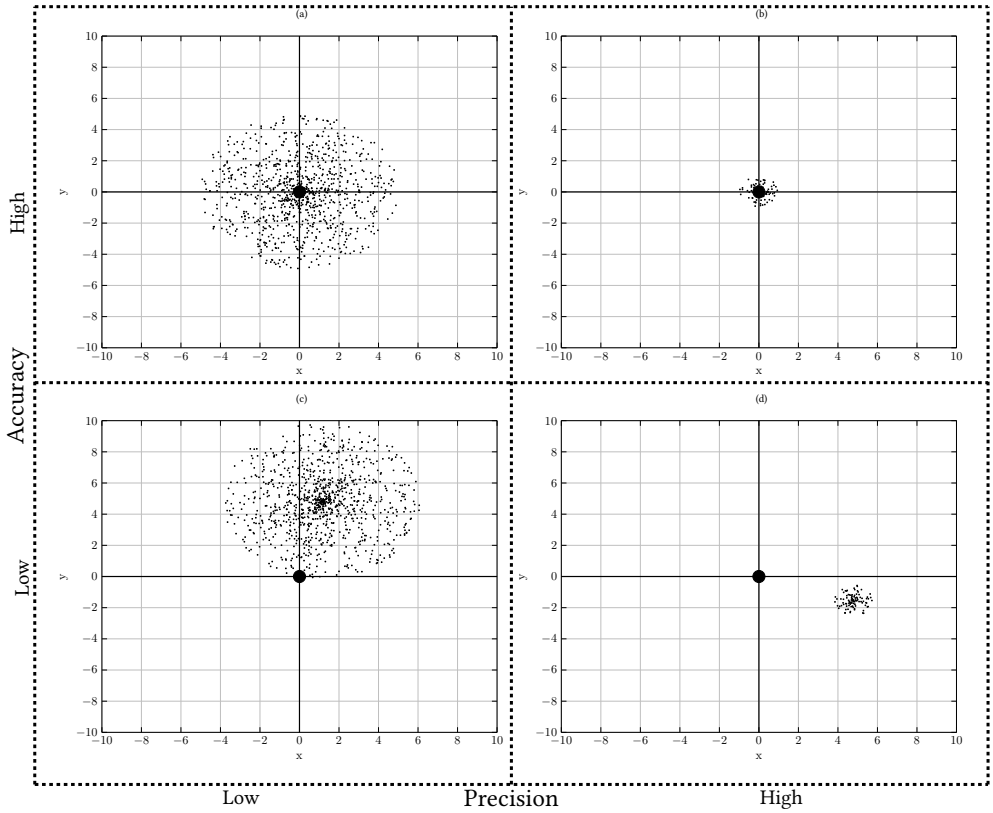


FIGURE 1.7 – *Accuracy and precision on the example of position estimation with real position at (0,0) and estimated positions (small black dots).*

Figure 1.7 illustrates combinations of the extremes of accuracy and precision on the example of position estimation.

Estimation theory further provides tools to determine the absolute theoretical lower bound on precision, given an observation as well as indications to the existence of an estimator capable of attaining the bound [Kay93]. Among those tools are the so-called Cramer Rao Lower Bound (CRLB) and Ziv Zakai Lower Bound (ZZLB) which will be introduced in Chapter 3.3. Applied to the field of signal processing and more specifically to radio signal based localization, these tools indicate the potential of a chosen localization technique from a theoretical perspective (see Chapter 1.5.3 and Chapter 3.3).

1.4.2 Availability and Refresh Rate

Performing observations of measurable quantities and applying dedicated signal processing schemes based on adequate models results in an estimate of the user or object position. Availability and refresh rate of position estimates depends on the availability and frequency with which observations can be performed and the required processing time.

While for certain applications a position update every hour is sufficient, others require sub-second refresh rates.

For packet tracking, an hourly estimate is satisfying to determine if an expected parcel is in the post office or still in the depot. However, navigation applications such as those based on Global Navigation Satellite System (GNSS) require regular location updates for continuous real-time navigation instructions.

Further, the more location estimations per time and real position are available, the better methods exploiting the statistics of these estimates can be applied. If several estimates for one real position are available, techniques such as averaging or outlier detection and elimination can be applied. This is however hardly feasible in mobile LPWA applications with radio signal based localization techniques. Periods during which the mobile node remains stationary are probably shorter than the intervals between transmissions, which are bound by power consumption and duty cycle requirements (see Chapter 1.4.5 and Chapter 2.1.5).

1.4.3 Complexity and Cost

Besides the indicators for the quality of the actual estimated location information, complexity and cost can equally be used as criteria for comparing different positioning techniques.

Complexity can be split into deployment and hardware complexity on one side and computational complexity on the other side. Localization techniques can differ in the deployment of a required infrastructure *e.g.* anchors, georeferenced points or the creation of maps (see Chapter 1.5.1.4). Complexity on the side of the user or object to localize can be described by the hardware that needs to be added in order to enable localization functionality. To illustrate deployment and hardware complexity, the example of forest fire detection (Chapter 1.1) is considered. Integrating a GNSS module to each wireless temperature sensor node adds more hardware to the device, possibly increasing its energy consumption. However, from an application point of view, deployment complexity remains low, as GNSS satellites acting as reference anchors are available and not part of the user specific deployment problem. From a global system perspective however, GNSS deployment is very complex considering the satellite and the control segement (see Chapter 1.6.1.5).

LPWA radio signal based localization methods can possibly avoid additional hardware on wireless nodes. Base stations need to be capable to perform metric extraction for position estimation (see Chapter 1.5.2). Depending on the hardware compatibility of existing base stations, these can be enhanced with positioning features by straightforward firmware updates.

Depending on the localization technique, computational complexity can vary a lot, ranging from the simple estimation of the received signal power (see Chapter 1.5.2.6) to solving complex integer-ambiguity functions, i.e. in Real-Time Kinematic GPS (RTK-GPS) (see Chapter 1.5.2.8).

Another important, although more commercial, factor is the necessary initial investment and continuous costs of a positioning system. Launching space vehicles to bring GNSS satellites into orbit is a huge investment and operating the GNSS control segment produces continuous cost while adding a positioning enabled LPWA base station to an existing radio telecommunication mast is a manageable effort.

1.4.4 Protocol Requirements

Positioning techniques can also be compared under the angle of protocol requirements. In the wider sense, this includes the necessary steps to obtain the observations that then serve to estimate position. For example position can be estimated by comparing the current observation to a beforehand acquired map, *e.g.* fingerprinting (see Chapter 1.5.1.4) and interfering position from similarity to a specific point. Therefore, a map must be generated and kept up to date for this purpose. Other methods rely on calibration measurements or differential measurement methods *e.g.* RTK-GPS to eliminate unknown offsets.

More specifically for radio signal based localization, the number and type of required packet exchanges is of interest. Operating in uplink or downlink, synchronized or asynchronous mode, in star or mesh networks will affect channel occupation and power consumption. Intelligently splitting transmission time between localization estimation and data transfer [Gha+18] or mutualizing both in RADAR-communication [Sit17], are approaches to enable massive access required for IoT and to be regulation compliant.

1.4.5 Power Consumption

Power consumption is a critical design parameter for LPWA radio technologies and applications depending on LPWA connectivity. Main reason for this constraint is the requirement for autonomous battery powered operation over several years without space for large batteries, the cost for regular battery replacements or the impracticality for replacement, *e.g.* for sealed devices.

LPWA radio chipsets and protocols are constantly optimized to consume less power. Likewise, a localization function has to meet the demands for low-power consumption. GNSS based positioning requires additional

hardware which increases the power consumption considerably as GNSS chips consume more power than LPWA chips (see Table 1.3).

	Sleep in µW	**Idle in** µW	**Transmission in** mW		**Reception in** mW
Sigfox					
Foxy [Lac+17]	0.50	1.50	10.0 dBm	79.20	14.52
Si4461 [Sil16]	0.20	5.90	14.0 dBm	122.10	45.21
S2_LP [STM16]	3.00	1050.00	14.0 dBm	57.00	2.40
CC1125 [Tex16]	3.00	3900.00	14.0 dBm	141.00	78.00
LoRa					
SX1276 [Sem16]	3.30	5940.00	14.0 dBm	92.40	39.60
			20.0 dBm	396.00	
SX1280 [Sem17b]	5.90	3960.00	12.5 dBm	79.20	27.06
GNSS					
NEO-M8P [Ubl]				n/a	typ.: 105.00 peak: 201.00

TABLE 1.3 – *Typical power consumption for LPWA and GNSS chip sets.*

LPWA radio signal based localization potentially offers the opportunity to add positioning without additional power consumption, as radio signals are simultaneously used for both, data transfer and localization.

The number of packet exchanges and computational complexity and hence power consumption may vary depending on the application specific refresh rate, the localization technique (see Chapter 1.5) and the underlying ranging metrics (see Chapter 1.5.2).

Besides power consumption on the (battery autonomous) node to be localized, power consumption on the infrastructure, including base stations and servers, needs to be considered, especially in a holistic approach and from an eco-conception perspective.

1.5 Localization Techniques

In this section, fundamental localization principles and models are explained. Following this description of how observations are linked to position, an overview on localization metrics extractable from observation is given in Chapter 1.5.2. The quality of extracted metrics as well as the localization scenario itself influences the quality of the estimated position. This fundamental dependency is studied in Chapter 1.5.3 and provides a methodology for comparing localization performance, especially accuracy and precision. Finally, existing LPWA localization solutions, including their strengths and weaknesses are presented in Chapter 1.6.1 as well as a review on techniques possibly providing higher accuracy and precision for LPWA positioning is given in Chapter 1.6.2.

1.5.1 Fundamental Localization Principles

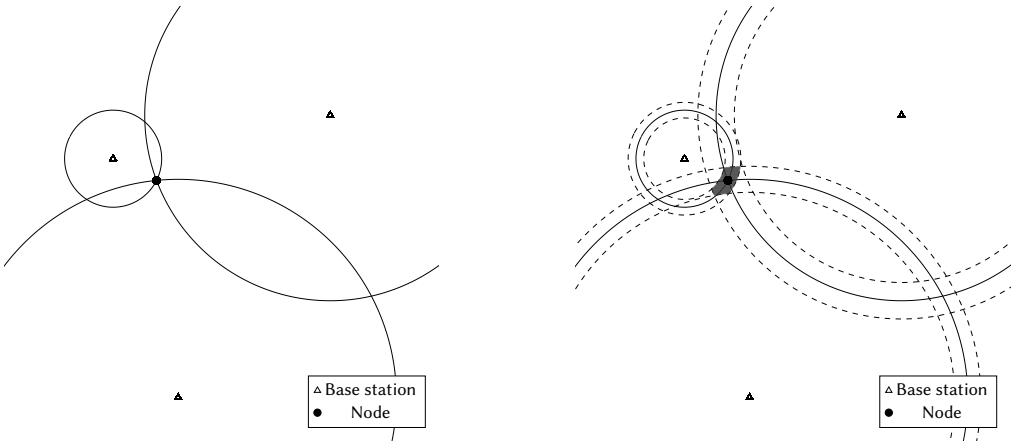
Localization can be performed in two or three dimensions in space. While airplane localization relies on three-dimensional positioning, localizing for ships can be restricted to two dimensions. Principles are introduced with the general case of three-dimensional localization, while examples are given for the two-dimensional case in order to simplify the presentation. In the present work, the hypothesis is made, that LPWA localization focuses on two-dimensional localization because most applications are ground based and hence require only horizontal location information. However, in mountainous regions, three-dimensional localization might be necessary in order to obtain correct three-dimensional location estimates.

1.5.1.1 Trilateration

Circular

A classical approach to determine position is based on measuring the distance to reference points, anchors, of known location. Each distance measurement allows drawing a sphere around the corresponding anchor with radius equal to the measured distance. A minimum of four anchors is needed theoretically, so that there is only one unique intersection point, which corresponds to the position to be determined.

Figure 1.8a visualizes the localization scenario for the two-dimensional case, where spheres reduce to circles and a minimum of three anchors is needed for unique intersection.



(a) *Perfect range estimation.* (b) *With range estimation errors.*

FIGURE 1.8 – *Circular trilateration in two dimensions.*

In order to formalize the general three dimensional case, K_{BS} anchors at position (x_i,y_i,z_i) are considered. For mathematical traceability and without loss of generality, the coordinate systems origin is chosen to be at anchor 0 $(x_0,y_0,z_0) = (0,0,0)$. The node whose position (x_u,y_u,z_u) is to be determined and the anchors/base stations are depicted in Figure 1.8a. The known distances $d_{i,0}$ from anchor i to anchor 0 can be expressed (in three dimensions) by

$$d_{i,0} = \sqrt{x_i^2 + y_i^2 + z_i^2}. \tag{1.20}$$

Equally the measured or estimated distances $d_{u,i}$ from node u to anchor i are given by

$$d_{u,i} = \sqrt{(x_u - x_i)^2 + (y_u - y_i)^2 + (z_u - z_i)^2}. \tag{1.21}$$

After reformulation, the following equation relates anchor positions, known and estimated distances to the unknown node position

$$-2(x_u x_i + y_u y_i + z_u z_i) = d_{u,i}^2 - d_{u,0}^2 - d_{i,0}^2. \tag{1.22}$$

For an unique solution, four distance estimations are required leading to the set of three equations in matrix form

$$-2\begin{pmatrix} x_1 & y_1 & z_1 \\ & \vdots & \\ x_i & y_i & z_i \\ & \vdots & \\ x_{K_{\mathrm{BS}}-1} & y_{K_{\mathrm{BS}}-1} & z_{K_{\mathrm{BS}}-1} \end{pmatrix}\begin{pmatrix} x_u \\ y_u \\ z_u \end{pmatrix} = \begin{pmatrix} d_{u,1}^2 - d_{u,0}^2 - d_{1,0}^2 \\ \vdots \\ d_{u,i}^2 - d_{u,0}^2 - d_{i,0}^2 \\ \vdots \\ d_{u,K_{\mathrm{BS}}-1}^2 - d_{u,0}^2 - d_{K_{\mathrm{BS}}-1,0}^2 \end{pmatrix}, \tag{1.23}$$

or in short form

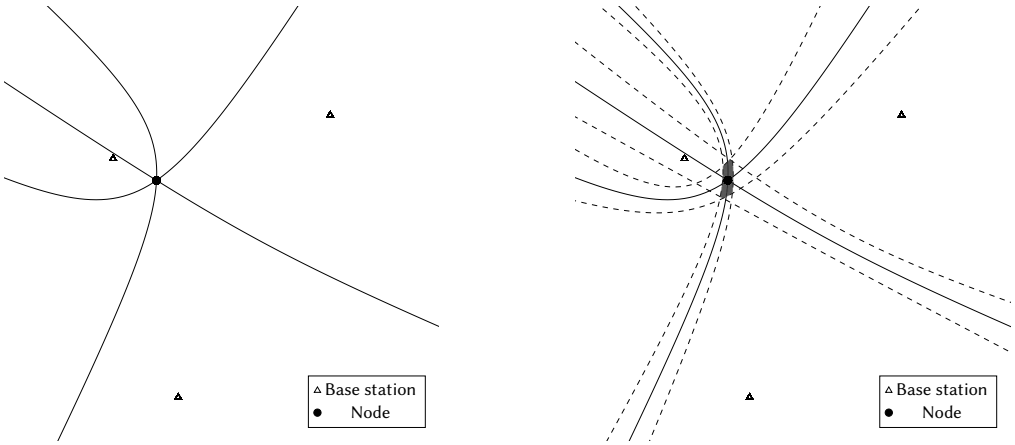
$$-2\boldsymbol{X}\boldsymbol{x}_u = \boldsymbol{d}, \tag{1.24}$$

where $\boldsymbol{X}$ holds all the information about the anchor placement, $\boldsymbol{d}$ the estimated ranges and $\boldsymbol{x}_u = [x_u\, y_u\, z_u]^T$ is the coordinate vector of the node whose position is to be determined.

This linear equation can be solved *e.g.* with a linear least squares approach given in Chapter 1.5.4

$$\boldsymbol{x} = -\frac{1}{2}\left(\boldsymbol{X}^T\boldsymbol{X}\right)^{-1}\boldsymbol{X}^T\boldsymbol{d}. \tag{1.25}$$

Considering estimation errors on the measured distances results in a localization error as depicted in Figure 1.8b. The theoretical positioning precision bounds for given anchor deployment and range estimation errors are studied in Chapter 1.5.3.



(a) *Perfect range difference estimation.* (b) *With range difference estimation errors.*

FIGURE 1.9 – *Hyperbolic trilateration in two dimensions.*

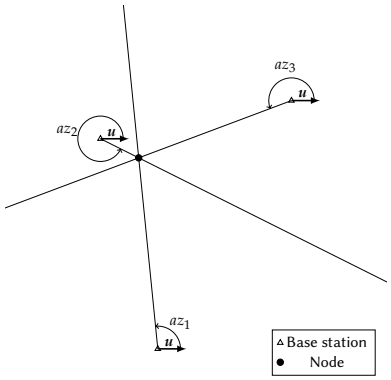


FIGURE 1.10 – *Triangulation in two dimensions.*

Hyperbolic

In certain cases, node to anchor distance is not accessible but only the difference of distance of the node to two anchors is observable. An illustrative example is the underwater localization of whales that are communicating with peers via acoustic signals [Sim+06]. Detecting the difference of arrival of these acoustic signals at multiple synchronized anchors and knowing the acoustic propagation speed in water allows measuring the difference in distance between a whale and two anchors. As a result, possible positions in two dimensions lie on a hyperbole as depicted in Figure 1.9. Again, similar to circular trilateration, the intersection of sufficient hyperboloids (in three dimensions) gives a unique estimated position.

The measurable distance differences of a node with unknown position (x_u,y_u,z_u) at the anchor i of position (x_i,y_i,z_i) and the anchor k of position (x_k,y_k,z_k) are expressed as

$$\Delta d_{u,i,k} = \sqrt{(x_u - x_i)^2 + (y_u - y_i)^2 + (z_u - z_i)^2} - \sqrt{(x_u - x_k)^2 + (y_u - y_k)^2 + (z_u - z_k)^2}. \tag{1.26}$$

This set of equations is non-linear and a least squares closed-form solution is given by [SA87]. Location solving algorithms are outlined in Chapter 1.5.4.

1.5.1.2 Triangulation

Instead of measuring distances to reference points, triangulation is based on estimating position by measured angles between the node and the anchors with respect to a reference direction. Historically, maritime navigation has relied on this type of position estimation with the help of a sextant to measure angles [Enc]. Figure 1.10 illustrates the basic scenario for angular based positioning. For three-dimensional localization, azimuth and polar angles are defined with respect to the x-axis and the z-axis respectively.

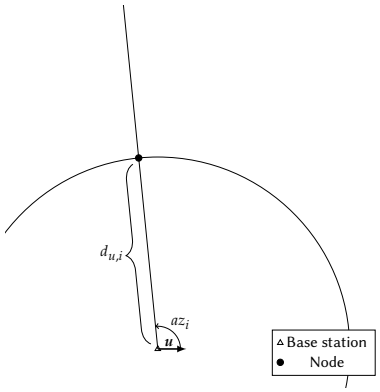


FIGURE 1.11 – *Hybrid localization: Ranging as well as azimuth angle in two dimensions.*

Measurable azimuth az_i and polar pol_i angles are linked to node (x_u,y_u,z_u) and anchor i (x_i,y_i,z_i) coordinates by

$$\text{Azimuth} \qquad \tan(az_i) = \frac{y_u - y_i}{x_u - x_i}, \tag{1.27a}$$

$$\text{Polar} \qquad \cos(pol_i) = \frac{z_u - z_i}{\sqrt{(x_u - x_i)^2 + (y_u - y_i)^2 + (z_u - z_i)^2}}. \tag{1.27b}$$

In order to obtain a position in three-dimensional space, at least two anchors are necessary to obtain an intersection of at least two direction vectors defined by azimuth, polar angles and anchor position.

1.5.1.3 Hybrid Localization

Instead of exclusively relying on distance or angle measurements, a combination of these two approaches is possible which leads to the so-called hybrid localization. Measuring azimuth and polar angle as well as the distance from one anchor to the node is sufficient to get its position relative to the anchor. The principle is depicted in Figure 1.11. Typical applications are airplane surveillance Radio Detection and Ranging (RADAR) systems that measure angles with mechanically and electronically steered antennas. Distance is measured from the radio wave echo reflected from the airplane, allowing its position estimation.

1.5.1.4 Fingerprinting

Airplanes are usually in Line of Sight (LoS) to ground based positioning systems and hence accurate angle and distance estimates can be obtained for geometric localization. However, many applications exist where these estimates are strongly biased and noisy. Localizing oneself in the streets of a city by estimating the distance to distinctive points of known location such as churches or skyscrapers is challenging as these points might not be in LoS. Instead of geometric positioning, an approach that infers location based on the similarity of observed features to a given map, the so-called fingerprinting, is used. Regarding the example of localizing oneself in a city, the fingerprinting analogy is given as follows. In order to determine position in an urban environment, street names, prominent buildings and other features are observed. Searching and finding them on a street map results in position information.

This principle can be generalized to any type of observable that varies with position. Depending on the scenario, a sufficient large set of observations is necessary for precise localization, e.g. two street names are required to determine the intersection and hence position. This approach further needs the construction of maps from which position is estimated by similarity. The construction of these maps is based on the collection of large sets of georeferenced observations. Besides the complexity for map construction, updating the latter is equally necessary as the environment changes and hence observables too.

A standard algorithm for fingerprinting is the k-Nearest Neighbors (kNN) algorithm [JABW18].

1.5.2 Overview on Localization Metrics

Localization techniques are based on distance or angle estimates or other observations that carry information about the nodes position as explained in Chapter 1.5.1. These observations are in return extracted from primary

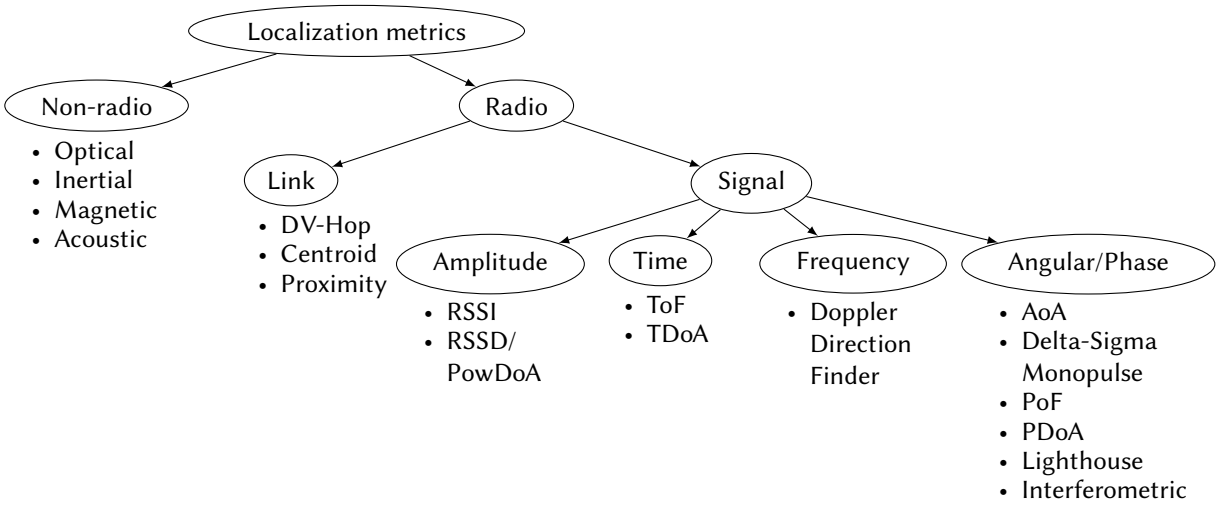


FIGURE 1.12 – *Overview on localization metrics with a strong focus on radio signal based metrics.*

metrics that are called localization metrics in the following. An overview on available localization metrics with a focus towards LPWA localization is given in the following.

Figure 1.12 classifies localization metrics extractable from radio transmissions as well as non-radio metrics.

1.5.2.1 Optical

Optical localization can be split into camera i.e. vision based localization and optical based localization techniques that are based measuring the propagation delay of emitted light pulses. Analog to RADAR, light based positioning techniques are called Light Detection and Ranging (LIDAR). It is hence a type of radio signal based localization metric. However, in contrast to classical radio localization techniques, light based methods only extract information from amplitude i.e. intensity variations. With regard to LPWA localization this requires additional hardware i.e. a light source and an optical sensors, hence it can also be classified as non-radio metric [Zhu+18].

Earth-moon distance measurements with laser beams pointing to a mirror setup on the moon, are a prominent example of LIDAR. Recently, LIDAR systems are integrated for vehicular localization [HFJK19; dBLD19]. Due to the properties of light propagation, visible LoS condition is required for LIDAR operation. Regarding LPWA localization, LIDAR are unlikely be integrated into nodes, however it is possible to address the problem of inter-base station synchronization with optical links.

1.5.2.2 Inertial

Inertial positioning is based on accelerometers that capture acceleration. Acceleration $\boldsymbol{a}(t)$ is linked to position $\boldsymbol{x}(t)$ by double integration

$$\begin{cases} \ddot{\boldsymbol{x}}(t) & = \boldsymbol{a}(t), \\ \dot{\boldsymbol{x}}(t_0) & = \boldsymbol{v}_0, \\ \boldsymbol{x}(t_0) & = \boldsymbol{x}_0. \end{cases} \tag{1.28}$$

Positioning by inertial methods provides relative information to a given initial position $\boldsymbol{x}_0$ and absolute position can only be obtained with a prior knowledge of this initial position $\boldsymbol{x}_0$. Inertial localization consequently focuses on navigation applications. Inertial navigation does not require an infrastructure of georeferenced anchors as only the starting point $\boldsymbol{x}_0$ and the initial velocity $\boldsymbol{v}_0$ need to be known for absolute positioning. Major drawbacks of the double integration are large location errors due to biases in the estimated accelerations. To combat this, sophisticated calibration steps are necessary [Gro13]. Inertial navigation, providing good short-term position estimates, is often combined with other modalities to keep long-term errors to a minimum. For indoor navigation, algorithms might take floor plans of the building into account to constrain the positions [ZVL17]. In vehicular localization GNSS, inertial localization information and street map constaints are fused to obtain *e.g.* precise location in tunnels where GNSS is temporarily not available (dead reckoning) [KH06; Gro13].

1.5.2.3 Magnetic

Magnetic localization takes advantage of distortions in the earth magnetic field inside buildings to localize. Concrete reinforcement of walls and floors results in modifications of the magnetic field which can be used in a mapping step to construct magnetic maps for fingerprinting based indoor localization [Ang+12]. Typical localization precisions are $\approx 5\,\mathrm{m}$ [MS15] which can be degraded by moving metal objects such as lifts. This localization modality is usually fused with *e.g.* inertial positioning, both available on modern smart-phones, for accurate pedestrian navigation [Ash+13] or to provide initialization information for the orientation of a device [VFF19].

1.5.2.4 Acoustic

A prominent example for acoustic localization is the rule of thumb for determining the distance of a thunderstorm [Enc12]

> *"Count the seconds between the lightning strike and the thunder. Dividing the seconds by three results in the distance of the thunderstorm from the observer in kilometers."*

The principle behind this rule of thumb is the difference in propagation speed for electromagnetic and acoustic waves. While electromagnetic waves, hence the lightning, propagate at c_0, acoustic waves propagate at the much lower speed c_{sound} as listed in Table 1.4. The rule of thumb results from the simplification and hypothesis that

	Electromagnetic	**Acoustic**
	c_0 in m/s	c_{sound} in m/s at 20 °C
Vacuum	299 792 458	n/a
Air	299 700 000	343
Water	225 000 000	1480

Table 1.4 – *Propagation speed of light and sound in different media.*

the lightning is instantly and its propagation time is neglected. The most prominent field of acoustic localization is underwater maritime positioning [Sim+06] where electromagnetic waves suffer extensively high propagation attenuations and make RADAR based localization techniques impractical [Jim+16].

1.5.2.5 Introduction to Radio Localization Metrics

Radio transmission based localization metrics offer the advantage that they can possibly be added and integrated to existing communications systems. Hence position information becomes available without the necessity to add a further sensor *e.g.* accelerometer or microphone. Therefore, radio based positioning is interesting in terms of system complexity and cost, which are critical to LPWA localization.

As illustrated in Figure 1.12 radio based metrics can be separated into the two main groups of link and signal based metrics. A comprehensive survey of localization, tracking and navigation technologies for networks is given in [Lao+18]

Link metrics such as connectivity and packet error rate are obtained on the link level and serve to obtain a rough position estimate. Connectivity to a base station of known location can be used to conclude, that the wireless node is near the base station. Vicinity is hereby defined by the coverage of a communication system. LoS propagation to a faraway base station and blockage to a nearby base station due to *e.g.* buildings, create significant estimation errors and illustrate the limitation of such a simple localization metric. In meshed networks, algorithms such as DV-Hop [NN01] or the Centroid algorithm [He+03] allow to localize with connectivity metrics.

While link metrics are directly accessible when wireless communication is performed, the localization accuracy is in the order of magnitude of the node to base station distance. For a sparse LPWA base station density, aimed to reduce deployment effort and cost, link metric based positioning will only provide kilometer-level precision.

Signal metrics rest upon the idea to measure the impact, which the radio propagation channel has on the transmitted signal. Main hypothesis herby is the variation of the propagation channel with node and base station position.

A radio signal can be varied in amplitude, time, phase, and any combination of these. While time and phase modifications by the radio channel are equivalent as they both arise from time delays, they are regarded separately in the following classification.

1.5.2.6 Amplitude

Signal amplitude A and signal power P_r are exchangeable as linked by

$$P_\mathrm{r} = \frac{A^2}{Z}, \tag{1.29}$$

with system impedance Z.

Considering free-space propagation between the wireless node and the base station, received power P_r depends on distance according to Friis law [Fri46] given in (1.1).

Assuming transmit power P_t, transmitter G_t and receiver G_r antenna gain as well as carrier wavelength λ_w to be invariant, they can be summarized in constant C_st as

$$P_\mathrm{r} = C_\mathrm{st} d^{-2} = C_\mathrm{st0} \left(\frac{d}{d_0}\right)^{-2}, \tag{1.30}$$

with $C_\mathrm{st0} = C_\mathrm{st} d_0^{-2}$ the received power at the reference distance d_0. In logarithmic scale, received power and distance are linked by

$$(P_\mathrm{r})^\mathrm{dBm} = (C_\mathrm{st0})^\mathrm{dBm} - 20 \log_{10}\left(\frac{d}{d_0}\right). \tag{1.31}$$

For known transmit power, antenna gains and a given carrier frequency i.e. known constant C_st0, distance can be deduced directly from received power

$$d = d_0 \, 10^{\left(-\frac{(P_\mathrm{r})^\mathrm{dBm} - (C_\mathrm{st0})^\mathrm{dBm}}{20}\right)}. \tag{1.32}$$

If transmit power P_t and hence C_st0 are not known to the receiver, a so-called Received Signal Strength Difference (RSSD) or Power Difference of Arrival (PowDoA) technique, not to be confused with Phase Difference of Arrival (PDoA), can be applied. Measuring the received power $P_{\mathrm{r}i}$ and $P_{\mathrm{r}k}$ at two base stations i and k and calculating the PowDoA $(P_{\mathrm{r}i})^\mathrm{dBm} - (P_{\mathrm{r}k})^\mathrm{dBm}$ of known position, allows to establish the distance ratio d_i/d_k [Guo+11; JWI11; NCAC18].

The received signal strength metric is available on most communication systems, which provide it as Received Signal Strength Indicator (RSSI). Besides indicating communication quality, it can be used to notify the transmitter to increase transmission power. While integrated into almost all digital wireless radio transceiver chips, the RSSI does not provide accurate positioning estimates due to the following reasons:

- Multipath propagation channels.
- Precision degrades with node to base station or inter-node distance and due to measurement noise.

Free-space propagation assumed for Friis law in (1.1) only applies in approximation to inter-satellite and earth-satellite communication. However, the free-space condition is in general not given in terrestrial communication scenarios, where multipath reflections result in constructive or destructive signal interference.

As a rule of thumb, 60% of the 1st Fresnel zone need to be free from obstruction so that there is no additional attenuation [McL97].

These Fresnel zones are ellipsoid volumes between the two communicating nodes with the antennas in the ellipsoid foci as illustrated in Figure 1.13.

The k^th Fresnel zone is defined as the volume in which the distance difference between the direct and the once reflected path is in the interval $[(k-1)\lambda_\mathrm{w}, k\lambda_\mathrm{w}]$. The radius $R_{\mathrm{Fresnel},k}$ of the k^th Fresnel zone with distance d_1, d_2 to the nodes can be calculated approximately (derivation in Appendix A) by

$$R_{\mathrm{Fresnel},k} \approx \sqrt{\frac{k\lambda_\mathrm{w} d_1 d_2}{d_1 + d_2}}. \tag{1.33}$$

Fresnel zone radius in the center between the two nodes i.e. $d_1 = d_2$ is given in Table 1.5 for the SRD 868 MHz band and ISM 2.4 GHz band as

$$R_{\mathrm{Fresnel},k} \approx \sqrt{\frac{k\lambda_\mathrm{w} d}{2}}. \tag{1.34}$$

For scenarios where this condition does not hold, i.e. in multipath propagation channels, empirical channel models are used, such as the Hata model [Hat80] for urban scenarios. These so-called log-normal models are given by

$$(P_\mathrm{r})^\mathrm{dBm} = (C_\mathrm{st0})^\mathrm{dBm} - 10\gamma_L \log_{10}\left(\frac{d}{d_0}\right) + (n_\mathrm{Channel})^\mathrm{dB}, \tag{1.35}$$

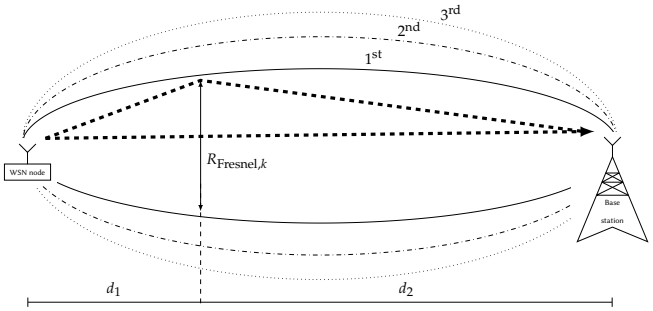


FIGURE 1.13 – *The first three Fresnel zones for radio signal propagation.*

		Fresnel zone radius $R_{\text{Fresnel},k}$ in m							
	f	868 MHz				2.4 GHz			
k	$2d$	10 m	100 m	3 km	5 km	10 m	100 m	3 km	5 km
1		0.9	2.9	16.1	20.8	0.6	1.8	9.7	12.5
2		1.3	4.2	22.8	29.4	0.8	2.5	13.7	17.7
3		1.6	5.1	27.9	36.0	1.0	3.1	16.8	21.7

TABLE 1.5 – *Center Fresnel zone radius of two nodes at distance* $2d$.

with path loss exponent γ_L and $C_{\text{st0}} = C_{\text{st}} d_0^{-\gamma_L}$. On average, received power decreases logarithmical with distance. In addition, to model actual received power, shadowing and small-scale fading effects are approximated with a zero-mean Gaussian random variable $(n_{\text{Channel}})^{\text{dB}}$ of variance $\left(\sigma^2_{\text{Channel}}\right)^{\text{dB}}$.

Performing an RSSI measurement is an estimation process where real received signal strength and estimated RSSI are linked by

$$\left(\widehat{P}_{\text{r}}\right)^{\text{dBm}} = (P_{\text{r}})^{\text{dBm}} + (n_{\text{RSSI}})^{\text{dB}}, \tag{1.36}$$

with Gaussian distributed measurement noise $(n_{\text{RSSI}})^{\text{dB}}$ of variance $\left(\sigma^2_{\text{RSSI}}\right)^{\text{dB}}$.

From (1.36) the theoretical lower bound on the distance standard deviation is given by the CRLB (derivation in Appendix B.1) as

$$\sqrt{\text{Var}\left(\widehat{d}\right)} \geq \left(\frac{d \ln 10}{-10\gamma_L}\right) \sqrt{\sigma^2_{\text{Channel}} + \sigma^2_{\text{RSSI}}}. \tag{1.37}$$

From (1.37) it can be concluded, that the minimum achievable precision for RSSI based range estimation depends on the actual range.

For numerical evaluation of (1.37), empirical path loss model values γ_L and σ_{Channel} are taken from an existing LPWA deployment scenario [Wd15]. It is assumed that the RSSI readings provided by the radio receiver have a standard deviation of $(\sigma_{\text{RSSI}})^{\text{dB}} = 1\,\text{dB}$. The theoretical range estimation error lower bound is given in Table 1.6.

This illustrates the fundamental dilemma of RSSI based ranging and therefore RSSI based trilateration localization (see Chapter 1.5.1.1) with long-range LPWA networks. Utilizing RSSI measurements for localization remains however interesting due to its implementation simplicity. Fingerprinting techniques can possibly provide more precise and accurate location estimates, as they associate a RSSI measurement directly to a position based on the similarity of previously recorded geo-referenced RSSI measurements.

1.5.2.7 TIME

While signal amplitude decreases with distance due to attenuation, signals are delayed in time as electromagnetic waves propagate at the finite speed of light c_0. Compared to acoustic wave propagation at c_{sound}, electromagnetic signal delays are much shorter as listed in Table 1.7. Measuring the delay τ of a wireless transmitted message allows to calculate the distance d between transmitter and receiver by

$$d = c_0 \tau. \tag{1.38}$$

	Pathloss exponent γ_L	**Shadowing and small-scale fading standard deviation σ_{Channel} in dB**	**Distance error normalized to real distance $\frac{\sqrt{\text{Var}\left(\widehat{d}\right)}}{d}$**
Free-space theoretical	2.00	0	0.12
Free-space realistic	2.00	3.00	0.36
Hata suburban [Hat80]	4.00	6.00	0.35
LoRa suburban [Wd15]	2.55	8.48	0.77

TABLE 1.6 – *Range estimation error CRLB for RSSI based range estimation according to a log-normal path loss model.*

	Electromagnetic	**Acoustic**	
	τ at $(c_0)_{\text{air}}$ in s	τ at $(c_{\text{sound}})_{\text{air}}$ in s at 20 °C	τ at $(c_{\text{sound}})_{\text{water}}$ in s at 20 °C
1 cm	$33.4 \cdot 10^{-12}$	$29.2 \cdot 10^{-6}$	$6.8 \cdot 10^{-6}$
1 m	$3.3 \cdot 10^{-9}$	$2.9 \cdot 10^{-3}$	$675.7 \cdot 10^{-6}$
1 km	$3.3 \cdot 10^{-6}$	2.9	$675.7 \cdot 10^{-3}$

TABLE 1.7 – *Delay of light/radio and sound waves for different ranges.*

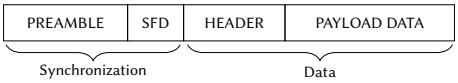


FIGURE 1.14 – *Typical wireless packet structure, comprising both synchronization and data.*

Time of Arrival (ToA) Estimation

In order to measure the propagation delay $\tau^{[T_1,R_2]}$, the transmitter adds a time stamp to the packet to send. This time stamp represents the Time of Departure (ToD) $t_{\text{D}}^{[T_1]}$ when the packet was sent from transmitter T_1. At the receiving side at receiver R_2, the time of packet reception i.e. the ToA $t_{\text{A}}^{[R_2]}$ is recorded. The time difference corresponds to the propagation delay $\tau^{[T_1,R_2]}$ and the distance $d^{[T_1,R_2]}$ between the nodes

$$d^{[T_1,R_2]} = c_0 \left(t_{\text{A}}^{[R_2]} - t_{\text{D}}^{[T_1]} \right) = c_0 \left(t_{\text{D}}^{[T_1]} + \tau^{[T_1,R_2]} - t_{\text{D}}^{[T_1]} \right) = c_0 \tau^{[T_1,R_2]}. \tag{1.39}$$

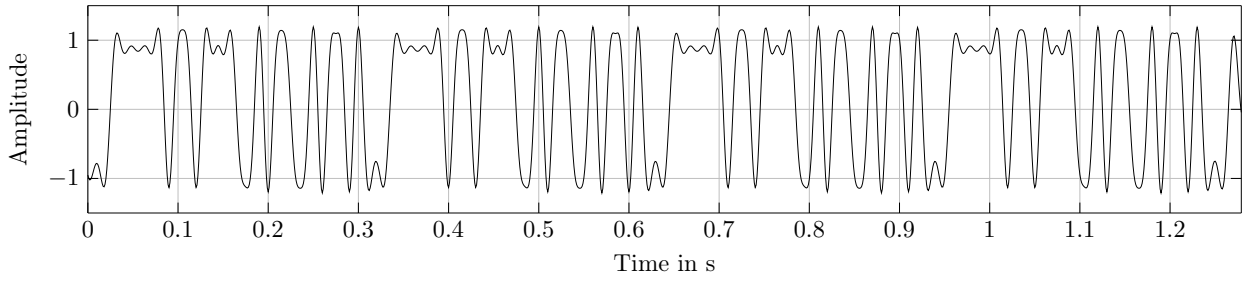
Additional delays, such the time between adding the transmission time stamp and actually sending the packet and radio frequency delays in the antenna cables are assumed constant or controllable and can be encountered for in a calibration step.

The process of determining the time of packet reception is generally called synchronization in communication systems. Wired communication systems, such as Peripheral Component Interconnect (PCI) or Serial Peripheral Interface (SPI) buses, use dedicated clock lines to share a common time reference. This mutual clock ensures that the receiver reads data lines at time instances when transmitted signals are valid. In wireless communication systems, no such common clock is available and synchronization is part of each data transfer. In general, packets are composed of a synchronization and a data part as depicted in Figure 1.14. The receiver searches for the preamble, a predefined sequence known to both, transmitter and receiver. This sequence is used to align the receiver clock so that it is synchronized with the following data part of the received packet. A SFD indicates the end of the preamble for clock synchronization and the start of the data part. Synchronization can be achieved by correlating the received signal r with the known preamble s_0 of length T_{preamble}

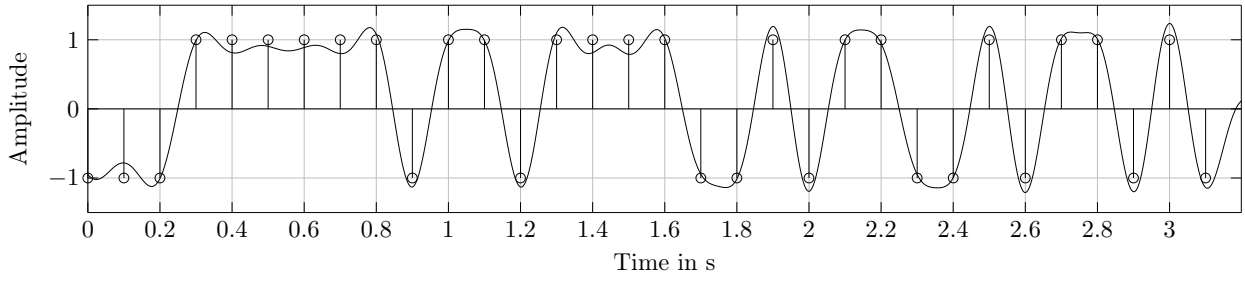
$$\Omega_{r,s_0}(t) = \int_0^{T_{\text{preamble}}} r(\gamma + t) s_0^*(\gamma) d\gamma. \tag{1.40}$$

The time shift corresponding to the maximum of the correlator output yields the ToA estimation

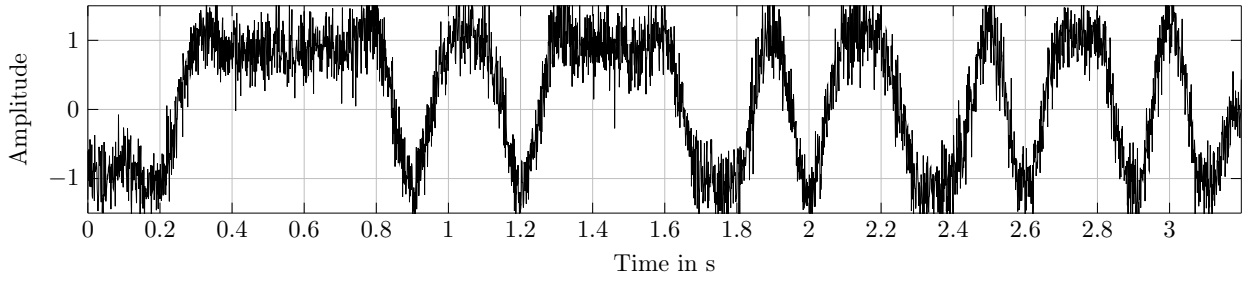
$$\widehat{t_{\text{A}}} = \arg\max_t \left| \Omega_{r,s_0}(t) \right|. \tag{1.41}$$



(a) $R = 100\,\text{kHz}$, 128 bit.



(b) $R = 10\,\text{kHz}$, 32 bit.



(c) $R = 10\,\text{kHz}$, 32 bit *with noise.*

FIGURE 1.15 – *ToA estimation illustrated on a root-raised cosine BPSK signal.*

Due to this synchronization process, the receiver holds the estimated ToA $\widehat{t_\text{A}}$ of the received packet, which is required for a propagation delay measurement according to (1.39).

Figure 1.15a illustrates a BPSK preamble of 128 bits. For a bit rate of 100 bit/s, symbols have sharp edges and ToA detection can be more precise than for a lower symbol rate of 10 bit/s in Figure 1.15b. This is due to the width of the correlation peak, directly linked to bit duration. Further, noise blurs the exact maximum of symbols and degrades precise ToA estimation as illustrated in Figure 1.15c. Intuitively, ToA precision depends invers proportional on signal bandwidth for resolution and available symbol energy for averaging noise. For a delayed signal in Additive White Gaussian Noise (AWGN) n

$$r(t) = s_0(t - \tau) + n(t), \tag{1.42}$$

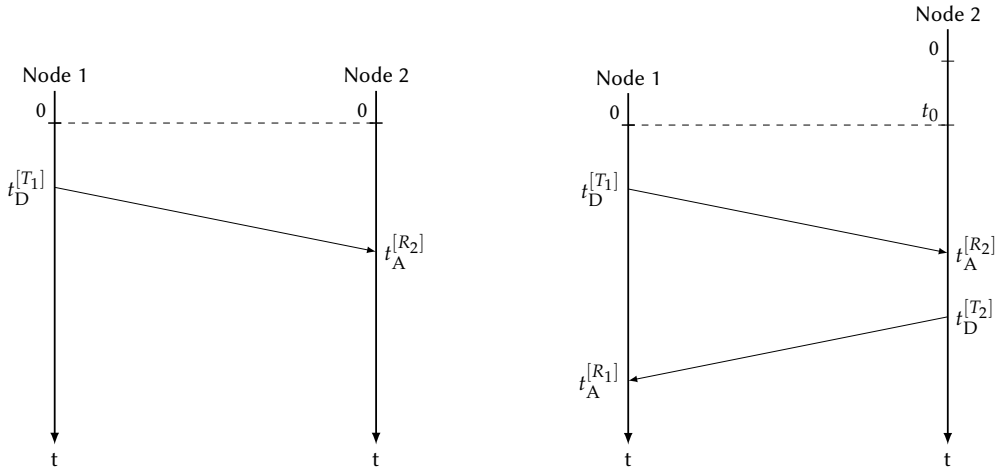
the lowest achievable ToA precision is given by the theoretical CRLB (see full derivation in Appendix B.2)

$$\sqrt{\text{Var}\left(\widehat{t_\text{A}}\right)} \geq \sqrt{\frac{1}{4\pi^2 \frac{E_\text{S}}{N_0} B_\text{RMS}^2}}, \tag{1.43}$$

where the symbol energy to noise spectral density ratio E_S/N_0 accounts for the sequence used for ToA estimation, i.e. the whole preamble sequence. The Root Mean Square (RMS) bandwidth is given by

$$B_\text{RMS} = \sqrt{\frac{\int_{-\infty}^{\infty} f^2 \left|S_0(f)\right|^2 df}{\int_{-\infty}^{\infty} \left|S_0(f)\right|^2 df}}, \tag{1.44}$$

where $S_0(f)$ represents the spectrum of the baseband waveform s_0.



(a) *One-way protocol for synchronized nodes.*

(b) *Two-way protocol for unsynchronized nodes.*

FIGURE 1.16 – *ToA based ranging protocol.*

Synchronized Nodes, One-Way

Transmit time stamp and receive time stamp obtained from ToA estimation can only be used in (1.39) to obtain node distance if they are in a common time reference. This requires that transmitting and receiving node share the exact time reference as depicted in Figure 1.16a. In mono-static RADAR systems [Sko90], where transmitter and receiver are co-located and share a common clock, ToA estimation can be directly translated to radar-target range d by

$$\widehat{d} = c_0 \frac{\widehat{t_{\mathrm{A}}} - t_{\mathrm{D}}}{2}, \tag{1.45}$$

with one ToA estimation $\widehat{t_{\mathrm{A}}}$ and the known ToD t_{D}. The precision limit improves compared to pure ToA estimation by

$$\sqrt{\mathrm{Var}\left(\widehat{d}\right)} = c_0 \frac{\sqrt{\mathrm{Var}\left(\widehat{t_{\mathrm{A}}}\right)}}{2}, \tag{1.46}$$

due to the division by 2 in (1.45) accounting for the round-trip delay between the radar and the target.

Unsynchronized Nodes, Two-Way

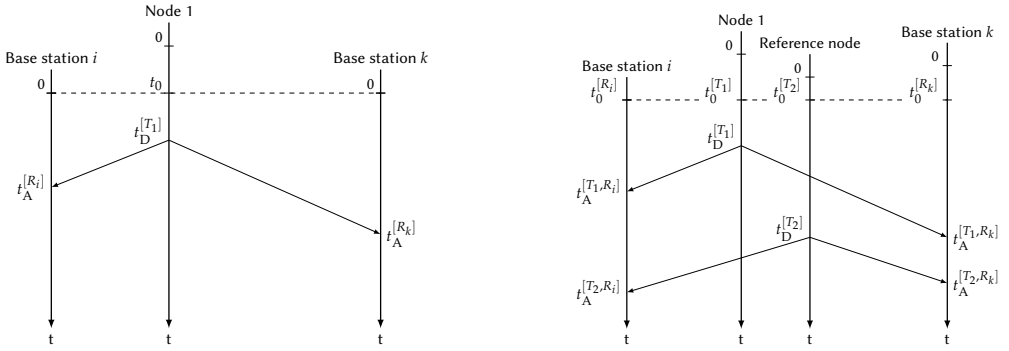
When transmitter and receiver are separated and do not share a common clock, time synchronization needs to be established in the range estimation protocol. Considering a time-offset t_0 between the clocks of node 1 and node 2 according to Figure 1.16b the ToA estimation is given by

$$d^{[T_1,R_2]} = c_0 \left(t_{\mathrm{A}}^{[R_2]} - t_{\mathrm{D}}^{[T_1]} \right) = c_0 \left(t_{\mathrm{D}}^{[T_1]} + \tau^{[T_1,R_2]} + t_0 - t_{\mathrm{D}}^{[T_1]} \right) = c_0 \left(\tau^{[T_1,R_2]} + t_0 \right). \tag{1.47}$$

The propagation delay $\tau^{[T_1,R_2]}$ cannot be derived from the time stamp $t_{\mathrm{D}}^{[T_1]}$ and ToA estimation $t_{\mathrm{A}}^{[R_2]}$ as time-offset t_0 is arbitrary and unknown. This time-offset t_0 can be eliminated in a two-way packet exchange where node 2 responds with a packet to node 1 as depicted in Figure 1.16b

$$\begin{aligned} d^{[T_1,R_2]} = d^{[T_2,R_1]} &= \frac{c_0}{2} \left[\left(t_{\mathrm{A}}^{[R_1]} - t_{\mathrm{D}}^{[T_1]} \right) - \left(t_{\mathrm{D}}^{[T_2]} - t_{\mathrm{A}}^{[R_2]} \right) \right] \\ &= \frac{c_0}{2} \left[\left(t_{\mathrm{D}}^{[T_2]} + \tau^{[T_1,R_2]} - t_0 \right) + \left(t_{\mathrm{D}}^{[T_1]} + \tau^{[T_1,R_2]} + t_0 \right) - \left(t_{\mathrm{D}}^{[T_2]} + t_{\mathrm{D}}^{[T_1]} \right) \right] \\ &= c_0 \tau. \end{aligned} \tag{1.48}$$

In practice, node 1 measures the Time of Flight (ToF) $\widehat{t_{\mathrm{A}}}^{[R_1]} - t_{\mathrm{D}}^{[T_1]}$ and the response time $t_{\mathrm{D}}^{[T_2]} - \widehat{t_{\mathrm{A}}}^{[R_2]}$ of node 2 is considered to be known to node 1. The precision limit is given by the average of two ToA estimates and evaluates



(a) *Synchronized base stations.*

(b) *Unsynchronized base stations with a reference node.*

FIGURE 1.17 – *TDoA based ranging protocol.*

to

$$\sqrt{\mathrm{Var}\left(\widehat{d}\right)} = c_0\sqrt{\left(\frac{1}{2}\right)^2\left[\mathrm{Var}\left(\widehat{t_A}^{[R_2]}\right) + \mathrm{Var}\left(\widehat{t_A}^{[R_1]}\right)\right]} = c_0\frac{\sqrt{\mathrm{Var}\left(\widehat{t_A}\right)}}{\sqrt{2}}. \tag{1.49}$$

Independent clocks on node 1 and node 2 do not only introduced time-offsets but also different clock frequencies. These are result of hardware imperfections and their influence on radio signal based ranging estimation methods will be investigated in Chapter 3.2.

Differential, Time Difference of Arrival (TDoA)

Two-way packet exchanges allowing the elimination to unknown time-offset t_0 might be unfeasible in a given application. Considering circular trilateration, one two-way exchange needs to be performed for each base station. For two-dimensional positioning, at least three two-way exchanges are required. As a result, in order to obtain one position estimate, six packets must be exchanged. Further, node and base stations must operate in bi-directional mode.

In LPWA networks, wireless nodes are often transmitter only. To comply with this requirement, TDoA measurements can be performed on a single uplink packet only. For two time synchronized base stations (i,k) that receive the same uplink packet from a node the two ToA measurements are given by

$$t_A^{[R_i]} = t_D^{[T_1]} + \tau^{[T_1,R_i]} + t_0, \tag{1.50a}$$

$$t_A^{[R_k]} = t_D^{[T_1]} + \tau^{[T_1,R_k]} + t_0, \tag{1.50b}$$

where t_0 accounts for the fact that the node is not synchronized with the base stations, as depicted in Figure 1.17a. The difference of these two ToA estimates is given by

$$\Delta T_A^{[T_1]} = t_A^{[R_k]} - t_A^{[R_i]} = \tau^{[T_1,R_k]} - \tau^{[T_1,R_i]}, \tag{1.51}$$

where the unknown t_0 cancels. This time difference multiplied by the speed of light c_0 translates to a range difference. All possible node positions satisfying this range difference lie on a hyperbola between base station i and k given by (1.26). Unique position can be estimated based on at least three TDoA estimates using a hyperbolic trilateration approach. The approach can equally be inversed, where the base stations transmit beacon messages and position estimation is done in downlink, *e.g.* GNSS localization. The precision limit of a TDoA range difference is given by the sum of the variances of two independent ToA estimates as

$$\sqrt{\mathrm{Var}\left(\widehat{\Delta d}\right)} = c_0\sqrt{\mathrm{Var}\left(\widehat{t_A}^{[R_2]}\right) + \mathrm{Var}\left(\widehat{t_A}^{[R_1]}\right)} = \sqrt{2}c_0\sqrt{\mathrm{Var}\left(\widehat{t_A}\right)}, \tag{1.52}$$

assuming equal variance for both ToA estimates.

Time synchronization of base stations required for TDoA estimation can be achieved using synchronization over the network backbone or by adding a GNSS module on the base station *e.g.* [LoR18] where power consumption and integration constraints are less restrictive than on a wireless sensor node. Moreover, base station synchronization can also be performed by using a reference node of known location *e.g.* [PSSV09a; Sch11]. Such a reference node

will allow aligning the base station clocks as illustrated in Figure 1.17b. In addition to the Time Difference of Arrivals (TDoAs) of the node of unknown position, the set of TDoAs of the reference node are available

Node of unknown position

$$t_{\mathrm{A}}^{[T_1,R_i]} = t_{\mathrm{D}}^{[T_1]} + \tau^{[T_1,R_i]} + t_0^{[R_i]}, \tag{1.53a}$$

$$t_{\mathrm{A}}^{[T_1,R_k]} = t_{\mathrm{D}}^{[T_1]} + \tau^{[T_1,R_k]} + t_0^{[R_k]}, \tag{1.53b}$$

Reference node of known position

$$t_{\mathrm{A}}^{[T_2,R_i]} = t_{\mathrm{D}}^{[T_2]} + \tau^{[T_2,R_i]} + t_0^{[R_i]}, \tag{1.53c}$$

$$t_{\mathrm{A}}^{[T_2,R_k]} = t_{\mathrm{D}}^{[T_2]} + \tau^{[T_2,R_k]} + t_0^{[R_k]}. \tag{1.53d}$$

Unknown base station time-offsets $t_0^{[R_i]}$ and $t_0^{[R_k]}$ can be cancelled by calculating the double TDoA

$$\begin{aligned}\Delta\Delta T_{\mathrm{A}} &= \Delta T_{\mathrm{A}}^{[T_1]} - \Delta T_{\mathrm{A}}^{[T_2]} \\ &= \left(t_{\mathrm{A}}^{[T_1,R_k]} - t_{\mathrm{A}}^{[T_1,R_i]}\right) - \left(t_{\mathrm{A}}^{[T_2,R_k]} - t_{\mathrm{A}}^{[T_2,R_i]}\right) \\ &= \left(\tau^{[T_1,R_k]} - \tau^{[T_1,R_i]}\right) - \left(\tau^{[T_2,R_k]} - \tau^{[T_2,R_i]}\right).\end{aligned} \tag{1.54}$$

The TDoA $\tau^{[T_2,R_k]} - \tau^{[T_2,R_i]}$ is known due to known reference node position with respect to the base stations and hence the problem reduces to hyperbolic TDoA. The accuracy and precision with which the ToAs of the reference node can be estimated will directly affect the quality of base station synchronization and hence the quality of estimating the position of the unknown node. The precision limit is given by the double-difference of four ToA estimates

$$\sqrt{\mathrm{Var}\left(\widehat{\Delta\Delta d}\right)} = 2c_0\sqrt{\mathrm{Var}\left(\widehat{t_{\mathrm{A}}}\right)}. \tag{1.55}$$

Channel Impulse Response $h(\tau)$

Accurate and precise ToF and TDoA localization relies on the hypothesis that the measurable propagation delay is directly linked to the actual range between the nodes. In this case, a single delayed path with amplitude a_0 and delay τ_0 can express the channel impulse response h

$$h(\tau) = a_0\delta\left(\tau - \tau_0\right). \tag{1.56}$$

In multipath and None Line of Sight (NLoS) propagation scenarios this hypothesis is violated and the channel impulse response becomes the superposition of multiple paths (see Chapter 2.3)

$$h(\tau) = \sum_{p=0}^{P} a_p\delta\left(\tau - \tau_p\right). \tag{1.57}$$

With Ultra-Wide Band (UWB) ranging technologies, it is possible to resolve the different propagation paths due to short pulses. Assuming that these pulses are much shorter than the delay between adjacent multipath components it is hence possible to get an estimate of the channel impulse response h according to Figure 1.18 and

$$\widehat{h}_{s_0}(\tau) = s_0(t) * h(\tau). \tag{1.58}$$

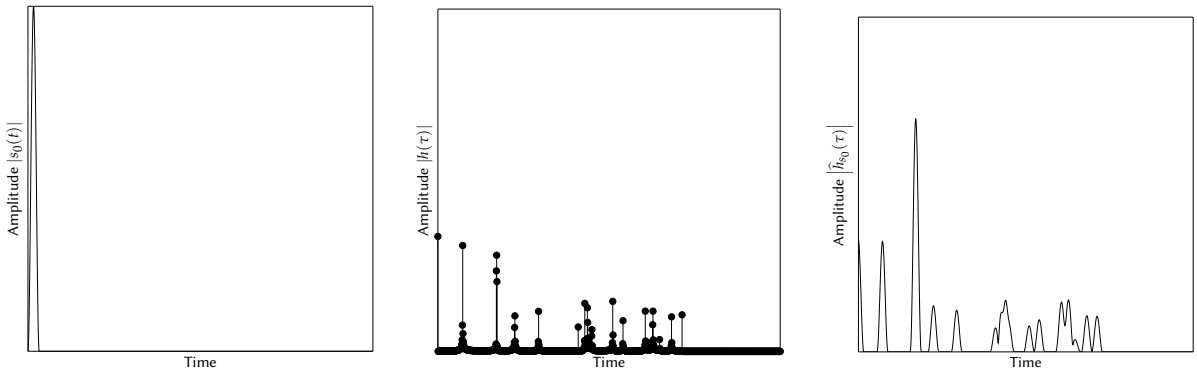
Adequate algorithms are used to track the temporal evolution of multipath components and to predict the range i.e. LoS component during NLoS phases [MDDU17]. Other approaches combine the estimated channel impulse response with geometric information of the propagation environment to infer position [Mei14; Lei15].

1.5.2.8 Phase

Besides observing amplitude or time delay modifications of the radio signal to estimate position, it is also possible to extract location information from the signal phase. As stated in the introduction, time delay τ and carrier phase shifts ϕ are equivalent and linked by

$$\phi = -2\pi f\tau. \tag{1.59}$$

Hence, the techniques and the protocols in order to obtain ranging information are analog to those introduced for time based ranging. In the following, the basic steps as well as specificities for the phase metric are outlined.



(a) *UWB pulse* $s_0(t)$. (b) *Channel impulse response* $h(t)$. (c) *Estimated channel impulse response* $\widehat{h}_{s_0}(t)$.

FIGURE 1.18 – *Estimation of the channel transfer function through UWB signals.*

The sinusoidal carrier signal generated by the local oscillator X in node i, where X stands for transmitter T or receiver R, is given by

$$s_{\mathrm{LO}}^{[X_i]}(t) = e^{j\left(2\pi f^{[X_i]}t + \phi_{\mathrm{R}}^{[X_i]}\right)}. \tag{1.60}$$

Considering the baseband signal s_0, the signal transmitted in a free-space channel from node i and received by node k at a distance $d^{[T_i,R_k]} = c_0\tau^{[T_i,R_k]}$ is given by

$$s^{[T_i,R_k]}(t) = A_c^{[T_i,R_k]} \cdot g_{\mathrm{R}}^{[T_i]} \cdot g_{\mathrm{R}}^{[R_k]} \cdot s_0(t-\tau^{[T_i,R_k]}) \cdot s_{\mathrm{LO}}^{[T_j]}(t-\tau^{[T_i,R_k]}) \cdot s_{\mathrm{LO}}^{*[R_k]}(t), \tag{1.61}$$

with antenna gains $g_{\mathrm{R}}^{[T_i]}$ and $g_{\mathrm{R}}^{[R_k]}$ and path loss $A_c^{[T_i,R_k]}$.

Combining (1.60) and (1.61) yields

$$s^{[T_i,R_k]}(t) = A_c^{[T_i,R_k]} \cdot g_{\mathrm{R}}^{[T_i]} \cdot g_{\mathrm{R}}^{[R_k]} \cdot s_0(t-\tau^{[T_i,R_k]}) \cdot e^{j\left(2\pi\left[f^{[T_i]}-f^{[R_k]}\right]t - f^{[T_i]}\tau^{[T_i,R_k]} + \phi_{\mathrm{R}}^{[T_i]} - \phi_{\mathrm{R}}^{[R_k]}\right)}. \tag{1.62}$$

This signal has a frequency offset and is phase shifted compared to the original baseband signal. In the following, it is assumed that both oscillators have identical frequency $f^{[T_i]} = f^{[R_k]}$, a hypothesis that does not hold for independent oscillators but which is chosen here for illustration of the principle. The general case of CFO will be discussed in Chapter 3.2. Remaining the phase shift which is called Phase of Arrival (PoA) analogue to the Time of Arrival (ToA). It can be estimated through the correlation Ω_{r,s_0} of received r and original signal s_0 as follows

$$\begin{aligned}\widehat{\phi_{\mathrm{A}}}^{[T_i,R_k]} &= \arg\left\{\Omega_{r,s_0}\left(\widehat{t_{\mathrm{A}}}\right)\right\} \\ &= -2\pi f^{[T_i]}\tau^{[T_i,R_k]} + \phi_{\mathrm{R}}^{[T_i]} - \phi_{\mathrm{R}}^{[R_k]},\end{aligned} \tag{1.63}$$

where $\widehat{t_{\mathrm{A}}}$ corresponds to ToA estimate defined in (1.41).

Phase Synchronized Nodes

Besides the hypothesis of identical carrier frequency at both nodes, the unrealistic assumption of phase-synchronized oscillators is made. For phase synchronous oscillators initial phase $\phi_{\mathrm{R}}^{[T_i]} = \phi_{\mathrm{R}}^{[R_k]}$. With these two hypotheses the inter-node distance can be estimated from the PoA by

$$\widehat{d}^{[T_i,R_k]} = -c_0\frac{\widehat{\phi_{\mathrm{A}}}^{[T_i,R_k]}}{2\pi f^{[T_i]}}. \tag{1.64}$$

Phase Unsynchronized Nodes

The more general case considers two independent nodes with identical carrier frequency but different initial phase $\phi_{\mathrm{R}}^{[T_i]} \neq \phi_{\mathrm{R}}^{[R_k]}$. A two-way ranging protocol as illustrated in Figure 1.16b will cancel the initial phases,

as $\phi_{\mathrm{R}}^{[T_i]} = \phi_{\mathrm{R}}^{[R_i]}$ due to the same local oscillator for transmission and reception. After PoA extraction on each receiver, the distance can be estimated from the sum of the two PoAs as

$$\widehat{d}^{[T_i,R_k]} = -c_0 \frac{\widehat{\phi_{\mathrm{A}}}^{[T_i,R_k]} + \widehat{\phi_{\mathrm{A}}}^{[T_k,R_i]}}{4\pi f}. \tag{1.65}$$

Differential, Phase Difference of Arrival (PDoA)

Analogue to the principle of Time Difference of Arrival (TDoA) measurements, the Phase Difference of Arrival (PDoA) technique extracts range information from phase differences. Considering a pair of frequency and phase synchronized base stations (i,k) and a node 1 of unknown position but synchronized in frequency with the base stations, the PoAs are given by

$$\phi_{\mathrm{A}}^{[T_1,R_i]} = -2\pi f^{[T_1]} \tau^{[T_n,R_i]} + \phi_{\mathrm{R}}^{[T_1]} - \phi_{\mathrm{R}}^{[R_i]}, \tag{1.66a}$$

$$\phi_{\mathrm{A}}^{[T_1,R_k]} = -2\pi f^{[T_1]} \tau^{[T_n,R_k]} + \phi_{\mathrm{R}}^{[T_1]} - \phi_{\mathrm{R}}^{[R_k]}. \tag{1.66b}$$

The difference of these PoAs results in a PDoA estimate where the nodes initial phase cancels

$$\Delta\phi_{\mathrm{A}}^{[T_1,R_i,R_k]} = \phi_{\mathrm{A}}^{[T_1,R_i]} - \phi_{\mathrm{A}}^{[T_1,R_k]} = -2\pi f^{[T_1]} \left[\tau^{[T_1,R_i]} - \tau^{[T_1,R_k]}\right], \tag{1.67}$$

as $\phi_{\mathrm{R}}^{[R_i]} = \phi_{\mathrm{R}}^{[R_k]}$. Range difference is given by

$$\widehat{\Delta d}^{[T_1,R_i,R_k]} = -c_0 \frac{\widehat{\Delta\phi_{\mathrm{A}}}^{[T_1,R_i,R_k]}}{2\pi f^{[T_1]}}. \tag{1.68}$$

Relaxing the requirement of phase synchronized base stations and including a frequency synchronized reference node 2 of known location, PDoA allows cancelling the initial phase of the sending node. However, the initial phases of the base stations remain unresolvable

$$\Delta\phi_{\mathrm{A}}^{[T_1,R_i,R_k]} = \phi_{\mathrm{A}}^{[T_1,R_i]} - \phi_{\mathrm{A}}^{[T_1,R_k]} \qquad = -2\pi f^{[T_1]} \left[\tau^{[T_1,R_i]} - \tau^{[T_1,R_k]}\right] + \phi_{\mathrm{R}}^{[R_i]} - \phi_{\mathrm{R}}^{[R_k]}, \tag{1.69a}$$

$$\Delta\phi_{\mathrm{A}}^{[T_2,R_i,R_k]} = \phi_{\mathrm{A}}^{[T_2,R_i]} - \phi_{\mathrm{A}}^{[T_2,R_k]} \qquad = -2\pi f^{[T_2]} \left[\tau^{[T_2,R_i]} - \tau^{[T_2,R_k]}\right] + \phi_{\mathrm{R}}^{[R_i]} - \phi_{\mathrm{R}}^{[R_k]}. \tag{1.69b}$$

They cancel in the difference of the PDoA of the node and the reference node. The Double Difference Phase Difference of Arrival (DPDoA) is given by

$$\begin{aligned}
\Delta\Delta\phi_{\mathrm{A}}^{[T_1,T_2,R_i,R_k]} &= \Delta\phi_{\mathrm{A}}^{[T_1,R_i,R_k]} - \Delta\phi_{\mathrm{A}}^{[T_2,R_i,R_k]} \\
&= \left\{\phi_{\mathrm{A}}^{[T_1,R_i]} - \phi_{\mathrm{A}}^{[T_1,R_k]}\right\} - \left\{\phi_{\mathrm{A}}^{[T_2,R_i]} - \phi_{\mathrm{A}}^{[T_2,R_k]}\right\} \\
&= -2\pi f^{[T_1]} \left[\tau^{[T_1,R_i]} - \tau^{[T_1,R_k]}\right] + 2\pi f^{[T_2]} \left[\tau^{[T_2,R_i]} - \tau^{[T_2,R_k]}\right].
\end{aligned} \tag{1.70}$$

Range difference can be directly extracted with (1.68)

$$\widehat{\Delta d}^{[T_1,R_i,R_k]} = -c_0 \frac{\Delta\Delta\phi_{\mathrm{A}}^{[T_1,T_2,R_i,R_k]} - 2\pi f^{[T_2]} \left[\tau^{[T_2,R_i]} - \tau^{[T_2,R_k]}\right]}{2\pi f^{[T_1]}}, \tag{1.71}$$

where the reference node delays $\tau^{[T_2,R_i]}$ and $\tau^{[T_2,R_k]}$ are known.

Ambiguity

The 2π periodicity of phase measurements translates to a range ambiguity concerning all previously introduced phase based ranging methods. Compared to (1.59), where phase periodicity was neglected, the observable phase is within $[0, 2\pi)$

$$\widehat{\phi_{\mathrm{A}}} = -2\pi f\tau \mod 2\pi \tag{1.72}$$

and the ambiguous distance estimation from a phase observation $\widehat{\phi_{\mathrm{A}}}$ is given by

$$\widehat{d}_{\mathrm{PoA}} = -c_0 \frac{\widehat{\phi_{\mathrm{A}}}}{2\pi f} \in [0, \lambda_{\mathrm{w}}). \tag{1.73}$$

	Carrier frequency f_w in MHz	**Carrier wavelength λ_w in** mm
ISM 169	169.000	1773.37
ISM 433	433.000	692.15
SRD 868	868.000	345.27
ISM 2400	2400.000	124.88
ISM 5000	5000.000	59.94
GPS (L_5, L_2, L_1)	1176.450, 1227.600, 1575.420	254.75, 244.13, 190.23
GLONASS (L_3, L_2, L_1)	1201.000, 1246.000, 1602.000	249.54, 240.53, 187.08
Galileo (E_5, E_6, L_1)	1191.795 , 1278.000, 1575.420	251.47, 234.51, 190.23
Beidou ($B_{2,I}$, B_3, $B_{1,I}$)	1207.140, 1268.520, 1561.0980	248.27, 236.26, 191.98

TABLE 1.8 – *Carrier frequency and wavelength for LPWA communication in SRD and ISM bands and GNSS systems.*

Phase ambiguity will not be of concern for systems where the carrier wavelength is larger than the distance to estimate. However, as Table 1.8 reveals, range ambiguity has to be considered for LPWA localization with sub-GHz signals as well as for GNSS where the wavelength is in the decimeter range.

In order to resolve the range ambiguity several different approaches are possible:

- Resolving ambiguity on the system level, *e.g.* based on street constraints.
- Push the ambiguity further away by using multiple carrier frequencies.
- Resolving ambiguity by resolving the number of integer cycles between node and base station.

These main approaches will be explained in the following. Examples of real systems applying these approaches or their combination are discussed.

To extract the PoA, a correlation between template and received signal is performed, which also provides the ToA based range estimate $\hat{d}_\mathrm{ToA}$. This ToA estimate can potentially be used to resolve range ambiguity. If the ranging accuracy and precision of the time based ranging method is smaller than the range ambiguity, range can be estimated by [SVPS08]

$$\widehat{d} = \widehat{d}_\mathrm{PoA} + l\lambda_\mathrm{w}, \tag{1.74}$$

with integer phase ambiguity

$$l = \underset{k\in\mathbb{Z}}{\arg\min} \left| \left(\widehat{d}_\mathrm{PoA} + \lambda_\mathrm{w} k\right) - \widehat{d}_\mathrm{ToA} \right|. \tag{1.75}$$

This approach however fails for time-based errors larger than the range ambiguity. Considering a sub-GHz LPWA system and the CRLB for time based ranging (1.43), it is obvious that this approach will not work for narrowband long-range localization as decimeter ToA accuracy cannot be achieved in theory.

As the range ambiguity is conditioned by the carrier wavelength, it is sufficient to increase carrier wavelength and the ambiguity will be further away automatically. Changing i.e. lowering the carrier frequency for a given communication system is not practical. However, it is possible to virtually create large wavelengths as the difference of two adjacent channels with carrier frequency f_1 and f_2

$$\Delta\lambda_\mathrm{w} = \frac{c_0}{f_2 - f_1}. \tag{1.76}$$

This means that not the absolute phase between node and base station is of interest, but the relative phase difference on two or more carrier frequencies. For a set of carrier frequencies $\{c\Delta f + f_\mathrm{w}\}$ with $c \in [0 \dots C-1]$, the observable phases in a LoS channel are given by

$$\phi_{\mathrm{PoF}c} = -2 \cdot 2\pi(c\Delta f + f_\mathrm{w})\tau + \Delta\tilde{\phi}_\mathrm{R}. \tag{1.77}$$

Range information can be extracted from the slope of the set $\phi_{\mathrm{PoF}c}$ with $c \in [0 \dots C-1]$

$$\widehat{d}_\mathrm{PoF,Slope} = -\frac{c_0}{4\pi\Delta f} \cdot \frac{\Delta\widehat{\phi_{\mathrm{PoF}c}}}{\Delta c} = \tau c_0. \tag{1.78}$$

The typical sub-GHz SRD band channel spacing of 100 kHz results in a range ambiguity of 1500 m. This ambiguity can then be resolved with a time-based method according to (1.74).

While range information can be extracted directly by differentiation in a free-space channel with (1.78), it is also possible to interpret the PoA measurements as the argument of the channel transfer function $H(f)$ at the

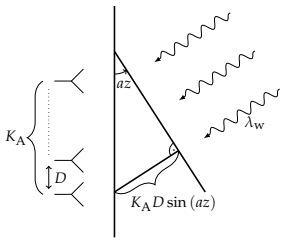


FIGURE 1.19 – *Principle of an electronically steered antenna.*

frequency $c\Delta f + f_w$. Combined with an amplitude estimation of the received signal in the same channel the sampled version of the channel transfer function can be reconstructed. This sampled channel transfer function can be converted to the estimated channel impulse response with the inverse Fourier transform. In multipath radio channels this approach takes into account that phase is not linear over frequency. Range can be estimated by detecting the first path component in the estimated channel impulse response.

Alternatively, the double difference phase measurement from (1.70) can be converted to a double difference distance by determining the number of integer cycles l

$$\widehat{\Delta\Delta d}^{[T_1,T_2,R_i,R_k]} = -c_0 \frac{\Delta\Delta\phi_A^{[T_1,T_2,R_i,R_k]}}{2\pi f_w} + l\lambda_w. \tag{1.79}$$

Estimating this actual number of integer cycles l between the transmitting and receiving node is called integer-ambiguity resolution. This technique is used *e.g.* in the Real-Time Kinematic GPS (RTK-GPS) processing, that is capable to provide centimeter accuracy for positioning [KH06]. With a set of four satellites, the user position can be determined in three dimensions through a TDoA approach, resulting in a location estimate with a ± 2 m error. Adding a reference node of known position to the setup, allows establishing four DPDoA estimates. With a range ambiguity of about 19 cm (see Table 1.8), the unknown number of integer cycles can be constrained to ± 11 solutions by constraining the problem with the time based estimates. An exhaustive search within the resulting $23^4 \approx 300\,000$ possible solutions is computational complex and impractical. Therefore, DPDoA estimates on different frequency bands are used to create larger wavelengths i.e. $\Delta\lambda_{w\,L_1,L_2} \approx 86$ cm. The set of solutions reduces to ± 3 per satellite and $7^4 \approx 3000$ for positioning. The set of solutions is further reduced until only one solution remains due to satellite motion during measurement epochs.

Trying to resolve the integer cycles for LPWA localization is impractical. A LoS channel, for clear phase estimates cannot be guaranteed, base stations are fixed and a network deployment where only a few base stations receive the same node are in contradiction with the requirements for integer cycle resolution.

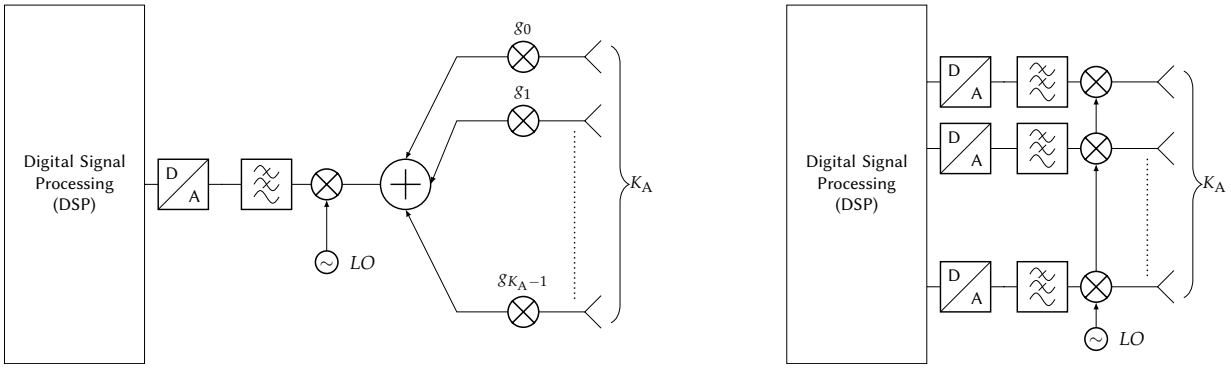
The previously presented amplitude, time and phase based localization metrics provide range information for trilateration techniques. Moreover, phase or in more general, angular information can also lead to triangulation approaches.

1.5.2.9 Angular

Angular information in form of the Direction of Arrival (DoA) or Angle of Arrival (AoA) can be obtained with a directional antenna. Due to the directional radiation pattern of the antenna and depending on the orientation of the emitting node to localize, received power will vary. Rotating the antenna around its axis, will result in a temporally varying received signal strength. The angle at which the received power is maximized corresponds to the AoA. Antenna rotation can be achieved by mechanically rotating the antenna. Mechanically steering the antenna works very well when AoA estimation is required only in one dimension such as in maritime positioning, however when both azimuth and elevation angle are required mechanical rotation becomes complicated.

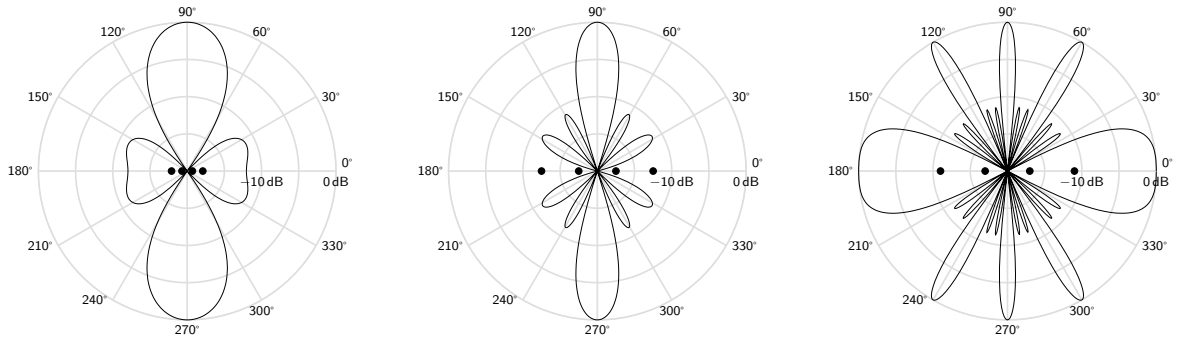
Therefore mechanical rotation in one dimension (horizontal) is combined with an electronically antenna beam steering in the second dimension, or beams are steered fully electronically in both dimensions. Electronically steered antennas further offer the advantage of non-moving hardware. The principle of electronically steered antennas is based on the constructive or destructive combination of the radio signal on multiple antenna elements. It is illustrated in Figure 1.19 with a linear antenna array with K_A antenna elements. Electronic beam steering is explained for the receiving case, however the principle remains valid also in transmission. Depending on the AoA az, the signals received by the adjacent elements are phase shifted by

$$\Delta\phi_A = 2\pi \frac{D}{\lambda_w} \sin(az), \tag{1.80}$$



(a) *Analog.* (b) *Digital.*

FIGURE 1.20 – *Beamforming radio hardware architectures.*



(a) *Element spacing* $D = 0.4\lambda_W$. (b) *Element spacing* $D = 0.75\lambda_W$. (c) *Element spacing* $D = 2.0\lambda_W$.

FIGURE 1.21 – *Azimuth radiation pattern of an antenna array with four omnidirectional elements (black dots).*

with antenna element spacing D.

In order to determine the AoA, the received power of the sum over all antenna element signals r_k needs to be maximized. This can be achieved by appropriately weighting the amplitude and dephasing the received signal of each element with the complex gain g_k as depicted in Figure 1.20a.

Amplitude and phase weighting can be realized by adding on each antenna element an analog amplifier and phase shifter, called analog beam steering/beamforming. Element signals are summed in analog radio frequency domain (see Figure 1.20a). In contrast to this, numerical beamforming requires on each antenna element a complete receiver including radio frequency to intermediate frequency or baseband mixing, and analog to digital conversion. The numerical architecture depicted in Figure 1.20b provides K_A data streams that can be arbitrarily amplitude and phase weighted to steer into different directions. Moreover, sophisticated algorithms such as Multiple Signal Classification (MUSIC) [Sch86] or Estimation of Signal Parameters via Rotational Invariance Technique (ESPRIT) [PRK85; RK89] may take advantage of special signal characteristics for precise AoA estimation. Hybrid architectures of analog and digital beamforming combine advantages of both approaches [Bek+18].

Numerical beamforming relies on a common phase reference for all antenna elements, which can be achieved by feeding all mixers with the same local oscillator signal. Assuming independent but phase synchronized oscillators on each antenna element results in the same architecture as for PDoA with synchronized nodes.

While for PDoA the nodes have an arbitrary distance, antenna array-element spacing is usually chosen to be less than $\lambda_W/2$. This design rule arises from the fact that for $D \geq \lambda_W$ the same signal phase shift corresponds to multiple AoAs leading to angular ambiguities called grating lobes. These grating lobes are characterized by the same amplitude as the main lobes. An illustration for grating lobes with different antenna element spacing is given in Figure 1.21. These ambiguities are identical to the range ambiguities in PDoA. Hence, each grating lobe corresponds to a hyperbole.

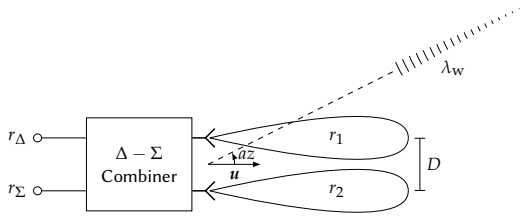


FIGURE 1.22 – *Delta-Sigma monopulse direction finder with passive radio frequency combiner.*

1.5.2.10 Exotic Localization Principles

In the following, some techniques are listed that are special cases of traditional amplitude, time or phase based methods, which use these signal properties in an original manner to provide location information.

Radio Interferometric Localization

In radio interferometric localization [Mar+05] two transmitters simultaneously transmit the same signal (pure sinusoidal) at slightly different frequencies (frequency offsets from independent clock reference are sufficient). At a receiving node, these two signals interfere and after down mixing the envelope of the power of the sum signal varies with the frequency difference of the two nodes. At two receiving nodes at different locations, the envelopes of the received power variations have a phase shift. This phase shift is directly linked to the sum-difference range between the two transmitting and two receiving nodes. This theoretical concept translates range information via phase shifts to received signal strength, easily measurable with radio transceivers. While this technique has been implemented with sinusoidal signals in an interference free environment, the application to modulated signals has not yet been demonstrated.

Delta-Sigma Monopulse Angle of Arrival (AoA) Estimation

Similarly, the so-called Delta-Sigma monopulse approach translates the AoA to an amplitude signal [Sko90]. A two element antenna array as depicted in Figure 1.22 and a passive radio frequency combiner provide the difference r_Δ and sum r_Σ signal of the two antenna signals r_1 and r_2

$$r_\Delta = r_1(t) - r_2(t) = s_0(t)e^{-j(2\pi ft+\phi_R)} - s_0(t)e^{-j(2\pi ft+\phi_R-\Delta\phi_A)}, \tag{1.81a}$$

$$r_\Sigma = r_1(t) + r_2(t) = s_0(t)e^{-j(2\pi ft+\phi_R)} + s_0(t)e^{-j(2\pi ft+\phi_R-\Delta\phi_A)}, \tag{1.81b}$$

where s_0 the baseband waveform. The ratio of the difference to the sum signal yields a waveform independent and constant amplitude signal that varies as function of AoA az

$$\frac{r_\Delta(t)}{r_\Sigma(t)} = \frac{r_1(t) - r_2(t)}{r_1(t) + r_2(t)} = \frac{1 - e^{j\Delta\phi_A}}{1 + e^{j\Delta\phi_A}} = -j\tan\left(\frac{\Delta\phi_A}{2}\right) = -j\tan\left(\frac{\pi D\sin(az)}{\lambda_w}\right), \tag{1.82}$$

with antenna spacing D. This technique is widely used in RADAR direction finding systems [Sko90; Zha+16] due to its simple setup, its robustness and the fact that a single RADAR pulse is sufficient for detection, hence the name monopulse. Extensions with four antennas arranged in a two-by-two array allow both azimuth and elevation/polar angle estimation [Sko90; FJ18].

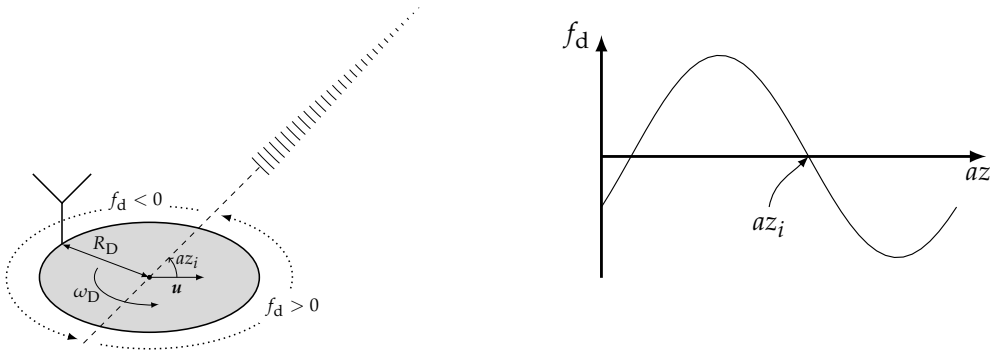
The CRLB on Delta-Sigma Monopulse AoA estimation is given according to Appendix B.3 by

$$\sqrt{\mathrm{Var}\left(\widehat{az}\right)} \geq \sqrt{I_{az}^{-1}} = \sigma\frac{\cos^2\left(\frac{\pi D\sin(az)}{\lambda_w}\right)}{\frac{\pi D\cos(az)}{\lambda_w}} \overset{|az|\ll 2\pi}{\approx} \frac{\sigma\lambda_w}{\pi D}\cos^2\left(\frac{\pi D}{\lambda_w}az\right). \tag{1.83}$$

Assuming small angles close to the broadside $\boldsymbol{u}$, i.e. $|az| \ll 2\pi$ and an antenna spacing $D = \lambda_w/2$ allows evaluating the CRLB. For a r_Δ/r_Σ ratio estimation precision $\sigma = 10\%$, the lower bound on the angle estimation evaluates to $\sqrt{\mathrm{Var}\left(\widehat{az}\right)} \geq 2\sigma/\pi \approx 3.6°$. Considering an even lower precision for σ shows how precise angle estimations with the Delta-Sigma monopulse are possible under LoS conditions. However, the CRLB does not take multipath propagation in urban LPWA scenarios into account which will significantly degrade angular accuracy.

Doppler Direction Finder

The Doppler direction finder principle [LVST08] extracts AoA information from the Doppler signal received by an antenna placed on the edge of a rotating disc as illustrated in Figure 1.23. The AoA corresponds to the axis defined



(a) *Principle.* (b) *Doppler signal as function of AoA.*

FIGURE 1.23 – *Doppler direction finder.*

by the two angular positions of the rotating antenna when the Doppler frequency is zero. The DoA is given by the side where Doppler passes from positive to negative frequency. Variations with a circular placed antenna array where antenna elements are electronically switched in a circular order avoid mechanically moving parts [PO97]. Generalization of the principle to non-circular moving antennas is given in [AW08].

The CRLB is given according to Appendix B.4 by

$$\sqrt{\mathrm{Var}\left(\widehat{az}_i\right)} \geq \sqrt{I_{az_i}^{-1}} = \frac{\sigma}{f_\mathrm{w}} \frac{c_0}{\omega_\mathrm{D} R_\mathrm{D}} \sqrt{\frac{2}{T}}. \tag{1.84}$$

For practical implementation a disc radius $R_\mathrm{D} = \lambda_\mathrm{w}/2$ is assumed. If a Doppler variation $(f_\mathrm{d})_\mathrm{max} = 500\,\mathrm{Hz}$ should be achieved, the minimum rotation speed is given by

$$\omega_\mathrm{D} = \frac{(f_\mathrm{d})_\mathrm{max}\,\lambda_\mathrm{w}}{R_\mathrm{D}} = 2 \cdot 500\,\mathrm{Hz} = 1000\,\mathrm{rad/s}. \tag{1.85}$$

It is hence most convinient to realize rotation at this angular speed by electronical switching. Under the assumption, that the Doppler variation can be estimated with a precision $\sigma = 10\,\mathrm{Hz}$ (equivalent to 10 ppb at $f_\mathrm{w} = 868\,\mathrm{MHz}$), the CRLB on AoA estimation evaluates to $\sqrt{\mathrm{Var}\left(\widehat{az}_i\right)} \geq \sqrt{8} \cdot 10\,\mathrm{Hz}/1\,\mathrm{kHz} \approx 1.6°$. This 1.6° angular precision converts to $\approx 20\,\mathrm{m}$ tangential position error at a distance of 1 km and scales proportional with distance. Although this method is precise, LPWA typical multipath channels will impede accuracy of Doppler Direction finding.

Lighthouse Angle of Arrival (AoA) Estimation Principle

In the lighthouse method [Röm03], a directional, non-divergent beam is rotated around its source as depicted in Figure 1.24. The distance between a receiver/detector and the source can be determined by measuring the time the receiver dwells in the beam T_beam and the time the beam needs for a complete rotation T_turn according to

$$d \overset{d \gg D}{\approx} \frac{D}{2\sin\left[\pi\left(\frac{T_\mathrm{beam}}{T_\mathrm{turn}}\right)\right]}. \tag{1.86}$$

As this method requires non-divergent beams, practical implementations rely on laser beams.

The CRLB is given according to Appendix B.5 by

$$\sqrt{\mathrm{Var}\left(\widehat{d}\right)} \geq \sqrt{I_d^{-1}} \approx \sigma \frac{\pi}{T_\mathrm{turn}} \frac{2d^2}{D}. \tag{1.87}$$

Besided the fact that parallel, non-diverent beams are required, (1.87) reveals, that the ranging error grows with the square of the distance making it impractical for long-range LPWA systems. For numerical evaluation, a lighthouse ranging system with two parallel laser beams of baseline $D = 1\,\mathrm{m}$, a revolution time $T_\mathrm{turn} = 1\,\mathrm{s}$ and a dwell time estimation error $\sigma = 1\,\mu\mathrm{s}$ is considered. The ranging error for a distance $d = 1\,\mathrm{km}$ is bound by

$$\sqrt{\mathrm{Var}\left(\widehat{d}\right)} \geq \sqrt{I_d^{-1}} \approx 1\,\mu\mathrm{s}\,\frac{\pi}{1\,\mathrm{s}}\,\frac{2\,(1\,\mathrm{km})^2}{1\,\mathrm{m}} \approx 6.3\,\mathrm{m}. \tag{1.88}$$

For a 10 km distance the CRLB is given by $\sqrt{\mathrm{Var}\left(\widehat{d}\right)} \geq 630\,\mathrm{m}$ and hence impractical for LPWA localization.

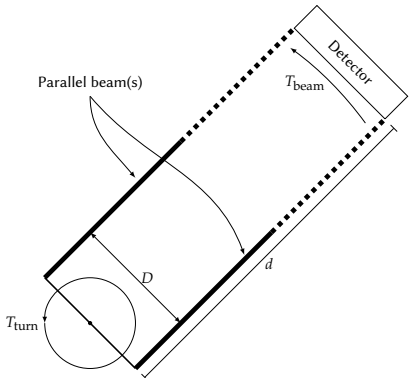


FIGURE 1.24 – *Lighthouse ranging approach requiring parallel beams.*

1.5.3 Ranging and Localization

Localization metrics (see Chapter 1.5.2) provide range, range difference or angle estimates that allow determining position according to the adequate localization technique (see Chapter 1.5.1). Noisy and biased observations of the localization metrics result in errors on range, range difference or angles. These errors translate to errors on position.

In the following, a framework for converting range and range difference errors to position errors is given for circular and hyperbolic trilateration (see Chapter 1.5.1.1).

This framework is then used throughout this thesis to extrapolate the ranging errors obtained by simulation and experimentation, to predict achievable localization precision. Furthermore, this methodology allows comparing the extrapolated localization precision to existing state of the art LPWA localization functions (reviewed in Chapter 1.6).

1.5.3.1 Circular

As introduced in Chapter 1.5.1.1, the observable range between the node of unknown position (x_u,y_u,z_u) and anchor i of defined position (x_i,y_i,z_i) is given by

$$d_{u,i} = \sqrt{(x_u - x_i)^2 + (y_u - y_i)^2 + (z_u - z_i)^2}. \tag{1.89}$$

In the process of acquiring and processing any underlying localization metric, such as RSSI, ToF or Phase of Flight (PoF), the estimated range is given by

$$\widehat{d_{u,i}} = d_{u,i} + n_{\text{Range}_i}, \tag{1.90}$$

with noise n_{Range_i}.

In the following, it is assumed that noise n_{Range_i} is Gaussian distributed with zero mean and variance $\sigma^2_{\text{Range}_i}$. This hypothesis is rather restrictive as it excludes *e.g.* multipath introduced biases (Chapter 2.3). However, this allows to apply the CRLB to transform ranging errors to positioning errors.

For K_{BS} base stations, observation is given by

$$\widehat{\boldsymbol{d}} = \boldsymbol{d} + \boldsymbol{n}_{\text{Range}}, \tag{1.91}$$

with $\widehat{\boldsymbol{d}} = [\widehat{d}_{u,0} \dots \widehat{d}_{u,K_{\text{BS}}-1}]^T$, $\boldsymbol{d} = [d_{u,0} \dots d_{u,K_{\text{BS}}-1}]^T$ and $\boldsymbol{n}_{\text{Range}} = [n_{\text{Range}_0} \cdots n_{\text{Range}_{K_{\text{BS}}-1}}]^T$ with $\boldsymbol{\sigma}^2_{\text{Range}} = \left[\sigma^2_{\text{Range}_0} \cdots \sigma^2_{\text{Range}_{K_{\text{BS}}-1}}\right]^T$.

The variance of the estimated position $\boldsymbol{x}_u = [x_u\, y_u\, z_u]^T$ is bound, according to [Kay93], by

$$\text{Var}(\boldsymbol{x}_u) = \text{Var}\begin{pmatrix} x_u \\ y_u \\ z_u \end{pmatrix} = \begin{pmatrix} \sigma^2_{x_u} \\ \sigma^2_{y_u} \\ \sigma^2_{z_u} \end{pmatrix} \geq \text{diag}\left(\boldsymbol{I}^{-1}_{\boldsymbol{d}}(\boldsymbol{x}_u)\right), \tag{1.92}$$

with Fisher Information Matrix (FIM) $\boldsymbol{I}_{\boldsymbol{d}}(\boldsymbol{x}_u)$ of the range observation $\boldsymbol{d}$ (see Appendix B.6 for full derivation).

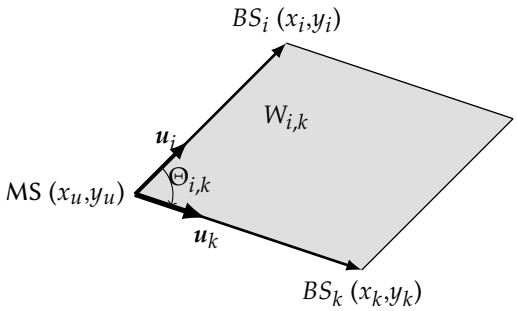


FIGURE 1.25 – *Geometric intepretation of the* $\mathrm{GDoP_c}$.

The Position Error Bound (PEB) is defined as

$$\mathrm{PEB}\left(\boldsymbol{x}_u\right) = \sqrt{\mathrm{trace}\left(\boldsymbol{I}_{\boldsymbol{d}}^{-1}\left(\boldsymbol{x}_u\right)\right)} = \sqrt{\sigma_{x_u}^2 + \sigma_{y_u}^2 + \sigma_{z_u}^2}. \tag{1.93}$$

The analytic PEB expression in a two-dimensional localization scenario derived in [Spi01] is given by

$$\mathrm{PEB}\left(\boldsymbol{x}_u\right) = \sqrt{\frac{\sum_{i=0}^{K_{\mathrm{BS}}-1}\left(\sigma_{\mathrm{Range}_i}\right)^{-2}}{\sum_{i=0}^{K_{\mathrm{BS}}-1}\sum_{k>i}^{K_{\mathrm{BS}}-1}\left(\sigma_{\mathrm{Range}_i}\sigma_{\mathrm{Range}_k}\right)^{-2}\left|\boldsymbol{u}_i \times \boldsymbol{u}_k\right|^2}}, \tag{1.94}$$

with the unit direction vector pointing from the node (x_u, y_u) to anchor i (x_i, y_i)

$$\boldsymbol{u}_i = \frac{1}{d_{u,i}}\begin{pmatrix} x_i - x_u \\ y_i - y_u \end{pmatrix}. \tag{1.95}$$

In the following it is assumed, that all K_{BS} node to base station range estimations have the same error distribution, resulting in $\sigma_{\mathrm{Range}_i} = \sigma_{\mathrm{Range}}$. Hence, (1.94) can be simplified and the PEB becomes a product of range estimation standard deviation σ_{Range} and a purely geometry dependent term called Geometric Dilution of Precision (GDOP)

$$\begin{aligned}\mathrm{PEB} &= \sigma_{\mathrm{Range}}\mathrm{GDoP_c} \\ &= \sigma_{\mathrm{Range}}\sqrt{\frac{K_{\mathrm{BS}}}{\sum_{i=0}^{K_{\mathrm{BS}}-1}\sum_{j>i}^{K_{\mathrm{BS}}-1}\left|\boldsymbol{u}_i \times \boldsymbol{u}_k\right|^2}} \\ &= \sigma_{\mathrm{Range}}\sqrt{\frac{K_{\mathrm{BS}}}{\sum_{i=0}^{K_{\mathrm{BS}}-1}\sum_{k>i}^{K_{\mathrm{BS}}-1} W_{i,k}^2}},\end{aligned} \tag{1.96}$$

with the parallelogram area $W_{i,k}$ spanned by the two unit direction vectors $\boldsymbol{u}_i$ and $\boldsymbol{u}_k$

$$W_{i,k} = \left|\boldsymbol{u}_i \times \boldsymbol{u}_k\right| = \left|\boldsymbol{u}_i\right|\left|\boldsymbol{u}_k\right|\left|\sin\left(\Theta_{i,k}\right)\right|, \tag{1.97}$$

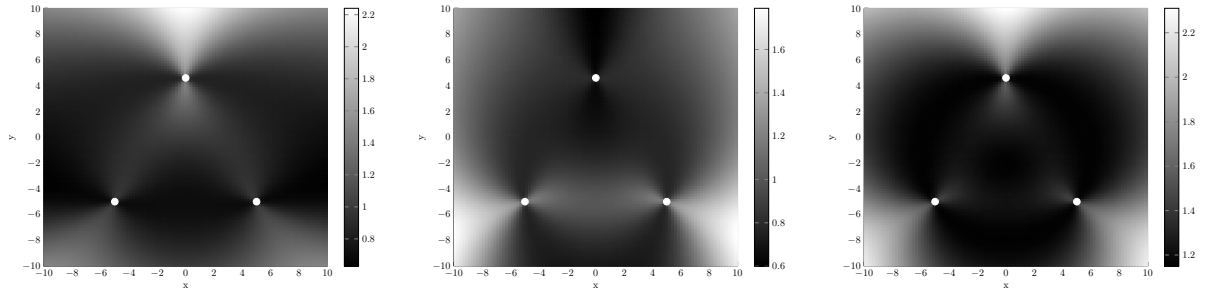
where $\Theta_{i,k}$ the angle between the two direction vectors as illustrated in Figure 1.25.

In order to reduce the PEB, either ranging precision needs to be increased i.e. lower σ_{Range} or the $\mathrm{GDoP_c}$ needs to be decreased. Maximizing all areas $W_{i,k}$ minimizes the $\mathrm{GDoP_c}$, which is achieved when unit vectors $\boldsymbol{u}_i$ and $\boldsymbol{u}_k$ have a maximum angular distance i.e. $\Theta_{i,k} = \pi/2$ [Spi01].

Figure 1.26 illustrates σ_{x_u} and σ_{y_u} normalized to σ_{Range} as well as the $\mathrm{GDoP_c}$ for a minimal base station deployment ($K_{\mathrm{BS}} = 3$).

Low $\mathrm{GDoP_c}$ is achieved for the center point of the equilateral triangle spanned by the three base stations as well as on imaginary half circles where the angular distance is $\pi/2$ (Thales theorem). For minimum $\mathrm{GDoP_c}$, $W_{i,k}$ has to be maximum, which is the case if the base stations i and k are span a $\pi/2$ angle with the node

$$W_{i,k} = \left|\sin(\Theta_i - \Theta_k)\right| = \left|\sin(\frac{\pi}{2})\right| = 1. \tag{1.98}$$



(a) *X-dimension* σ_{x_u}. (b) *Y-dimension* σ_{y_u}. (c) $\mathrm{GDoP_c}$.

FIGURE 1.26 – *GDOP normalized to* σ_{Range} *for circular trilateration for a base station deployment spanning an equilateral triangle (white dots).*

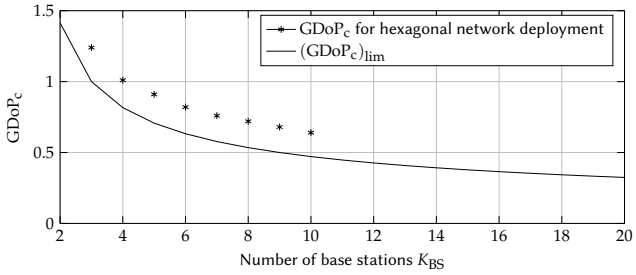


FIGURE 1.27 – $\mathrm{GDoP_c}$ *for hexagonal network deployment [Spi01] and theoretical limit* (1.99).

This assumption is not feasible in a two-dimensional configuration with more than two base stations, as not all angles can be $\pi/2$. It is only considered to find the absolute lower bound

$$\mathrm{GDoP_c} \geq (\mathrm{GDoP_c})_{\mathrm{lim}} = \sqrt{\frac{K_{\mathrm{BS}}}{\sum_{i=0}^{K_{\mathrm{BS}}-1} \sum_{k>i}^{K_{\mathrm{BS}}-1} 1}} = \sqrt{\frac{2}{K_{\mathrm{BS}}-1}}, \tag{1.99}$$

with

$$\sum_{i=0}^{K_{\mathrm{BS}}-1} \sum_{k>i}^{K_{\mathrm{BS}}-1} 1 = \sum_{i=0}^{K_{\mathrm{BS}}-1} K_{\mathrm{BS}} - i = \frac{K_{\mathrm{BS}}(K_{\mathrm{BS}}-1)}{2} = \frac{K_{\mathrm{BS}}!}{(K_{\mathrm{BS}}-2)!2!} = \binom{K_{\mathrm{BS}}}{2}. \tag{1.100}$$

Simulated $\mathrm{GDoP_c}$ values for hexagonal network deployment from [Spi01] as well as $(\mathrm{GDoP_c})_{\mathrm{limit}}$ from (1.99) are plotted in Figure 1.27 as function of the number of base stations K_{BS}.

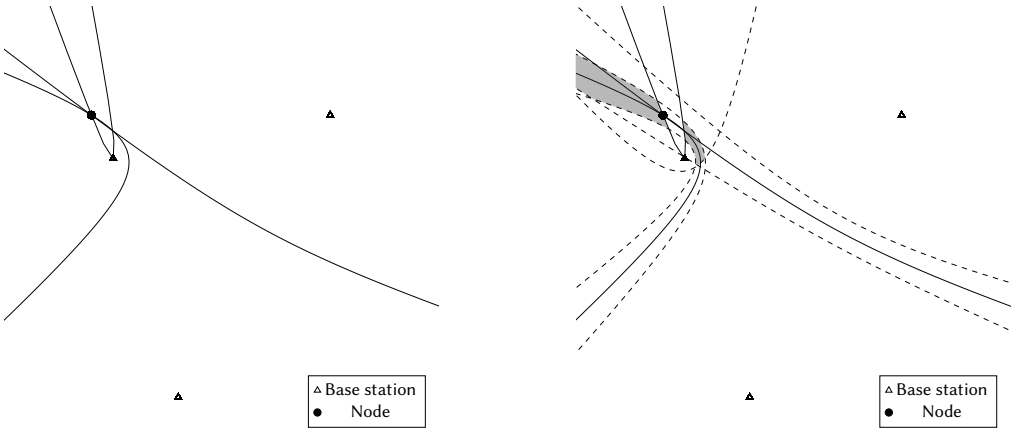
In conclusion, under the hypothesis that all node to base station range estimates are Gaussian zero mean distributed, deploying more base stations does improve the Position Error Bound (PEB) only marginally (factor $2 \ldots 0.5$). However, increasing the number of base stations, increases the chances that there are sufficient precise and unbiased range estimates so that the PEB can be decreased. Selecting the set of range estimates out of all the available estimates that minimizes the position error is achieved with adequate algorithms (see Chapter 1.5.4).

1.5.3.2 Hyperbolic

Analog to the analysis for circular trilateration, the hyperbolic trilateration PEB can be derived from the observation

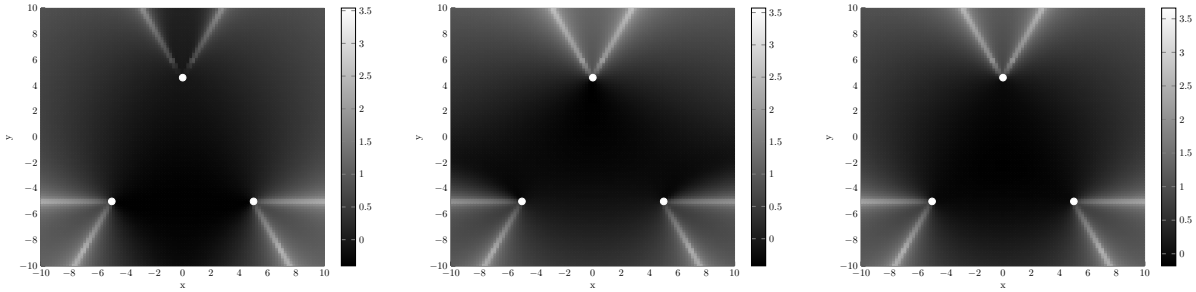
$$\begin{aligned}\widehat{\Delta d_{u,i,k}} &= \Delta d_{u,i,k} + n_{\mathrm{Range}}, \\ &= \sqrt{(x_u - x_i)^2 + (y_u - y_i)^2 + (z_u - z_i)^2} - \sqrt{(x_u - x_k)^2 + (y_u - y_k)^2 + (z_u - z_k)^2} + n_{\mathrm{Range}}.\end{aligned} \tag{1.101}$$

A full analysis including mixed mode between circular and hyperbolic trilateration are discussed in [Spi01]. Figure 1.29 illustrates the hyperbolic trilateration PEB for three base stations on logarithmic scale. Compared to circular trilateration, the achievable precision in the center area improves (see Table 1.9). However, errors for hyperbolic trilateration are increasing drastically outside the area spanned by the base stations as illustrated in Figure 1.28.



(a) *Perfect range difference estimation.* (b) *With range difference estimation errors.*

FIGURE 1.28 – *Hyperbolic trilateration in two dimensions for a node outside the area spanned by the base stations.*



(a) *X-dimension* $10\log_{10}\left(\sigma_{x_u}\right)$. (b) *Y-dimension* $10\log_{10}\left(\sigma_{y_u}\right)$. (c) $10\log_{10}\left(\mathrm{GDoP_h}\right)$.

FIGURE 1.29 – *GDOP normalized to* $10\log_{10}\left(\sigma_{\mathrm{Range}}\right)$ *for hyperbolic trilateration for a base station deployment spanning an equilateral triangle (white dots), considering all possible range difference measurements.*

$(\mathrm{GDoP_c})_{\min}$		1.15
$(\mathrm{GDoP_h})_{\min}$	Range differences only with respect to the serving base station	0.92
	All range differences	0.67

TABLE 1.9 – *Minimum achievable GDOP for circular and hyperbolic trilateration (in two dimensions).*

This position error bound analysis has shown that precise and accurate range estimates are required to achieve precise localization. Providing such precise and accurate range estimates is the aim of this thesis and investigated in Chapter 3, Chapter 4 and Chapter 5.

1.5.4 Introduction to Location Solving Algorithms

Localization metrics presented in the previous section provide the input to location solving algorithms that according to a localization model, estimate position based on these metrics. For a known anchor, i.e. base station setup $(\boldsymbol{x}_0, \ldots, \boldsymbol{x}_{K_{\mathrm{BS}}-1})$, the set of localization metrics $\mathcal{M}_i(\boldsymbol{x}_u)$ depends on the actual user position $\boldsymbol{x}_u$ according to a given model $\mathcal{M}$. This model depends on the used localization metric (see Chapter 1.5.2). A basic approach to estimate position $\widehat{\boldsymbol{x}_u}$, aims at minimizing the error between the set of measured localization metrics $\widehat{\mathcal{M}_i}$ and the model. The problem can be formulated as weighted least squares minimization problem

$$\widehat{\boldsymbol{x}_u} = \arg\min_{\boldsymbol{x}_u} \sum_i w_i \left| \widehat{\mathcal{M}_i} - \mathcal{M}_i(\boldsymbol{x}_u) \right|^2, \tag{1.102}$$

with weights w_i. These weights can take the reliability of the corresponding localization metric measurement into account. Weights can be deduced *e.g.* from the SNR or an indicator for a biased single link ranging measurement (see Chapter 4.3.2). Various algorithms exist in literature to solve this optimization problem.

1.6 LPWA Network Localization

1.6.1 Existing Localization Solutions for LPWA Networks

In the previous sections, Low Power Wide Area (LPWA) technologies and localization techniques have been introduced. The following section brings these two fields together by giving a state of the art overview on LPWA localization techniques and systems from both a scientific and a product or service point of view.

1.6.1.1 Sigfox

The Sigfox service providers offers a geolocation service called "SpotIt" [Sig17]. The geolocation functionality is based on a fingerprinting method utilizing the uplink Received Signal Strength Indicator (RSSI). In order to enhance precision of the estimated position, complex machine-learning algorithms are employed. Due to the highly variable propagation scenarios, errors will be about 1 km − 10 km according to Sigfox [Sig17]. Semi-parametric models achieve a 2 km − 4 km mean error for RSSI-based localization [BPE18]. Because of long transmission times, the number of packets per day is very limited, leading to an equally low number of position estimates. This almost excludes continuous tracking and any form of filtering over multiple location estimates.

Sigfox equally holds patents [SF13; SF16] for time based localization techniques. It is however hardly possible to achieve accurate time-based positioning with signal bandwidths of 100 Hz resulting, according to (1.43), in a $c_0\sqrt{\mathrm{Var}\left(\widehat{t_\mathrm{A}}\right)} \approx 26\,\mathrm{km}$ at $E_\mathrm{b}/N_0 = 10\,\mathrm{dB}$ and a 4 bytes preamble.

Extensive RSSI kNN-fingerprinting studies [ABBW18] have shown that mean location estimation errors around 700 m are achievable. The results are however, sensitive to the available training set and vary depending on the propagation scenario (i.e. rural/urban). Relying on some geo-referenced nodes equipped with a GNSS module allows constructing and updating the fingerprinting training set with sophisticated machine learning algorithms. Positioning accuracy in such a setup can be significantly improved [SCRP19].

1.6.1.2 LoRa

The 868 MHz LoRa technology employs signal bandwidths between 7.8 kHz and 500 kHz. For the typical configuration of 125 kHz, a theoretical ToA precision of $c_0\sqrt{\mathrm{Var}\left(\widehat{t_\mathrm{A}}\right)} \approx 15\,\mathrm{m}$ is achievable at $E_\mathrm{b}/N_0 = 10\,\mathrm{dB}$ combining 6 symbols of each 12 bit for ToF or TDoA localization techniques. Compared to Sigfox where time base positioning remains impractical, the LoRa technology is compatible with both RSSI and ToF/TDoA based localization techniques. Semtech holds patents for both RSSI [Pen17a] and time based localization [Pen17b; Pen18; Sel14; Sel18]. Due to the possibility to send packets at a higher rate and hence of shorter duration than for Sigfox, tracking and filtering become options to enhance the positioning performances. The LoRa Alliance [LoR18] gives a summary of geolocation implementations. For RSSI based positioning a 1 km − 2 km accuracy is announced. In [ABVVW18] RSSI kNN fingerprinting has equally been applied to a LoRa data set. Mean errors are as low as 400 m, and the discrepancy with the Sigfox performances is explained by the difference in the data set sizes.

In a mesh network topology, with an average internode distance of only 20 m, RSSI based localization achieves positioning errors as low as 8 m [GJ18]. While applicable to specific application scenarios with small internode distance, errors scale with distance in LPWA deployments, see CRLB for RSSI in (1.37).

TDoA localization is most adapted to the star-of-stars LoRaWAN topology. Base station synchronization is achieved via GNSS, allowing to time stamp received packets with a GNSS timing precision of about 20 ns. Field trials [LoR18] indicate accuracies between 20 m − 200 m in 90% of the cases, depending on the propagation scenario. In an urban geolocation enabled public LoRa network [Pod+18] errors are smaller than 480 m in 90% of the cases.

In order to further improve ranging accuracy, Semtech provides a version of the LoRa technology with higher bandwidths (406 kHz-1625 kHz) at the trade-off of degraded receiver sensitivity [Sem17b]. The SX1280 chip operates in the ISM 2.4 GHz band, where more bandwidth per channel is available. However, free-space propagation attenuation increases and obstacle penetration degrades, which results in less long-range connectivity (see Chapter 2.3.9).

1.6.1.3 Narrow-Band IoT

NB-IoT supports positioning since the 3GPP Release 14. The positioning technique is based on TDoA measurements in downlink operation. A NB-IoT node observes the TDoAs of several pairs of synchronized base stations emitting special designed Positioning Reference Signals (PRSs). These TDoAs are used by the node to calculate its position with a hyperbolic trilateration technique.

A design target for a 50 m horizontal positioning accuracy has been specified in Release 14 and simulations assuming perfect network synchronization achieve less than 150 m in 90% of the cases [Lin+17]. Simulations of TDoA based positioning in static and mobile scenarios report errors between 30 m and 300 m for Extended Pedestrian A (EPA) and Extended Typical Urban (ETU) channel models respectively. Depending on the channel model, outliers up to 2 km are possible [Rad+17]. Specifically designed algorithms improve positioning precision despite the limited temporal resolution due to low analog radio front end sampling frequency [HBLR17].

A NB-IoT compatible System on Chip (SoC) implementation with TDoA capability achieves a positioning accuracy of 100 m [Kor+18].

1.6.1.4 IEEE 802.15.4k

No specific work concerning ranging and localization exists for the IEEE 802.15.4k standard. However, due to the signal bandwidth of 200 kHz, performances comparable to NB-IoT localization are expectable. Work concerning the IEEE 802.15.4 (ZigBee) standard [PSSV09a; Sch11] is reviewed in Chapter 1.6.2.

1.6.1.5 GNSS Tracker

Due to the low accuracy of localization features based on the inherent LPWA radio signals, presented in the previous section, highly accurate positioning is currently only achievable by adding supplementary systems such as a GNSS receiver that can provide precise location estimates. At the expense of an increased power consumption and more hardware on the device, meter-level accuracy is possible in outdoor environments with clear sky vision. For seamless outdoor-indoor localization other modalities such as UWB localization in indoor environments overcome the unavailability of GNSS signals indoors [CL].

1.6.1.6 WiFi Sniffing

"Wireless Fidelity" (WiFi) proximity methods can overcome the drawbacks of GNSS based LPWA localization in terms of energy consumption and limitation to outdoor environements. For this purpose LPWA nodes integrate a WiFi module that allows monitoring nearby WiFi Access Points (APs) and their respective RSSI. To keep energy consumption at a minimum, the WiFi module does not connect to the networks, but only sniffs their Basic Service Set Identifiers (BSSIDs). The LPWA node of which position is to be estimates, sends over the LPWA radio link BSSID and RSSI information to the network. In an offline mapping step a database with WiFi APs and their location is created. The online step determines position of the LPWA node based on the measured WiFi AP RSSIs. The upper positioning error limit is theoretically given by the coverage of WiFi and field trials achieve an 39 m mean error [JWB17].

1.6.2 New Localization Candidates for LPWA Networks

Either the reviewed localization features for LPWA technologies rely on inherent radio signals allowing low-power, low-complexity implementation at the expense of accuracy or they require additional hardware to provide precise positioning information. Low signal bandwidth and complex propagation scenarios are hence the main challenges for accurate LPWA localization. These challenges are formalized and studied in detail in Chapter 2.

Currently research pursues two complementary approaches in order to improve LPWA localization accuracy:

- Collecting as much radio metrics as possible and applying sophisticated algorithms such as machine learning and Deep Neural Network (DNN) algorithms to the data to extract precise position information.
- Provide new radio metrics that offer improved localization precision.

According to the ToA CRLB in (1.43), more bandwidth improves ToA estimation precision. Thereby it is insignificant whether bandwidth is available instantaneously, *e.g.* UWB systems or sequentially while respecting certain conditions. Step Frequency RADARs (SF-RADARs) combine large processing bandwidths while maintaining narrower instantaneous bandwidth, which relaxes the requirement for wideband analog to digital conversion [Sko90].

A general signal model framework for sequential multi-channel ranging with active transmissions instead of passive RADAR reflections integrating CFO and adapted estimation algorithms being asymptotically efficient are proposed by [Kaz+18; KRJd19].

The idea of sequential multi-channel ranging has been applied to short-range communication technologies where applied frequency hopping schemes cover the total available bandwidth *e.g.* 80 MHz in the ISM 2.4 GHz band while instantaneously transmitting in a much narrower channel. Prominent examples are scientific demonstrations

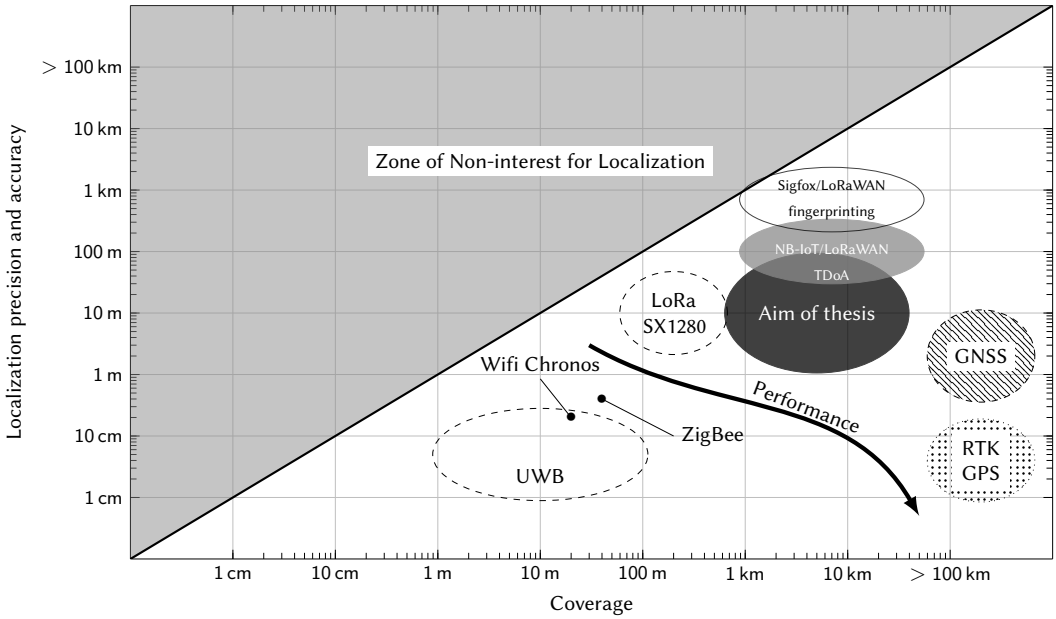


FIGURE 1.30 – *Positioning accuracy/precision and coverage of localization techniques from Table 1.10.*

with Radio Frequency Identification (RFID) [PS11], ZigBee [PSSV09a; Sch11], WiFi [VKK16] or commercial, proprietary implementations such as the Atmel [Atm13; Atm14] or Nanotron [Nan] chips.

In the case of RFID communication, a tag is sequentially interrogated on different frequencies. Decimeter-level accuracy has been achieved by covering a total virtual bandwidth of 26 MHz at a communication range of 2.4 m. Due to the instantaneous and possibly passive response from RFID tags, the setup is very similar to radar systems that rely on passive reflection of the electromagnetic waves.

The same principle of frequency hopping has been applied to indoor ZigBee standard compliant communication in a differential setup with a transmitter of unknown location, a reference transmitter for anchor synchronization and multiple receiving anchors [PSSV09a; Sch11]. The work focuses on carrier frequency offset mitigation and investigates how performances are influenced by multipath propagation. A commercial ZigBee transceiver [Atm13] implements a ranging feature based on the Phase of Flight (PoF) principle, however the ranging signals within the ZigBee packets are not compliant with the standard.

The WiFi Chronos implementation [VKK16] adopts a multi-channel phase coherent PoF approach between commodity WiFi cards. The implementation covers a virtual bandwidth of up to 2.6 GHz as both the ISM 2.4 GHz band and the Industrial, Scientific and Medical (ISM) 5 GHz band are utilized. PoF ranging performances improve by a factor 30 compared to time base ranging and a 0.5 m error is achieved in indoor scenarios.

Nanotron [Nan] provides a proprietary communication and localization feature based on Chirp Spread Spectrum (CSS) modulation covering the total 80 MHz of the ISM 2.4 GHz band. Nanotron claims a 1 m accuracy for ranges up to 500 m.

The key system parameters such as frequency band, bandwidth, sensitivity as well as ranging performances are summarized in Table 1.10.

Figure 1.30 illustrates the localization performances, i.e. positioning accuracy/precision and the corresponding system coverage for each technology.

In conclusion, all these practical implementations and proprietary solutions focus on short-range communication and no adaptation to LPWA transmissions is yet available. However, the listed implementations demonstrate the potential of multi-channel phase coherent ranging/localization with the PoA metric. Accuracy is improved by overcoming constrains of limited instantaneous bandwidth with a virtual increased bandwidth by sequential frequency hopping.

1.7 Conclusions

LPWA networks are key enablers for IoT applications that require long-range wireless connectivity combined with stringent energy consumption limitations. Applications such as smoke detectors, distant temperature sensors or water meters have only a few payload bytes to transmit. This allows employing narrowband or low spectral efficiency modulation schemes to attain low levels of receiver sensitivity required for long-range communication

	Band	B	P_{req}	**Localization metric**	**Ranging/ Localization error**	**Remark**
Unit	n/a	Hz	dBm	n/a	m	n/a
Sigfox						
Spot'It [Sig17]	SRD 868	100	−144	RSSI Fingerprinting	1000 − 10 000	▪ Machine learning
Aernouts [ABBW18]	SRD 868	100	−144	RSSI Fingerprinting	700	▪ Sensitive to training data set size and propagation environment
LoRa						
LoRa Alliance [LoR18]	SRD 868	$125 \cdot 10^3$	−147	RSSI Ranging	1000 − 2000	
LoRa Alliance [LoR18]	SRD 868	$125 \cdot 10^3$	−147	TDoA Ranging	20 − 200	▪ GNSS synchronized base stations
Public Network [Pod+18]	SRD 868	$125 \cdot 10^3$	−147	TDoA ranging	480	▪ Commercial available base stations
Aernouts [ABVVW18]	SRD 868	$125 \cdot 10^3$	−147	RSSI Fingerprinting	400	
Konica Minolta [GJ18]	SRD 868	$125 \cdot 10^3$	−147	RSSI Ranging	8	▪ Mesh setup ▪ Maximum distance between nodes < 20 m
SX1280 chip [Sem17a]	ISM 2400	$406.25 \cdot 10^3$	−122	ToF Ranging	< 5	▪ Spreading factor $m = 10$ ▪ Requires a two-way packet exchange ▪ 170 m distance ▪ Includes frequency hopping and averaging
NB-IoT [Rad+17]	Licensed	180 kHz	−160	TDoA	30 − 300	▪ Downlink ▪ Simulation (EPA/ETU channel model)
NB-IoT [Lin+17]	Licensed	180 kHz	−160	TDoA	150	▪ Simulation ▪ Perfect network synchronization ▪ 46 dBm transmit power
NB-IoT [Kor+18]	Licensed	180 kHz	−160	TDoA	100	▪ SoC implementation
GNSS Tracker i.e. based on [Ubl]	Licensed	n/a	n/a	TDoA, PDoA	< 1	▪ Extra hardware: GNSS module ▪ Clear sky visibility required
WiFi Sniffer [JWB17]	SRD 868	n/a	n/a	RSSI Fingerprinting/ Ranging	39	▪ Extra hardware: WiFi module
802.11.4k						
Zigbee [PSSV09a]	ISM 2400	$2 \cdot 10^6$	?	TDoA	2	▪ 9 m distance ▪ Virtual bandwidth 80 MHz ▪ 16 channels
				PDoA	0.2	
ATMEL [SZW15]	ISM 2400	?	?	PoF	1.63	▪ 50 m distance
RFID [PS11]	ISM 900	?	?	PDoA	0.14	▪ Virtual bandwidth 26 MHz ▪ 100 channels ▪ 2.4 m distance
WiFi						
Wifi Chronos [VKK16]	ISM 2400+5000	$40 \cdot 10^6$	?	ToF	15	▪ Virtual bandwidth 2.6 GHz ▪ 15 m distance
				PoF	0.5	
Nanotron [Nan]	ISM 2400	$80 \cdot 10^6$	−97	ToF Ranging	1	

TABLE 1.10 – *Overview on the state of the art on LPWA localization and new candidates (? indicate unknown information).*

respecting low-power requirements. Many of the cited IoT applications require positioning information, *e.g.* for tracking purposes or for geo-tagging data produced by the sensors.

Localization techniques in this context can be compared based on their accuracy, precision, availability, complexity, cost, deployment requirements and power consumption. Although GNSSs offer high accuracy and precision, they are limited to outdoor applications and they considerably increase complexity, cost and power consumption on LPWA enabled sensor nodes. For these reasons it is preferable to take advantage of the transmitted radio signals carrying sensor information. An overview on different radio signal based positioning techniques and their requirements is given.

RSSI based methods are straightforward to implement on LPWA networks without supplementary complexity, cost and power consumption. However, RSSI measurements vary largely with actual propagation conditions, *e.g.* blockage and fading, yielding poor positioning performance in large scale LPWA networks. Current RSSI based positioning solutions achieve approximately 500 m error in urban city setups.

Accuracy and precision can be improved when using time based methods. Typically, errors down to 200 m in real environments are achieved. The lack of large signal bandwidths for good time resolution is one of the main limitations of time based techniques. Low temporal resolution results in a limited capability to resolve multipath for accurate delay estimation. In order to achieve long-range communication, instantaneous bandwidth is intrinsically small on LPWA transceivers and hence precise positioning challenging.

In order to overcome this bandwidth limitation, phase based techniques allow combining multiple sequentially

transmitted narrowband signals to a virtually increased bandwidth. This method has proven to provide significant precision improvements compared to time based techniques when applied to various radio solutions and standards.

The application of multi-channel ranging in the LPWA context yet remains open and is the subject of this thesis.

Bibliography of Chapter 1

[3GP15] 3GPP. *3GPP Release 12*. http://www.3gpp.org/specifications/releases/68-release-12. 2015.

[3GP16] 3GPP. *3GPP Release 13*. https://www.3gpp.org/release-13. 2016.

[Abr70] N. Abramson. "THE ALOHA SYSTEM: another alternative for computer communications". In: *Proceedings of the November 17-19, 1970, fall joint computer conference*. ACM. 1970, pp. 281–285.

[Act] Actility. *Carrier grade IoT connectivity platform to manage your LoRaWAN/LPWA networks and build IoT solutions*. https://www.actility.com/. Accessed: 2020/07/31.

[ABBW18] M. Aernouts, B. Bellekens, R. Berkvens, and M. Weyn. "A Comparison of Signal Strength Localization Methods with Sigfox". In: *2018 15th Workshop on Positioning, Navigation and Communications (WPNC)*. 2018, pp. 1–6.

[ABVVW18] M. Aernouts, R. Berkvens, K. Van Vlaenderen, and M. Weyn. "Sigfox and LoRaWAN Datasets for Fingerprint Localization in Large Urban and Rural Areas". In: *Data* 3.2 (2018), p. 13.

[AW08] A. Amar and A. J. Weiss. "Localization of Narrowband Radio Emitters Based on Doppler Frequency Shifts". In: *IEEE Transactions on Signal Processing* 56.11 (2008), pp. 5500–5508.

[Ang+12] M. Angermann et al. "Characterization of the Indoor Magnetic Field for Applications in Localization and Mapping". In: *2012 International Conference on Indoor Positioning and Indoor Navigation (IPIN)*. 2012, pp. 1–9.

[Ash+13] R. Ashkar et al. "A Low-Cost Shoe-Mounted Inertial Navigation System with Magnetic Disturbance Compensation". In: *International Conference on Indoor Positioning and Indoor Navigation*. 2013, pp. 1–10.

[Atm13] Atmel. *Atmel AVR2152: RTB Evaluation Application Software User's Guide*. Accessed: 2020/07/31. Feb. 2013.

[Atm14] Atmel. "System, method, and circuit for distance measurement between two nodes of a radio network". Pat. 8,644,768. 2014.

[Bek+18] M. R. Bekkar et al. "Constant modulus hybrid beamforming for multi-user systems in the presence of blockers". In: *2018 25th International Conference on Telecommunications (ICT)*. 2018, pp. 378–382.

[BP17] M. Bertanha and R. W. Pazzi. "JLPR: Joint Range-Based Localization Using Trilateration and Packet Routing in Wireless Sensor Networks with Mobile Sinks". In: *2017 IEEE Symposium on Computers and Communications (ISCC)*. 2017, pp. 645–650.

[BPE18] P. Bianchi, F. Portier, and K. Elgui. "A semi parametric model for RSSI-based localization, Modele semi parametrique pour la localisation par RSSI". In: (2018).

[CL] CEA-Leti. *Hyloc - Une plateforme materielle embarquee flexible, analyse des algorithmes de surveillance de mouvement et de localisation multimodale*. http://www.leti-cea.fr/cea-tech/leti/Pages/innovation-industrielle/Demonstrateurs/HYLOC.aspx. Accessed: 2020/07/31.

[CEP18] CEPT. *ERC Recommendation 70-03*. Aug. 2018.

[Chu72] D. Chu. "Polyphase Codes With Good Periodic Correlation Properties (Corresp.)" In: *IEEE Transactions on Information Theory* 18.4 (1972), pp. 531–532.

[dBLD19] A. P. da Silva, I. H. Brahmi, S. Leirens, and B. Denis. "System-level Simulation of Cooperative Sensor Data Fusion Strategies for Improved Vulnerable Road Users Safety". In: *16th Workshop on Positioning, Navigation and Communications (WPNC)*. 2019.

[Eff] Effigis. *The Smart City And The Importance Of The "Where"*. https://www.effigis.com/en/smart-city-importance-of-the-where/. Accessed: 2020/07/31.

[Enc] Encyclopaedia Britannica. *Sextant*. https://www.britannica.com/technology/sextant-instrument. Accessed: 2020/07/31.

[Enc12] Encyclopaedia Britannica. *Calculating the Distance to a Lightning Strike*. 2012. URL: http://blogs.britannica.com/2012/07/calculating-the-distance-to-a-lightning-strike/.

[FZH62] R. Frank, S. Zadoff, and R. Heimiller. "Phase Shift Pulse Codes With Good Periodic Correlation Properties (Corresp.)" In: *IRE Transactions on Information Theory* 8.6 (1962), pp. 381–382.

[FJ18] H. Frid and B. L. G. Jonsson. "Determining Installation Errors for DOA Estimation with Four-Quadrant Monopulse Arrays by Using Installed Element Patterns". In: *2018 2nd URSI Atlantic Radio Science Meeting (AT-RASC)*. 2018, pp. 1–4.

[Fri46] H. T. Friis. "A Note on a Simple Transmission Formula". In: *Proceedings of the IRE* 34.5 (1946), pp. 254–256.

[GR17] O. Georgiou and U. Raza. "Low Power Wide Area Network Analysis: Can LoRa Scale?" In: *IEEE Wireless Communications Letters* 6.2 (2017), pp. 162–165.

[Gha+18] G. Ghatak et al. "Positioning Data-Rate Trade-Off in mm-Wave Small Cells and Service Differentiation for 5G Networks". In: *2018 IEEE 87th Vehicular Technology Conference (VTC Spring)*. 2018, pp. 1–5.

[GJ18] P. Gotthard and T. Jankech. "Low-Cost Car Park Localization Using RSSI in Supervised LoRa Mesh Networks". In: *2018 15th Workshop on Positioning, Navigation and Communications (WPNC)*. 2018, pp. 1–6.

[Gro13] P. D. Groves. *Principles of GNSS, Inertial, and Multisensor Integrated Navigation Systems*. Artech House, 2013.

[Guo+11] S. Guo et al. "A novel density-based geolocation algorithm for a noncooperative radio emitter using power difference of arrival". In: *Wireless Sensing, Localization, and Processing VI*. Vol. 8061. International Society for Optics and Photonics. 2011, 80610E.

[Hat80] M. Hata. "Empirical Formula for Propagation Loss in Land Mobile Radio Services". In: *IEEE Transactions on Vehicular Technology* 29.3 (1980), pp. 317–325.

[He+03] T. He et al. "Range-Free Localization Schemes For Large Scale Sensor Networks". In: *Proceedings of the 9th annual international conference on Mobile computing and networking*. ACM. 2003, pp. 81–95.

[HBLR17] S. Hu, A. Berg, X. Li, and F. Rusek. "Improving the Performance of OTDOA Based Positioning in NB-IoT Systems". In: *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*. 2017, pp. 1–7.

[HFJK19] C. Hungar, J. Fricke, S. Juergens, and F. Koester. "Detection of Feature Areas for Map-based Localization Using LiDAR Descriptors". In: *16th Workshop on Positioning, Navigation and Communications (WPNC)*. 2019.

[IEE13] IEEE. "IEEE Standard for Local and metropolitan area networks— Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)—Amendment 5: Physical Layer Specifications for Low Energy, Critical Infrastructure Monitoring Networks." In: *IEEE Std 802.15.4k-2013 (Amendment to IEEE Std 802.15.4-2011 as amended by IEEE Std 802.15.4e-2012, IEEE Std 802.15.4f-2012, IEEE Std 802.15.4g-2012, and IEEE Std 802.15.4j-2013)* (2013), pp. 1–149.

[Ing] Ingenu. *Random Phase Multiple Access (RPMA)*. https://www.ingenu.com/. Accessed: 2020/07/31.

[JWI11] B. Jackson, S Wang, and R Inkol. "Emitter geolocation estimation using power difference of arrival". In: *Defence R&D Canada Technical Report DRDC Ottawa TR* 40 (2011), p. 51.

[JABW18] T. Janssen, M. Aernouts, R. Berkvens, and M. Weyn. "Outdoor Fingerprinting Localization Using Sigfox". In: *2018 International Conference on Indoor Positioning and Indoor Navigation (IPIN)*. 2018, pp. 1–6.

[JWB17] T. Janssen, M. Weyn, and R. Berkvens. "Localization in Low Power Wide Area Networks Usering Wi-Fi Fingerprints". In: *Applied Sciences* 7.9 (2017), p. 936.

[Jim+16] E. Jimenez et al. "Investigation on Radio Wave Propagation in Shallow Seawater: Simulations and Measurements". In: *2016 IEEE Third Underwater Communications and Networking Conference (UComms)*. 2016, pp. 1–5.

[KH06] E. Kaplan and C. Hegarty. *Understanding GPS: Principles and Applications*. Second Edition. Artech House, 2006.

[Kay93] S. M. Kay. *Fundamentals of Statistical Signal Processing: Estimation Theory*. 1993.

[KRJd19] T. Kazaz, R. T. Rajan, G. J. M. Janssen, and A. v. der Veen. "Multiresolution Time-of-arrival Estimation from Multiband Radio Channel Measurements". In: *ICASSP 2019 - 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. 2019, pp. 4395–4399.

[Kaz+18] T. Kazaz et al. "Joint Ranging and Clock Synchronization for Dense Heterogeneous IoT Networks". In: *2018 52nd Asilomar Conference on Signals, Systems, and Computers*. 2018, pp. 2169–2173.

[Kor+18] M. Korb et al. "A Dual-Mode NB-IoT and EC-GSM RF-SoC Achieving -128-dBm Extended-Coverage and Supporting OTDOA and A-GPS Positioning". In: *ESSCIRC 2018 - IEEE 44th European Solid State Circuits Conference (ESSCIRC)*. 2018, pp. 286–289.

[Lac+17] D. Lachartre et al. "A TCXO-Less 100Hz-Minimum-Bandwidth Transceiver for Ultra-Narrow-Band Sub-GHz IoT Cellular Networks". In: *2017 IEEE International Solid-State Circuits Conference (ISSCC)*. 2017, pp. 134–135.

[LRV11] R. Lacoste, M. Robiolle, and X. Vital. *L'ecoconception en electronique*. Dunod, 2011.

[Lao+18] C. Laoudias et al. "A Survey of Enabling Technologies for Network Localization, Tracking, and Navigation". In: *IEEE Communications Surveys Tutorials* 20.4 (2018), pp. 3607–3644.

[Las14] T. Lassen. *White paper: Long-range RF communication: Why narrowband is the de facto standard*. Texas Instruments. 2014.

[LVST08] A. Ledeczi, P. Volgyesi, J. Sallai, and R. Thibodeaux. "A Novel RF Ranging Method". In: *2008 International Workshop on Intelligent Solutions in Embedded Systems*. 2008, pp. 1–12.

[Lei15] E. Leitinger. "Cognitive Indoor Positioning and Tracking using Multipath Channel Information". PhD thesis. Graz University of Technology, 2015.

[Lia+18] F. Liang et al. "A Survey on Big Data Market: Pricing, Trading and Protection". In: *IEEE Access* 6 (2018), pp. 15132–15154.

[Lin+17] X. Lin et al. "Positioning for the Internet of Things: A 3GPP Perspective". In: *IEEE Communications Magazine* 55.12 (2017), pp. 179–185.

[Lon19] Longman. *Longman Dictionary of Contemporary English Online*. 2019. URL: https://www.ldoceonline.com/.

[LoR18] LoRaAlliance. *Geolocation Whitepaper*. https://lora-alliance.org/resource-hub/lora-alliance-geolocation-whitepaper. Accessed: 2020/07/31. 2018.

[Loy99] M. Loy. *Understanding and Enhancing Sensitivity in Receivers for Wireless Applications*. Texas Instrument, Wireless Communication Business Unit, Technical Brief SWRA030. 1999.

[MDDU17] J. Maceraudi, F. Dehmas, B. Denis, and B. Uguen. "Multipath-Aided Direct Path ToA Reconstruction for Integrated UWB Receivers in Generalized NLoS". In: *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)*. 2017, pp. 1–5.

[Mar+05] M. Maróti et al. "Radio Interferometric Geolocation". In: *Proceedings of the 3rd international conference on Embedded networked sensor systems*. ACM. 2005, pp. 1–12.

[McL97] B. McLarnon. "VHF/UHF/microwave radio propagation: A primer for digital experimenters". In: *TAPR/ARRL Digital Communications Conference*. 1997.

[Mei14] P. Meissner. "Multipath-Assisted Indoor Positioning". PhD thesis. Graz University of Technology, 2014.

[MS15] M. V. Moreno and A. F. Skarmeta. "An Indoor Localization System Based on 3D Magnetic Fingerprints for Smart Buildings". In: *The 2015 IEEE RIVF International Conference on Computing Communication Technologies - Research, Innovation, and Vision for Future (RIVF)*. 2015, pp. 186–191.

[Nan] Nanotron. *Location-Aware IoT Sensors*. https://nanotron.com/. Accessed: 2020/07/31.

[NCAC18] A. Navarro, W. Cruz, C. Amu, and Y. Castano. "Broadcast Emitters Localization Using Power Difference of Arrival". In: *2018 IEEE MTT-S Latin America Microwave Conference (LAMC 2018)*. 2018, pp. 1–3.

[NGM15] NGMN 5G Initiative. *5G White Paper*. 2015.

[NN01] D. Niculescu and B. Nath. "Ad Hoc Positioning System (APS)". In: *GLOBECOM'01. IEEE Global Telecommunications Conference (Cat. No.01CH37270)*. Vol. 5. 2001, 2926–2931 vol.5.

[Obj] Objenious Bouygues Telecom. *Le Reseau Dedie Aux Objets Connectes*. https://objenious.com/reseau/. Accessed: 2020/07/31.

[OSMD18] M. N. Ochoa, L. Suraty, M. Maman, and A. Duda. "Large Scale LoRa Networks: From Homogeneous to Heterogeneous Deployments". In: *2018 14th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. 2018, pp. 192–199.

[Pal+16] M. R. Palattella et al. “Internet of Things in the 5G Era: Enablers, Architecture, and Business Models”. In: *IEEE Journal on Selected Areas in Communications* 34.3 (2016), pp. 510–527.

[PRK85] A. Paulraj, R. Roy, and T. Kailath. “Estimation Of Signal Parameters Via Rotational Invariance Techniques- Esprit”. In: *Nineteeth Asilomar Conference on Circuits, Systems and Computers, 1985*. 1985, pp. 83–89.

[PO97] D. Peavey and T. Ogumfunmi. “The Single Channel Interferometer Using a Pseudo-Doppler Direction Finding System”. In: *1997 IEEE International Conference on Acoustics, Speech, and Signal Processing*. Vol. 5. 1997, 4129–4132 vol.5.

[Pen17a] M. Peng. “System And Method For Robust And Accurate RSSI Based Location Estimation”. Pat. 3 173 807. 2017.

[Pen17b] M. Peng. “System And Method For Robust And Efficient TDOA Based Location Estimation In The Presence Of Various Multipath Delay”. Pat. 3 173 809. 2017.

[Pen18] M. Peng. “Positioning System And Method With Multipath Mitigation”. Pat. 404 440. 2018.

[PSSV09a] M. Pichler, S. Schwarzer, A. Stelzer, and M. Vossiek. “Multi-Channel Distance Measurement With IEEE 802.15.4 (ZigBee) Devices”. In: *IEEE Journal of Selected Topics in Signal Processing* 3.5 (2009), pp. 845–859.

[Pod+18] N. Podevijn et al. “TDoA-Based Outdoor Positioning with Tracking Algorithm in a Public LoRa Network”. In: *Wireless Communications and Mobile Computing* (2018).

[PS11] A. Povalac and J. Sebesta. “Phase Difference of Arrival Distance Estimation for RFID Tags in Frequency Domain”. In: *2011 IEEE International Conference on RFID-Technologies and Applications*. 2011, pp. 188–193.

[Pro01] J. G. Proakis. *Digital Communications*. Ed. by F. Edition. McGraw-Hill Higher Education, 2001.

[Rad+17] K. Radnosrati et al. “Performance of OTDOA Positioning in Narrowband IoT Systems”. In: *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*. 2017, pp. 1–7.

[RKS17] U. Raza, P. Kulkarni, and M. Sooriyabandara. “Low Power Wide Area Networks: An Overview”. In: *IEEE Communications Surveys Tutorials* 19.2 (2017), pp. 855–873.

[Röm03] K. Römer. “The Lighthouse Location System for Smart Dust”. In: *Proceedings of the 1st international conference on Mobile systems, applications and services*. ACM. 2003, pp. 15–30.

[Rot17] Y. Roth. “The Physical Layer for Low Power Wide Area Networks: A Study of Combined Modulation and Coding Associated with an Iterative Receiver”. PhD thesis. Université Grenoble Alpes, 2017.

[RK89] R. Roy and T. Kailath. “ESPRIT-Estimation of Signal Parameters Via Rotational Invariance Techniques”. In: *IEEE Transactions on Acoustics, Speech, and Signal Processing* 37.7 (1989), pp. 984–995.

[SCRP19] H. Sallouha, A. Chiumento, S. Rajendran, and S. Pollin. “Localization in Ultra Narrow Band IoT Networks: Design Guidelines and Trade-Offs”. In: *IEEE Internet of Things Journal* (2019), pp. 1–1.

[Sch86] R. Schmidt. “Multiple Emitter Location and Signal Parameter Estimation”. In: *IEEE Transactions on Antennas and Propagation* 34.3 (1986), pp. 276–280.

[SZW15] Y. Schröder, G. von Zengen, and L. Wolf. “Poster: NLOS-aware Localization Based on Phase Shift Measurements”. In: *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*. ACM. 2015, pp. 224–226.

[SVPS08] S. Schwarzer, M. Vossiek, M. Pichler, and A. Stelzer. “Precise distance measurement with IEEE 802.15.4 (ZigBee) devices”. In: *2008 IEEE Radio and Wireless Symposium*. 2008, pp. 779–782.

[Sch11] S. Schwarzer. “Entwicklung eines industriellen Funkortungssystems basierend auf der kohaerenten Kombination von Kommunikationssignalen mit IEEE-802.15.4-Geraeten”. PhD thesis. Technischen Universitaet Clausthal, 2011.

[Sel14] O. Seller. “Ranging and Positioning System”. Pat. 2 767 847. 2014.

[Sel16] O. Seller. “Low Complexity, Low Power And Long Range Radio Receiver”. Pat. 3 264 622. 2016.

[Sel18] O. Seller. “Method And System Of Timing And Localizing A Radio Signal”. Pat. 3 273 607. 2018.

[SF13] L. Sellier and C. Fourtet. “Procede De Synchronisation De Mesures De Temps Realisees Dans Un Reseau De Radiocommunication Aux Fins De Geolocalisation”. Pat. 2986680. 2013.

[SF16] L. Sellier and C. Fourtet. "Method For Synchronizing Time Measurements Carried Out In A Radio Communication Network For Geolocation Purposes". Pat. 9341701. 2016.

[Sem15] Semtech. *Application Note: LoRa Modulation Basics*. 2015.

[Sem16] Semtech. *SX1276/77/78/79 - 137 MHz to 1020 MHz Low Power Long Range Transceiver*. http://www.semtech.com/images/datasheet/sx1276.pdf. Accessed: 2020/07/31. Aug. 2016.

[Sem17a] Semtech. *Application Note: An Introduction to Ranging with the SX1280 Transceiver*. 2017.

[Sem17b] Semtech. *SX1280/SX1281 Long Range, Low Power, 2.4 GHz Transceiver with Ranging Capability*. 2017.

[Sha48] C. Shannon. "A Mathematical Theory of Communication". In: *The Bell System Technical Journal* 27.3 (1948), pp. 379–423.

[Sig] Sigfox. *Sigfox, a 0G Network*. https://www.sigfox.com/. Accessed: 2020/07/31.

[Sig17] Sigfox. *Sigfox Spot'it, the simplest and most efficient IoT location service*. https://www.sigfox.com/en/sigfox-spot-it. 2017.

[Sil16] Silicon Labs. *High-Performance, Low-Current Transceiver: Si4464/63/61/60*. 2016.

[Sim+06] Y. Simard et al. "Development and experimentation of a satellite buoy network for real-time acoustic localization of whales in the St. Lawrence". In: *OCEANS 2006*. 2006, pp. 1–6.

[Sit17] Y. L. Sit. "MIMO OFDM Radar-Communication System with Mutual Interference Cancellation". PhD thesis. Karlsruhe Institute of Technology, 2017.

[Sko90] M. Skolnik. *Radar Handbook*. 2nd ed. McGrawHill, 1990.

[SA87] J. Smith and J. Abel. "Closed-Form Least-Squares Source Location Estimation From Range-Difference Measurements". In: *IEEE Transactions on Acoustics, Speech, and Signal Processing* 35.12 (1987), pp. 1661–1669.

[Spi01] M. A. Spirito. "On the Accuracy of Cellular Mobile Station Location Estimation". In: *IEEE Transactions on Vehicular Technology* 50.3 (2001), pp. 674–685.

[STM16] STMicroelectronics. *S2-LP Ultra-low power, high performance, sub-1GHz transceiver*. http://www.st.com/content/ccc/resource/technical/document/datasheet/group3/bd/26/62/81/3d/86/4d/15/DM00339133/files/DM00339133.pdf/jcr:content/translations/en.DM00339133.pdf. Nov. 2016.

[TKL11] Y. Taniguchi, T. Kitani, and K. Leibnitz. "A uniform airdrop deployment method for large-scale wireless sensor networks". In: *International Journal of Sensor Networks* 9.3-4 (2011), pp. 182–191.

[Tex16] Texas Instruments. *CC1125 Ultra-High Performance RF Narrowband Transceiver*. http://www.ti.com/lit/ds/swrs120e/swrs120e.pdf. 2016.

[The] The Things Network. *Building a global open LoRaWAN network*. https://www.thethingsnetwork.org/. Accessed: 2020/07/31.

[Ubl] Ublox. *High precision GNSS performance for the mass market: NEO-M8P series*. https://www.u-blox.com/en/product/neo-m8p-series. Accessed: 2020/07/31.

[Uni] University Grenoble Alpes. *Need for IoT - Anticipate and support sustainable transition in nanoelectronic industry*. https://need.univ-grenoble-alpes.fr/. Accessed: 2020/07/31.

[VT04] H. L. Van Trees. *Detection, Estimation, and Modulation Theory*. John Wiley and Sons, 2004.

[VKK16] D. Vasisht, S. Kumar, and D. Katabi. "Decimeter-Level Localization with a Single WiFi Access Point". In: (2016).

[VFF19] C. Villien, A. Frassati, and B. Flament. "Evaluation of An Indoor Localization Engine". In: *2019 International Conference on Indoor Positioning and Indoor Navigation (IPIN)*. 2019, pp. 1–8.

[Wei] Weightless. *Weightless*. http://www.weightless.org/. Accessed: 2020/07/31.

[Wd15] F. Wolf and S. de Rivaz. *Characterisation of the Long Range (LoRa) technology's physical layer and medium access control layer study of a demonstrator Long Range Wide Area Network (LoRaWAN)*. Tech. rep. Commissariat a l'energie atomique et aux energies alternatives (CEA) Centre de Grenoble - France, 2015.

[Zha+16] Y.-X. Zhang et al. "A novel monopulse angle estimation method for wideband LFM radars". In: *Sensors* 16.6 (2016), p. 817.

[Zhu+18] Y. Zhuang et al. “A Survey of Positioning Systems Using Visible LED Lights”. In: *IEEE Communications Surveys Tutorials* 20.3 (2018), pp. 1963–1988.

[ZVL17] K. Zoubert-Ousseni, C. Villien, and F. Le Gland. “Post-processing optimization of piecewise indoor trajectories based on IMU and RSS measurements”. In: *2017 International Conference on Indoor Positioning and Indoor Navigation (IPIN)*. 2017, pp. 1–8.

2

Challenges for LPWA Radio Based Positioning

"But still try for who knows what is possible!"

– Michael Faraday (1791 – 1867)

Chapter contents

Radio signal based localization for Low Power Wide Area (LPWA) systems faces particular challenges, including system limitations, hardware specificities and impairments. Moreover, radio propagation channels impede positioning performances. In this chapter, limited signal bandwidth, topology of LPWA networks and clock offset implications on localization are investigated. Further, the impact of the radio channel, i.e. multipath propagation on the performances of wireless positioning techniques is studied. Based on these considerations, the arising research questions are outlined and the coverage of the present thesis is motivated.

2.1 System Level Challenges

2.1.1 Narrowband LPWA Waveforms

Low Power Wide Area (LPWA) technologies apply low data rate transmission schemes in order to achieve low levels of receiver sensitivity and hence long-range communication. Practical implementations of LPWA transceivers combine the low data rate with narrowband or even Ultra-Narrow Band (UNB) waveforms [Sem16; Sig].

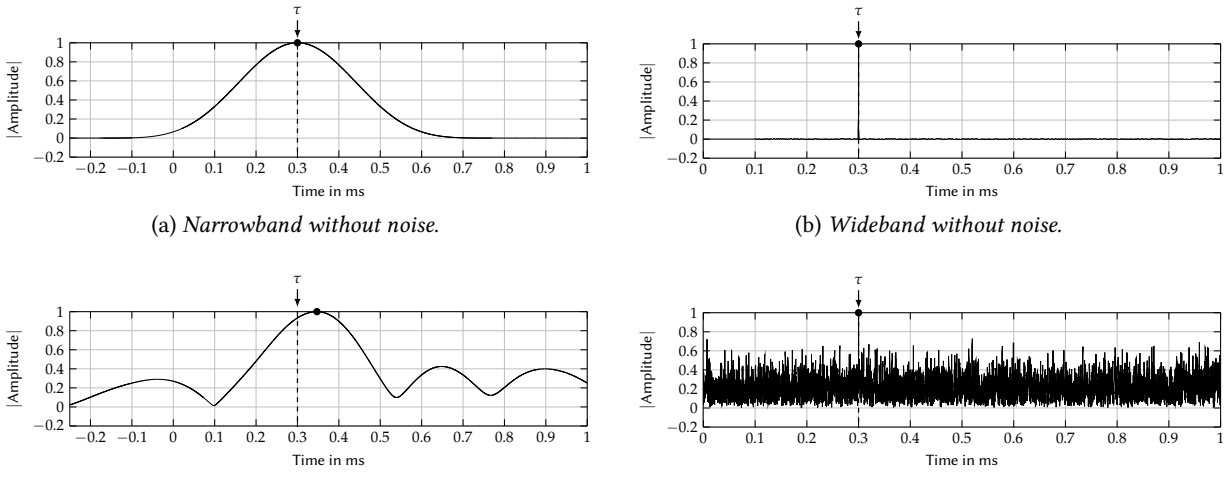
Narrowband signals are hence well localized in frequency domain, resulting in a degraded ability to localize them in time domain, impeding precision of time based positioning techniques.

Ultra-Wide Band (UWB) technologies, in contrast, use large signal bandwidths, i.e. at least 500 MHz or bandwidths larger than 20% of the carrier frequency f_W as defined *e.g.* by the Federal Communications Commission (FCC) [Fed02]. Excellent ranging precisions on the centimeter-level are achievable with UWB [Dec15]. However, communication range is limited to a few 100 m due to insufficient receiver sensitivity of typically $\approx -106\,\text{dBm}/500\,\text{MHz}$ [Dec15] and regulation constraints limiting the transmit Power Spectral Density (PSD) [Fed02].

Figure 2.1 illustrates the matched filter correlation output for a 2 kHz narrowband (Figure 2.1a, Figure 2.1c) and a wideband (Figure 2.1b, Figure 2.1d) pulse of 1 MHz bandwidth with a delay τ. In the absence of noise, the delay can be estimated in both cases through maximum peak detection. However, in a channel with Additive White Gaussian Noise (AWGN), peak detection might be erroneous due to noise. The resulting delay estimation error depends on the symbol energy to noise spectral density E_S/N_0. Further, the error is proportional to the width of the pulse and hence inverse proportional to the pulse bandwidth (see CRLB (1.43)).

It can be concluded from this illustration, that narrowband waveforms enabling long-range communication for LPWA networks, are contradictory requirements to precise radio signal based localization, requiring large bandwidths for time resolution.

However, for improved precision, signal bandwidth can be increased. Simultaneously lowering spectral efficiency *e.g.* through spreading codes (see Chapter 1.2.1.3), ensures that the receiver sensitivity (1.9) is maintained. This approach is nevertheless limited by transceiver complexity and power consumption increasing with bandwidth. Nonetheless, multi-user access to the radio resource, is often realized not only with Frequency Division Multiple Access (FDMA) but also with Code Division Multiple Access (CDMA) techniques that increase bandwidth. Multi-user access and larger bandwidth for improved ranging precision can hence be combined.



(a) *Narrowband without noise.*

(b) *Wideband without noise.*

(c) *Narrowband with noise.*

(d) *Wideband with noise.*

Figure 2.1 – *Delay estimation: Matched filter output (–), real delay τ (- - -) and delay estimation (•).*

Ranging precision can moreover be improved according to the Cramer Rao Lower Bound (CRLB) from (1.43) through increased Signal to Noise Ratio (SNR). This can be achieved with longer sequences, *e.g.* by performing Time of Arrival (ToA) estimation on the entier preamble or even include the payload part into the ToA estimation process [Sit+11; Sit17].

2.1.2 Stationary and Mobile Nodes

Depending on the application scenario, a LPWA node will have various mobility profiles, reaching from purely static to highly mobile nodes. Thus, the challenges for LPWA localization vary with node mobility:

- **Stationarity**: A fixed node is once placed and does not change position during its lifetime, *e.g.* a water meter. Combining location estimates over long intervals allows improving positioning precision through temporal averaging and by the rejection of biased outliers, *e.g.* due to temporal blockage by a vehicle in the Line of Sight (LoS) path between the node and the base station.

  The challenge lies in the design of appropriate averaging and rejection algorithms under the hypothesis of a stationary node and a possibly varying environment. Rejection techniques classify *e.g.* ranging measurements as biased due to None Line of Sight (NLoS) propagation. No range information is hence available, however the rejection can be taken into account in the location solving process through proper weighting (see Chapter 1.5.4).

- **Changing location**: A static node that changes position from time to time. Application data is only relevant for the stationary phases, *e.g.* an intelligent dustbin.

  Positioning algorithms that combine multiple estimates, as for the stationary case, need to detect location changes in order to reinitialize correctly.

- **Continuous mobility**: The application induces a continuously changing node position. Application data is constantly generated, *e.g.* for object tracking. Time varying radio channels (see Chapter 2.3) complicate radio signal based localization. Position estimation in tracking applications often relies on *e.g.* Kalman filtering [KH06], requiring continuous inputs to the filter in order to obtain location estimations. In the LPWA context, duty cycle limitations (see Chapter 2.1.5) impose a limited number of payload messages. This makes it difficult to exploit the statistics and physics of successive position estimates. In the case of a moving Sigfox node, allowed to transmit 140 messages per day, position between successive transmissions has totally changed and such filtering cannot be applied.

  The challenge hence consists in jointly optimizing position-tracking precision and the required number of packet exchanges, hence power consumption, while respecting radio regulation limitations.

LPWA localization is best suited for stationary nodes and those that change position from time to time, offering position information while conserving low-power operation. Continuous mobility applications can gain single position estimates through LPWA localization, however tracking is most likely realized with Global Navigation Satellite System (GNSS) based solutions providing high precision at the expense of increased power consumption.

2.1.3 Time Reference and Network Topology

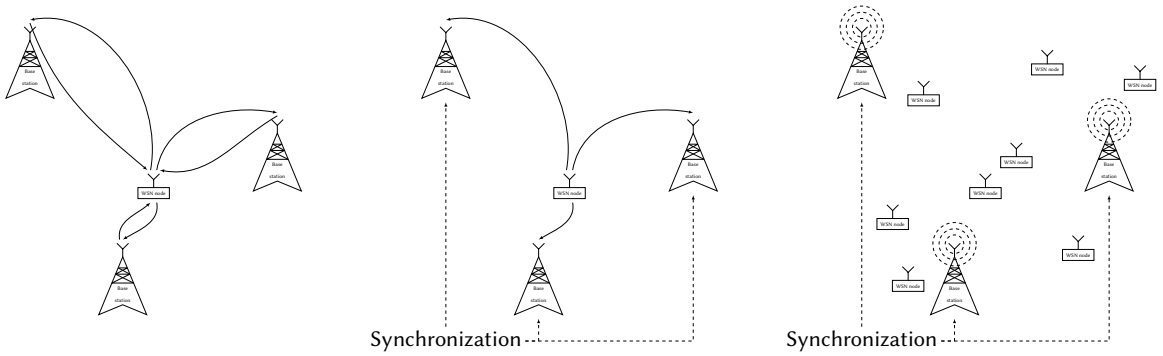
Usually LPWA networks operate in an asynchronous manner, i.e. base stations and nodes are not synchronized, do not share a common time basis, i.e. clock source and transmissions are not aligned to fixed time frames as it is the case for cellular communication.

In order to eliminate the unknown time reference t_0, a two-way packet exchange according to Figure 1.16b and (1.48) can be applied. For two-dimensional circular localization in Figure 2.2a, this requires three two-way exchanges with at least three base stations. This in turn increases time on air and hence power consumption. It should be noted that in the case of two-way ranging, the LPWA node must be capable of estimating ToA, which is not always compatible with existing LPWA chipsets, *e.g.* [Sem16];

Hyperbolic trilateration based on Time Difference of Arrival (TDoA) estimates, offers the advantage of less packets to be exchanged at the expense of synchronized base stations. This synchronization can be assumed through the network backbone i.e. fiber optic connection, GNSS based time synchronization [LoR18] or through a so-called reference node of known position (see Figure 1.17b).

TDoA based systems can be operated in both uplink and downlink direction depending on where location information is required, on the Medium Access Control (MAC) layer and on the processing capacity of the node.

Uplink message based localization as depicted in Figure 2.2b is most suited for nodes asynchronously transmitting their data packet to available base stations while being otherwise in low-power sleep mode. The



(a) *Circular two-way.* (b) *Hyperbolic uplink.* (c) *Hyperbolic downlink/broadcast.*

FIGURE 2.2 – *Network topologies for LPWA localization.*

hardware architecture of the node can be kept simple and existing LPWA technologies are compatible as required processing is exclusively performed on the base station side. Drawback of uplink localization is that the number of localizable nodes is limited to those nodes that are simultaneously received by at least three base stations in the case of two-dimensional localization. Just as for communication, inter-node interference issues grow with the number of nodes due to the asynchronous radio access. Systems such as GNSS positioning perform localization in downlink direction (see Figure 2.2c) and overcome these types of interference problems. A finite set of satellites, analog to base stations, transmits localization signals that can be received by an unlimited number of GNSS receivers that thereupon determine their position. The unlimited number of supported devices is traded of against an increased complexity of the receivers which require to acquire and track multiple satellites simultaneously and perform location solving algorithms [KH06] which results in a notably increased power consumption compared to LPWA transceivers (see Table 1.3).

Sigfox nodes will be limited to uplink localization, as nodes always have to initiate communication. Base stations require a precise and up to date estimation of the actual Carrier Frequency Offset (CFO), so that a downlink message lies within the receive filter of the node (see Chapter 1.2.2.1). Consequently, Sigfox does not propose a broadcasting mode necessary for downlink localization as depicted in Figure 2.2c.

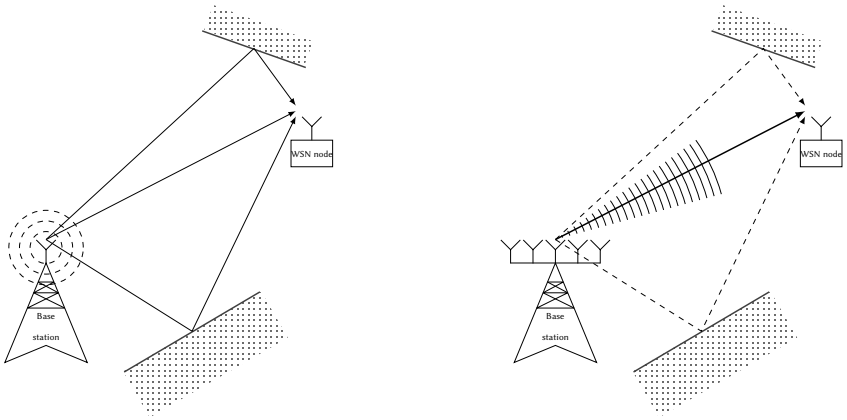
The Long-Range Wide Area Network (LoRaWAN) specification defines three device classes [Lor]:

- **Class A**: Default class supported by all devices. Nodes initiate communication in asynchronous manner. After an uplink message, the nodes opens two reception windows for downlink messages. This is the lowest power class and it is most adapted for uplink localization.
- **Class B**: Besides class A operation, nodes are synchronized to the base station by periodic beacons. The node opens scheduled reception windows guaranteeing a defined downlink latency. In this mode, downlink localization is feasible. However, current LoRa chipsets [Sem16] do not allow to receive multiple base stations simultaneously, as do GNSS receivers.
- **Class C**: Nodes are in continuous reception when not transmitting. Besides a reduced latency and an increased power consumption, implications for localization are the same as for class B.

The decision on uplink or downlink localization can also be viewed from the energy consumption perspective. While uplink localization requires only a packet to be transmitted, downlink positioning requires reception and numerical processing to determine location. Hence, if node power consumption is of primary concern, transmit consumption has to be compared to receive plus processing power consumption (see Table 1.3).

2.1.4 Antenna and Antenna Array Form Factor Constraints

Omnidirectional propagation typically results in multipath scenarios due to various reflections of the emitted signal in the surrounding environment. Figure 2.3a illustrates such a scenario. Definition and in-depth study of radio channels and the arising challenges for localization is given in Chapter 2.3. In contrast to omnidirectional antennas, directional antennas or beamforming allow implementing spatial filtering techniques to reduce the impact of multipath propagation as depicted in Figure 2.3b. In general, directional antennas antenna arrays for beamforming are larger than omnidirectional antennas. The higher the directivity, the larger the antenna needs to be.



(a) *Omnidirectional propagation.* (b) *Directive propagation.*

FIGURE 2.3 – *Multipath propagation and mitigation through beamforming.*

Due to the form factor constraints of LPWA nodes and their generally unknown orientation with respect to the base station, nodes have an omnidirectional antenna. As a result, the node captures radio signals from all directions including both, multipath reflections of the useful base station signal but also interference from other communication signals. Implementing beamforming and Angle of Arrival (AoA) estimation techniques is limited hence to the base station side, where the size of antenna arrays, associated hardware and processing is not in contradiction with cost, power consumption and form factor integration constraints of nodes. Beamforming possibly improves localization performances due to the reduction of multipath propagation and the limitation of interferences outside the main beam. As base stations do not have prior information on the node position, they need to start the positioning process with an omnidirectional configuration and refine the search space iteratively.

2.1.5 Legal Regulation Limitations

Another system level challenge are legal regulation constraints. Radio regulation has two main purposes. Firstly, legal limitations aim to protect from hazardous radio transmissions by restricting *e.g.* the maximum radiated power or the ratio of active and inactive intervals, i.e. the duty cycle. Secondly, legislation sets a framework for the coordination of the electromagnetic spectrum. By assigning different parts of the spectrum to different usages and operators, it aims reducing interference and to guarantee to each user a fair access to the spectrum resource.

Table 2.1 summarizes the main aspects from Short-Range Device (SRD), Industrial, Scientific and Medical (ISM) and licensed band regulation relevant for LPWA networks. The European Conference of Postal and Telecommunications Administrations (CEPT) defines license free SRD and ISM bands that are mainly characterized through a limited maximum transmit power and a low duty cycle or Listen Before Talk (LBT) techniques to control the access to the radio resource. In the licensed bands, operators are permitted to transmit with higher power, as interference is avoided through a centralized network coordination.

In terms of radio regulation, the SRD 868 MHz band and ISM 2.4 GHz band as well as the licensed bands are most interesting for localization purposes, as they offer large bands, required for sufficient time resolution for precise localization (see Chapter 2.1.1 and Chapter 2.3.6.2).

2.1.6 Comparison of LPWA and GNSS Operation Conditions

It is interesting to compare LPWA localization to GNSS positioning and its operation conditions to understand why legacy GNSS can achieve meter-level positioning precision and why LPWA localization with these levels of precision remains challenging.

Link budgets of Sigfox, LoRa and Global Positioning System (GPS) signals are for this purpose compared in Table 2.2. The considered LPWA and GNSS propagation scenarios, i.e. distance d and blockage/fading, are typical and chosen such that received power levels are comparable. This is equally reflected by the typical GNSS receiver sensitivity levels as low as $-160\,\mathrm{dBm}$ [Ubl], which is comparable to the best LPWA receiver sensitivities (see Table 1.1).

The theoretical ranging precision (1.43) hence depends mainly on signal bandwidth, as E_b/N_0 levels are comparable assuming integration durations only over a single symbol. Table 2.2 shows that GNSS achieves best ranging precision while Sigfox time based ranging is practically impossible due to UNB communication.

Frequency band	**Band in** MHz	**Channel bandwidth**	$(P_t)_{max}$ ERP	**Access techniques**
ISM 169 MHz				
CEPT A_1, f_1 Non-specific short range devices	169.400 – 169.475 (75.0 kHz)	≤ 50 kHz	27 dBm	≤ 1% duty cycle or LBT
CEPT A_1, f_4 Non-specific short range devices	169.400 – 169.4875 (87.5 kHz)	n/a	10 dBm	≤ 0.1% duty cycle or LBT
CEPT A_2, b Tracking, data acquisition	169.400 – 169.475 (75.0 kHz)	≤ 50 kHz	27 dBm	≤ 10% duty cycle
ISM 433 MHz				
CEPT A_1, g_1 Non-specific short range devices	433.050 – 434.790 (1.74 MHz)	n/a	10 dBm	≤ 10% duty cycle or LBT
CEPT A_1, g_3 Non-specific short range devices	434.040 – 434.790 (750.00 kHz)	≤ 25 kHz	10 dBm	n/a
SRD 868 MHz				
CEPT $A_1, h_{1.1}/h_{1.2}/h_{1.3}$ Non-specific short range devices	863.000 – 870.000 (7 MHz)	≤ 100 kHz	14 dBm	≤ 0.1% duty cycle or LBT or ≤ 1% duty cycle if 865.000 – 878.000 MHz
CEPT A_2, d_1 Tracking, data acquisition	865.000 – 868.000 (3 MHz)	≤ 200 kHz	27 dBm +APC	≤ 10% duty cycle if access point, else ≤ 2.5% duty cycle
CEPT A_3, a Wideband transmissions	863.000 – 868.000 (5 MHz)	≤ 1 MHz	14 dBm	≤ 10% duty cycle if access point, else ≤ 2.8% duty cycle
NB-IoT/LTE 900 MHz				
ETSI/3GPP	*e.g.* 880.000 – 915.000 (35 MHz)	180 kHz	≤ 33 dBm	licensed
ISM 2400 MHz				
CEPT A_1, i Non-specific short range devices	2400.0 – 2483.5 (83.5 MHz)	n/a	10 dBm EIRP	n/a
CEPT A_3, b Wideband transmissions	2400.0 – 2483.5 (83.5 MHz)	n/a	20 dBm EIRP	*e.g.* LBT

TABLE 2.1 – *Overview on SRD, ISM [CEP18] and licensed band [ETS17] regulation relevant for LPWA network applications.*

Localization precision for GNSS is further improved in the presence of clear LoS links between satellites in the sky and the receiver. Whereas LPWA propagation channels are generally horizontally oriented and are impacted by strong multipath and blockage in urban environments (see Chapter 2.3). GNSS receivers attain high precision due to continuously tracking multiple satellites that allows profiting from satellite movement, to smooth temporal variations and to detect outliers, i.e. by excluding low quality satellite signals from the location solving process. Continuous operation of LPWA transceivers and dense network deployment for improved positioning performances are contrary to long-range and power consumption constraints.

	Sigfox 868 MHz	**LoRa** 868 MHz	**GPS C/A** L_1 1575 MHz
Transmit power P_t	14 dBm		44 dBm
Transmit antenna gain G_t	0 dBi		13.4 dBi
Friis free-space loss (1.1)	−31.2 dB−72 dB ($d = 4$ km)		−36.4 dB−146 dB ($d = 20\,200$ km)
	−40 dB (Blockage/fading) (arbitrary chosen, but realistic in the LPWA context)		−4 dB (Atmospheric/polarization mismatch loss)
Receive antenna gain G_r	0 dBi		
Receive power P_r	−129.3 dBm		−129.1 dBm
Data rate R	100 bit/s	0.366 kbit/s ($m = 12$)	1 kbit/s
Noise figure N_F	6 dB		
Receive E_b/N_0	18.7 dB	13.1 dB	8.9 dB
Bandwidth B	100 Hz	125 kHz	1023 kHz
Ranging precision $c_0\sqrt{\mathrm{Var}\left(\widehat{t_A}\right)}$ (assuming a single symbol for estimation)	> 55 km	84.4 m	16.8 m

TABLE 2.2 – *Link budget comparison for LPWA technologies and GNSS.*

2.2 Hardware Dependent Challenges

Besides system-imposed limitations to precise LPWA positioning, hardware impairments and constraints are equally limiting localization performances.

2.2.1 Clock Impairments

Digital systems require a clock source that sequences the different processing steps. For wireless communication, clock sources are further used to derive analog signals such as waveform and carrier. An ideal clock source produces regular oscillations characterized by the oscillation period T_w or frequency f_w, linked by

$$f_w = \frac{1}{T_w}. \tag{2.1}$$

The signal s_{LO} of a sinusoidal oscillator can be given in complex notation by

$$s_{LO}(t) = e^{j\phi(t)}, \tag{2.2}$$

where oscillator phase ϕ is given by the temporal integration of instantaneous carrier frequency $f_w(t)$ and simplifies for an ideal oscillator with $f_w(t) = f_w$ to

$$\phi(t) = 2\pi \int_0^t f_w(\gamma)\, d\gamma = 2\pi f_w t. \tag{2.3}$$

Real oscillators however have various impairments and actual phase can be modeled by

$$\phi(t) = 2\pi \int_0^t f_w \left(1 + \delta_f + \delta'_f(\gamma)\right) d\gamma + \phi_{PN}(t). \tag{2.4}$$

The different contributions and impairments in (2.4) are given by:

- **Ideal frequency** f_w is the nominal defined frequency of the oscillator.
- **Relative frequency offset** δ_f is a time invariant discrepancy to the nominal frequency. Such a frequency offset arises if the oscillator is not calibrated. Aging effects are slow variations over time intervals much larger than time duration required for transmission and reception. In the following, they are therefore considered as a constant frequency offset.
- **Relative frequency drift** $\delta'_f(t)$ is the short term variation of the oscillator frequency due to power supply variations, thermal changes i.e. at the start-up of the device and other environmental influences.
- **Phase noise** ϕ_PN comprises short to ultra-short term variations of the oscillator output. Phase noise is due to the transformation of amplitude fluctuations into phase fluctuations, and hence, results from the amplification and integration of noise sources in the circuitry, i.e. white noise (f^0) and flicker noise (f^{-1}). A standard model [Dem06] for phase noise, neglecting flicker noise, combines a white Gaussian process ϕ_g, i.e. amplification of white noise (f^0) and a Wiener process ϕ_w, called Gaussian random-walk (f^{-2}), resulting from the integration of white noise

$$\phi_\mathrm{PN}(t) = \phi_\mathrm{g}(t) + \phi_\mathrm{w}(t), \qquad \phi_\mathrm{g}(t) \sim \mathcal{N}\left(0, \sigma_g^2\right), \tag{2.5a}$$

$$\phi_\mathrm{w}(t) = \int_0^t \delta\phi_\mathrm{w}(\gamma)\, d\gamma, \qquad \delta\phi_\mathrm{w}(t) \sim \mathcal{N}\left(0, \sigma_w^2\right), \tag{2.5b}$$

  with corresponding variances σ_g^2 and σ_w^2.

Figure 2.4 illustrates the time signal and spectrum of an ideal and a real oscillator with different impairments. While a single spectral ray represents the spectrum of an ideal oscillator, frequency drift broadens this spectral ray. The Gaussian phase noise process adds a constant noise floor to the spectrum, whereas Gaussian random-walk introduces a f^{-2}-dependent noise to the spectral ray.

Practical characterization of real oscillators is achieved by measuring, with a spectrum analyzer, their single-side phase noise spectrum $\mathcal{L}_\mathrm{single-side}(\delta f)$ with δf being the offset frequency from the nominal oscillator frequency. As resolution bandwidth B_res of a spectrum analyzer cannot be arbitrarily small, phase noise spectrum measurements for small offsets $\delta f \leq 100\,\mathrm{Hz}$ are falsified.

In order to overcome this shortcoming of spectrum analyzer based characterization, phase noise at small offsets, i.e. f^{-1} flicker noise and f^{-2} random-walk, can be measured in time domain. Therefore, the so-called Allan Variance [All83] characterizes temporal frequency stability on different time scales. The Allan Variance is based on multiple measurements of the average relative frequency $\overline{\delta_f}_k$ over successive intervals $[t + (k-1)T, t + kT)$ of duration T and it is defined by

$$\sigma^2_\mathrm{Allan}(T) = \frac{1}{2(K-1)} \sum_{k=0}^{K-1} \left(\overline{\delta_f}_{k+1} - \overline{\delta_f}_k\right)^2. \tag{2.6}$$

As the Allan Variance compares the difference of frequency measurements in adjacent intervals, frequency fluctuations over intervals shorter or longer than the interval T have no impact on the Allan Variance. As a result, Allan Variance gives frequency stability as function of the observation interval T.

The relationship between Allan Variance σ^2_Allan in time domain and the phase noise power spectral density $S_{\phi_\mathrm{PN}}(\delta f)$ is given according to [WA86] by

$$\sigma^2_\mathrm{Allan}(T) = \frac{2}{(\pi f_\mathrm{w} T)^2} \int_0^{B_\mathrm{m}} S_{\phi_\mathrm{PN}}(\delta f) \sin^4(\pi \delta f T) d(\delta f), \tag{2.7}$$

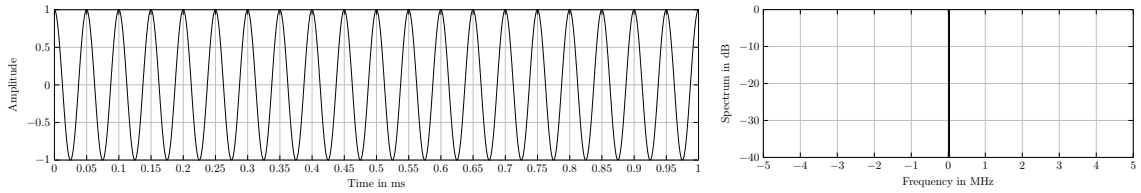
with measurement bandwidth B_m, over which the phase noise has been measured.

For small phase variations, phase noise power spectral density $S_{\phi_\mathrm{PN}}(\delta f)$ and single-side phase noise spectrum $\mathcal{L}_\mathrm{single-side}(\delta f)$ are linked through

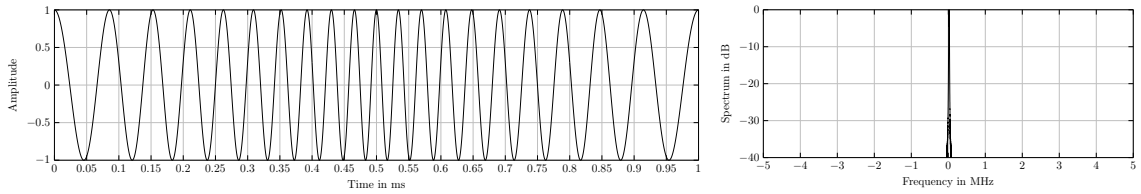
$$S_{\phi_\mathrm{PN}}(\delta f) \approx 2 \cdot \mathcal{L}_\mathrm{single-side}(\delta f). \tag{2.8}$$

Figure 2.5 depicts the typical Allan Variance of different oscillator technologies. Frequency stability attains an optimum, which separates short-term and long-term stability.

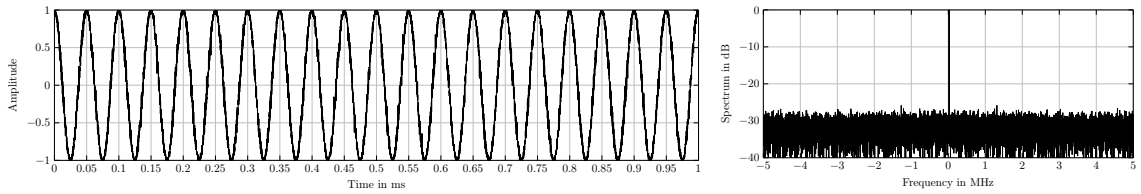
LPWA nodes integrate basic, low accurate clock sources, *e.g.* a quartz, to comply with low-cost and low-complexity requirements. Hence, transceivers, modulation and communication protocols are designed to support large clock offsets, *e.g.* up to $\pm 20\,\mathrm{ppm}$ [Sem16] and corresponding frequency drifts.



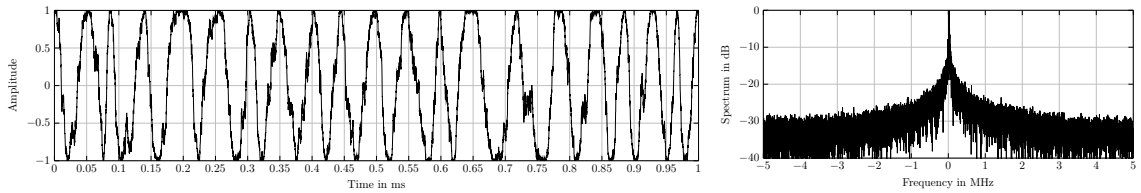
(a) *Ideal oscillator.*



(b) *Real oscillator with a sawtooth-like up-down clock drift of* $\pm 10\,\mathrm{kHz}/0.5\,\mathrm{ms}$.



(c) *Real oscillator with Gaussian phase noise* ($\sigma_g^2 = 0.08^2$).



(d) *Real oscillator with Gaussian random-walk* ($\sigma_w^2 = 0.05^2$).

FIGURE 2.4 – *Time signals and spectra of an ideal and real oscillators with nominal frequency* $f = 20\,\mathrm{kHz}$.

Besides the impact on communication, clock impairments have to be considered also for ranging and localization, especially in time and phase based techniques. For illustration, the impact of time invariant frequency offset δ_f on time based ranging is studied according to [SGG08] in the following. Considering Figure 2.6, the Time of Flight (ToF) and the response time can be defined as

$$T_{\mathrm{ToF}}^{[X]} = t_{\mathrm{A}}^{[X]} - t_{\mathrm{D}}^{[X]}, \tag{2.9a}$$

$$T_{\mathrm{response}}^{[Y]} = t_{\mathrm{D}}^{[Y]} - t_{\mathrm{A}}^{[Y]}. \tag{2.9b}$$

Due to constant frequency offset δ_f, the time duration which a node measures or waits locally, and the real time duration are linked by

$$T_{\mathrm{local}}^{[X]} = T_{\mathrm{real}}^{[X]} \left(1 + \delta_f^{[X]}\right). \tag{2.10}$$

For a positive frequency offset $\delta_f > 0$, the local clock runs faster and a node measuring a time duration counts more clock cycles than at nominal frequency, therefore the node locally believes it has measured a longer duration. Analog, a node configured to wait a certain time duration, actually waits shorter as its clock is running faster.

Considering the basic two-way ranging in Figure 2.6a, the real ToF is given by

$$T_{\mathrm{ToF}_{\mathrm{real}}}^{[1]} = 2\tau + T_{\mathrm{response}}{}_{\mathrm{real}}^{[2]}. \tag{2.11}$$

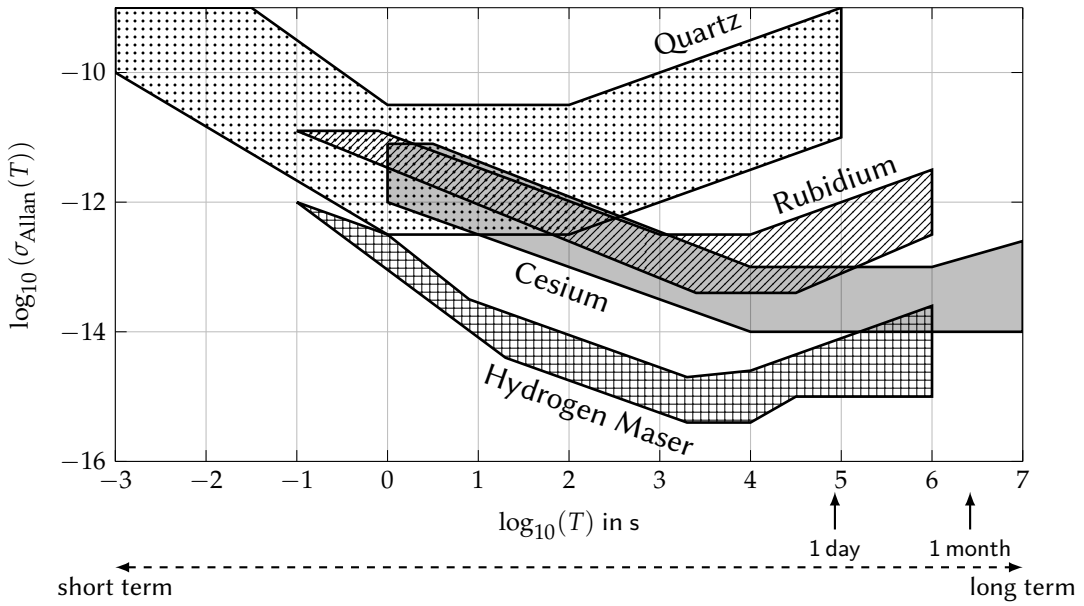
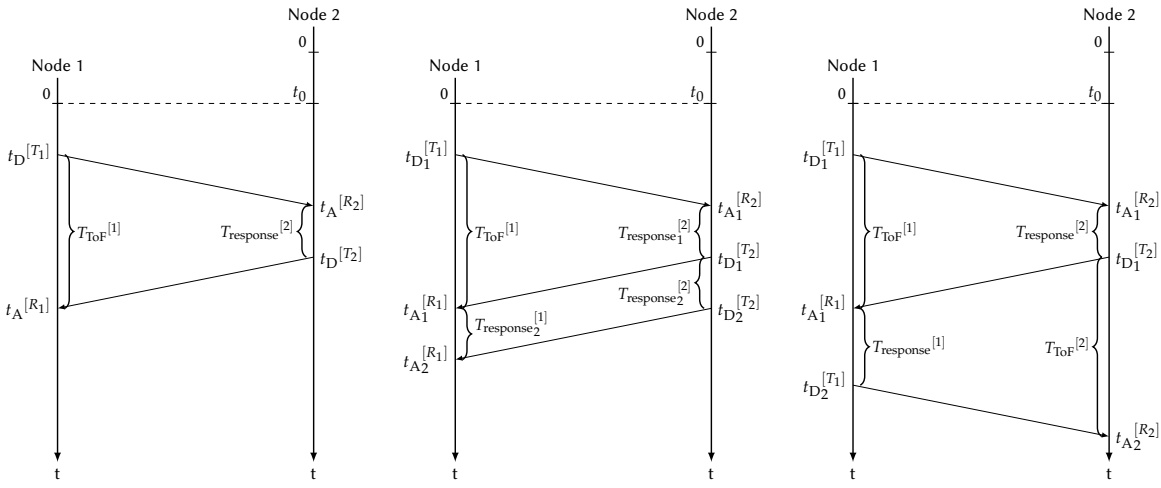


FIGURE 2.5 – *Typical oscillator frequency stability ranges [Vig16].*



(a) *Two-way ToF ranging.* (b) *Three-way ToF ranging.* (c) *Double-sided two-way ranging.*

FIGURE 2.6 – *ToF ranging protocols for frequency offset mitigation.*

However, range estimation according to (1.48) is based on the locally measured or believed time durations

$$\widehat{d} = c_0 \frac{T_{\text{ToF}}{}^{[1]}_{\text{local}} - T_{\text{response}}{}^{[2]}_{\text{local}}}{2} \tag{2.12a}$$

$$= c_0 \frac{\left(2\tau + T_{\text{response}}{}^{[2]}_{\text{real}}\right)\left(1+\delta_f^{[1]}\right) - T_{\text{response}}{}^{[2]}_{\text{real}}\left(1+\delta_f^{[2]}\right)}{2} \tag{2.12b}$$

$$= c_0\,\tau + c_0\,\tau\delta_f^{[1]} + c_0\,T_{\text{response}}{}^{[2]}_{\text{real}}\frac{\delta_f^{[1]} - \delta_f^{[2]}}{2} = c_0\,\tau + c_0\,\tau\delta_f^{[1]} + c_0\,T_{\text{response}}{}^{[2]}_{\text{local}}\frac{\delta_f^{[1]} - \delta_f^{[2]}}{2\left(1+\delta_f^{[2]}\right)}. \tag{2.12c}$$

The first term in (2.12) corresponds to the real range d, whereas the second term accounts for the clock offset of node 1 with respect to real time. For a range $d = 10\,\text{km}$ this induces a 1 m ranging error considering a frequency offset $\delta_f^{[1]} = 100\,\text{ppm}$. This error is no correctable without a precise external time reference, however it is small compared to $c_0\,\tau$ and hence neglectable. The third term reflects the clock mismatch error between node 1 and node 2 and the fact, that the actual response time $T_{\text{response}}{}^{[2]}_{\text{real}}$, varies from the nominal time duration $T_{\text{response}}{}^{[2]}_{\text{local}}$

known to node 1. Three cases exist:

- Identical frequency offset, $\delta_f^{[1]} - \delta_f^{[2]} = 0$: The real response time of node 2 is compensated by the same clock offset on node 1.
- Node 1 running faster than node 2, $\delta_f^{[1]} - \delta_f^{[2]} > 0$: Node 1 counts more clock cycles on the estimation of ${T_{\text{ToF}}}_{\text{real}}^{[1]}$, resulting in a over estimation of the ToF and hence a positive range error.
- Node 1 running slower than node 2, $\delta_f^{[1]} - \delta_f^{[2]} < 0$: The response time of node 2 is shorter than the nominal duration known to node 1, resulting in a negative range error.

This third term is in general the dominant error and needs to be corrected to obtain valid range estimates. Considering a relative frequency offset $\delta_f^{[1]} - \delta_f^{[2]} = 2\,\text{ppm}$ and a LPWA typical response time ${T_{\text{response}}}_{\text{real}}^{[2]} = 1\,\text{s}$ result in a range error $c_0 \cdot 1\,\text{s} \cdot 2\,\text{ppm}/2 = c_0 \cdot 1\,\mu\text{s} = 300\,\text{m}$.

Different strategies can be adopted to compensate this frequency offset induced error:

- **CFO estimation**: Both nodes perform synchronization on the packet preamble (see Figure 1.14) in order to align the receiver in both time and frequency, to correctly receive the data following the preamble. The receiver has hence an estimation of the relative frequency offset between itself and the transmitter. This CFO estimation $\left(1+\delta_f^{[1]}\right) / \left(1+\delta_f^{[2]}\right)$ can be used to calculate the response time ${T_{\text{response}}}_{\text{local}}^{[2]}$ $\left(1+\delta_f^{[1]}\right) / \left(1+\delta_f^{[2]}\right)$ to use it for range estimation calculation in (2.12a) instead of ${T_{\text{response}}}_{\text{local}}^{[2]}$.

  For a maximum residual ranging error $\left(\epsilon_{\widehat{d}}\right)_{\max}$, the required relative frequency offset estimation precision can be derived from (2.12) and is given by

$$\left(\epsilon_{\widehat{\delta}_f}\right)_{\max} < \frac{2\left(\epsilon_{\widehat{d}}\right)_{\max}}{c_0 {T_{\text{response}}}_{\text{real}}^{[2]}}. \tag{2.13}$$

  For a residual ranging error $\left(\epsilon_{\widehat{d}}\right)_{\max} < 1\,\text{m}$ and a response time ${T_{\text{response}}}_{\text{real}}^{[2]} = 1\,\text{s}$, CFO estimation precision of $\approx 6\,\text{ppb}$ is required. Techniques based on this strategy are adopted by *e.g.* [Sem16; DCM18].

- **Multi-way packet exchange**: Instead of performing only a two-way packet exchange, variations such as depicted in Figure 2.6b or Figure 2.6c are possible and allow correcting the frequency offset error.

  The three-way packet exchange depicted in Figure 2.6b supposes that node 2 responds with two packets ensuring that the two response times ${T_{\text{response}}}_{\text{local}}^{[2]}$ and ${T_{\text{response}}}_{2,\text{local}}^{[2]}$ are identical. This enables node 1 to measure the real response time ${T_{\text{response}}}_{2,\text{real}}^{[2]}$ in its own time basis as ${T_{\text{response}}}_{2,\text{local}}^{[1]}$, before using it in (2.12a)

$$\begin{aligned}
\widehat{d} &= c_0 \frac{{T_{\text{ToF}}}_{\text{local}}^{[1]} - {T_{\text{response}}}_{2,\text{local}}^{[1]}}{2} \\
&= c_0 \frac{\left(2\tau + {T_{\text{response}}}_{1,\text{real}}^{[2]}\right)\left(1+\delta_f^{[1]}\right) - {T_{\text{response}}}_{2,\text{real}}^{[2]}\left(1+\delta_f^{[1]}\right)}{2} \\
&= c_0\,\tau + c_0\,\tau\delta_f^{[1]} + c_0 \underbrace{\left({T_{\text{response}}}_{1,\text{real}}^{[2]} - {T_{\text{response}}}_{2,\text{real}}^{[2]}\right)}_{\overset{!}{\approx}0} \frac{\left(1+\delta_f^{[1]}\right)}{2}.
\end{aligned} \tag{2.14}$$

  To relax the requirement for sending two packets with identical response time, the double-sided two-way ranging with three packets, where the middle packet is used by both of the two inversed two-way exchanges, can be adopted as illustrated in Figure 2.6c. Range is calculated according to

$$\widehat{d} = c_0 \frac{{T_{\text{ToF}}}_{\text{local}}^{[1]} \cdot {T_{\text{ToF}}}_{\text{local}}^{[2]} - {T_{\text{response}}}_{\text{local}}^{[1]} \cdot {T_{\text{response}}}_{\text{local}}^{[2]}}{{T_{\text{ToF}}}_{\text{local}}^{[1]} + {T_{\text{ToF}}}_{\text{local}}^{[2]} + {T_{\text{response}}}_{\text{local}}^{[1]} + {T_{\text{response}}}_{\text{local}}^{[2]}}. \tag{2.15}$$

Defining $\delta_f^{+[X]} = \left(1 + \delta_f^{[X]}\right)$, (2.15) can be rewritten as

$$\begin{aligned}
\widehat{d} &= c_0 \frac{\left(2\tau + T_{\text{response}}^{[2]}_{\text{real}}\right)\delta_f^{+[1]} \cdot \left(2\tau + T_{\text{response}}^{[1]}_{\text{real}}\right)\delta_f^{+[2]} - T_{\text{response}}^{[1]}_{\text{real}}\delta_f^{+[1]} \cdot T_{\text{response}}^{[2]}_{\text{real}}\delta_f^{+[2]}}{\left(2\tau + T_{\text{response}}^{[2]}_{\text{real}}\right)\delta_f^{+[1]} + \left(2\tau + T_{\text{response}}^{[1]}_{\text{real}}\right)\delta_f^{+[2]} + T_{\text{response}}^{[1]}_{\text{real}}\delta_f^{+[1]} + T_{\text{response}}^{[2]}_{\text{real}}\delta_f^{+[2]}} \\
&= c_0 \frac{\delta_f^{+[1]}\delta_f^{+[2]}\left[\left(2\tau + T_{\text{response}}^{[2]}_{\text{real}}\right) \cdot \left(2\tau + T_{\text{response}}^{[1]}_{\text{real}}\right) - T_{\text{response}}^{[1]}_{\text{real}} \cdot T_{\text{response}}^{[2]}_{\text{real}}\right]}{\left(\delta_f^{+[1]} + \delta_f^{+[1]}\right)\left[2\tau + T_{\text{response}}^{[1]}_{\text{real}} + T_{\text{response}}^{[2]}_{\text{real}}\right]} \\
&= c_0 \frac{\delta_f^{+[1]}\delta_f^{+[2]}\left[4\tau^2 + 2\tau\left(T_{\text{response}}^{[1]}_{\text{real}} + T_{\text{response}}^{[2]}_{\text{real}}\right)\right]}{\left(\delta_f^{+[1]} + \delta_f^{+[2]}\right)\left[2\tau + T_{\text{response}}^{[1]}_{\text{real}} + T_{\text{response}}^{[2]}_{\text{real}}\right]} = c_0\tau \frac{2\delta_f^{+[1]}\delta_f^{+[2]}}{\delta_f^{+[1]} + \delta_f^{+[2]}}.
\end{aligned} \tag{2.16}$$

After re-expansion, the estimated distance is given by

$$\begin{aligned}
\widehat{d} = c_0\tau \frac{2\delta_f^{+[1]}\delta_f^{+[2]}}{\delta_f^{+[1]} + \delta_f^{+[2]}} &= c_0\tau \frac{2\left(1 + \delta_f^{[1]}\right)\left(1 + \delta_f^{[2]}\right)}{\left(1 + \delta_f^{[1]}\right) + \left(1 + \delta_f^{[2]}\right)} = c_0\tau + \underbrace{c_0\tau \frac{\delta_f^{[1]} + \delta_f^{[2]} + 2\delta_f^{[1]}\delta_f^{[2]}}{2 + \delta_f^{[1]} + \delta_f^{[2]}}}_{\text{Distance dependent ranging error}} \\
&\approx c_0\tau + c_0\tau \frac{\delta_f^{[1]} + \delta_f^{[2]}}{2}.
\end{aligned} \tag{2.17}$$

Frequency offset dependent ranging error is minimized and the error is only proportional to distance d, but not to response time $T_{\text{response}}^{[X]}$.

For phase based ranging and localization systems, frequency offset, frequency drift and phase noise become even more dominant issues, as frequency errors integrate to phase errors over time. Therefore, GNSS systems continuously track phase over time, to precisely estimate and correct frequency induced errors.

LPWA two-way ranging according to Figure 1.16b has to consider that the phase relation between node 1 and node 2 varies over time in the presence of frequency offsets. As a result, the two phase measurements $\widehat{\phi_{\text{A}}}^{[T_i,R_k]}$ and $\widehat{\phi_{\text{A}}}^{[T_k,R_i]}$ in (1.65) need to be corrected by the phase offset resulting from relative CFO integration between the two phase measurement times. A complete framework and details are given in Chapter 3.2.

2.2.2 Compatibility of Existing LPWA Technologies and Accessibility to Localization Metrics

Gaining access to radio localization metrics from the physical layer is a necessary hardware requirement for radio signal based positioning. UWB chips [Dec15] allow controlling Time of Departure (ToD) t_{D} and returning time stamps of the estimated ToA $\widehat{t_{\text{A}}}$ for received packets. GNSS receivers pass raw code pseudo range i.e. ToA estimates and carrier pseudo range i.e. Phase of Arrival (PoA) estimates directly into the integrated positioning/navigation processor to derive location, dedicated GNSS chipsets grant access to these raw data [Ubl] for external, custom processing.

LPWA radio modules are designed to meet low-power, low-complexity and low-cost constraints and are initially intended for data transmission only. While most radio chips implement Quality of Service (QoS) indicators such as the Received Signal Strength Indicator (RSSI), gaining access to precise time and phase information is not a straightforward task. It is even impossible if chipsets are not designed for giving access to those metrics. LoRaWAN networks provide node position estimation through uplink TDoA (see Chapter 1.6.1.2) with GNSS synchronized base stations and specific base station hardware [Sema; Semc] allowing to time stamp uplink packets. LPWA nodes with unmodified hardware can be used and a single uplink packet is sufficient for position estimation on the base station side. New radio chips *e.g.* [Sem17b], combine LPWA features and ranging functionalities, such as a two-way ranging protocol automated on the physical layer and range estimation.

LPWA localization has to consider not only positioning precision, but also the impact, that specific hardware requirements have on system complexity, power consumption and cost.

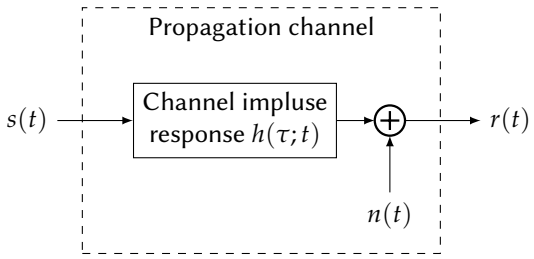


FIGURE 2.7 – *Tapped delay line channel model [Pro01].*

2.3 Channel Limitations

System and hardware limitations have a significant impact on positioning. However, addressing all these through adapted techniques does not guarantee accurate and precise positioning as the physical propagation channel remains as ultimate factor, possibly limiting localization performances. Multipath propagation and interference add additional noise and biases to radio localization metrics, and hence need to be taken into account in the location estimation process. These issues are outlined in the following and their specific impact for LPWA positioning is compared to the one on GNSS and UWB localization.

2.3.1 Tapped Delay Line Channel Model

The linear time variant filter channel [Pro01] depicted in Figure 2.7 is the standard model characterizing physical radio channels. The time variant channel impulse response $h(\tau;t)$ represents the impulse response of the channel at time t. Considering multipath propagation, the channel impulse response can be given in the form

$$h(\tau;t) = \sum_{p=0}^{P(t)-1} a_p(t)\delta\left(\tau - \tau_p(t)\right), \tag{2.18}$$

with P being the number of signal paths, time-varying complex path amplitude a_p and path delay τ_p. Its frequency dual is given by the channel transfer function

$$H(f;t) = \sum_{p=0}^{P(t)-1} a_p(t)e^{-j2\pi f\tau_p(t)}. \tag{2.19}$$

As a result, transmit $s(t)$ and receive signal $r(t)$ are linked by

$$r(t) = s(t) * h(\tau;t) + n(t) = \sum_{p=0}^{P(t)-1} a_p(t)s\left(t - \tau_p(t)\right) + n(t), \tag{2.20}$$

with Additive White Gaussian Noise (AWGN) $n(t)$.

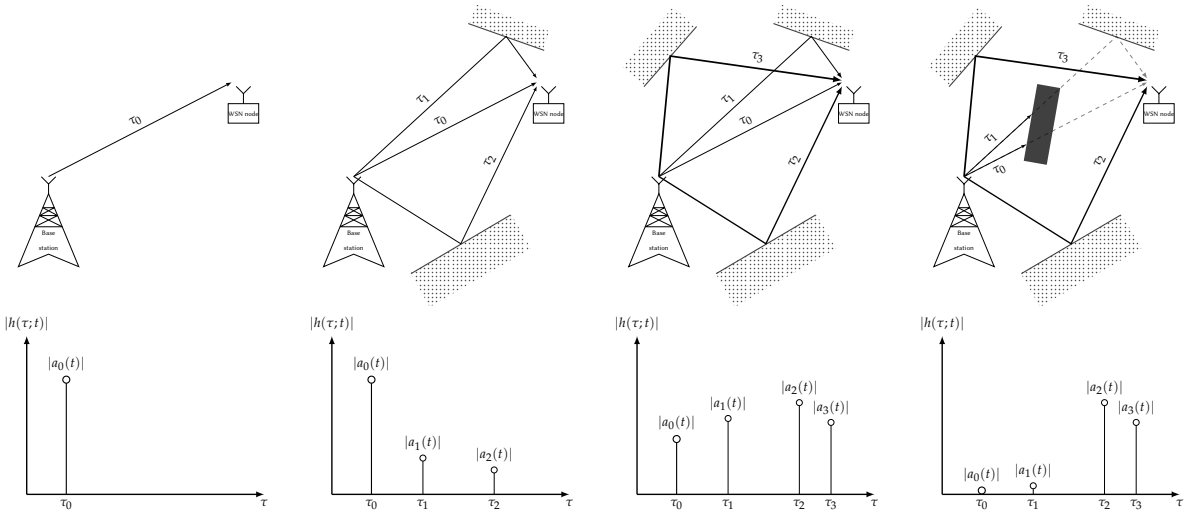
2.3.2 Classification of Propagation Channels

Wireless radio channels can be roughly classified into three groups as illustrated in Figure 2.8:

- Free-space: The channel impulse response is characterized by a pure delay corresponding to the straight line and hence distance between transmitter and receiver. The channel impulse response simplifies to

$$h(\tau;t) = a_0(t)\delta\left(\tau - \tau_0(t)\right). \tag{2.21}$$

- LoS: The transmitted radio signal arrives at the receiver via the direct LoS path but also via paths that are reflected in the environment. For LPWA scenarios, such reflections arise *e.g.* from nearby buildings. It has to be considered that optical LoS and radio signal LoS are not identical. A rough indicator for the LoS condition is the clearance of the 1st Fresnel zone (see (1.34) and Appendix A). As visible light and sub-GHz wavelengths differ by a factor $\lambda_{\text{W sub-GHz}}/\lambda_{\text{W visible light}} \approx 5.5 \times 10^4$, optical LoS does not strictly infer radio LoS propagation. For the purpose of illustration, a distinction between the following two scenarios can be made:
  - Weak multipath: The channel impulse response is composed of the direct path and multiple reflection paths whose amplitude is weaker than the first/direct path $|a_p| \lessapprox |a_0|$, $p = 1, \ldots, P-1$.



(a) *Free-space.* (b) *LoS: Weak multipath.* (c) *LoS: Strong multipath.* (d) *NLoS.*

FIGURE 2.8 – *Classification of wireless propagation channels.*

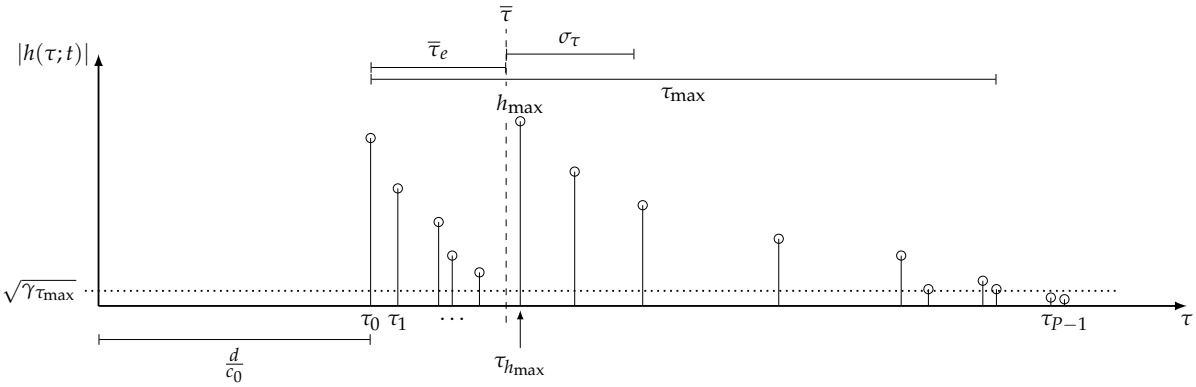


FIGURE 2.9 – *Macroscopic propagation channel characteristics.*

  - Strong multipath: At least one multipath component has an amplitudes larger than the direct/LoS path $|a_p| \gtrapprox |a_0|$, $p \geq 1$.

- NLoS: The direct/LoS path is strongly attenuated compared to the multipath components. This situation may arise from obstruction of the LoS through objects. In this case of severe attenuation, the LoS path may experience additional delays due to the materials it passes through.

2.3.3 Macroscopic Propagation Channel Characteristics

Various macroscopic indicators can be defined based on the presented channel types, characteristics and the underlying physical phenomena.

2.3.3.1 Time Domain Characteristics

In the following, the delay profile from (2.18) is considered. An arbitrary channel in Figure 2.9 illustrates the main macroscopic indicators presented in the following. The delays τ_p include the overall propagation delay due to the distance between transmitter and receiver, so in theory $\tau_0 = d/c_0$.

Power gain

Average power gain of the delay profile $h(\tau;t)$ is given by

$$\mathcal{E}(t) = \mathbb{E}_1\left[|h(\tau;t)|^2\right] = \sum_{p=0}^{P(t)-1} |a_p(t)|^2. \tag{2.22}$$

Maximum Amplitude

The maximum path amplitude is given by

$$h_{\max}(t) = \max_p \left\{|a_p(t)|\right\}. \tag{2.23}$$

Delay of Maximum Amplitude or Power

The delay of maximum path amplitude/power is given by

$$\tau_{h_{\max}}(t) = \left\{\tau_p(t) : \max_p \left\{|a_p(t)|\right\}\right\} = \left\{\tau_p(t) : \max_p \left\{|a_p(t)|^2\right\}\right\}. \tag{2.24}$$

Mean Delay

The mean delay $\overline{\tau}$ is defined as the first moment with respect to the delay τ of the power delay profile $|h(\tau;t)|^2$

$$\overline{\tau}(t) = \frac{\mathbb{E}_\tau\left[|h(\tau;t)|^2\right]}{\mathbb{E}_1\left[|h(\tau;t)|^2\right]} = \frac{\sum_{p=0}^{P(t)-1} |a_p(t)|^2 \tau_p(t)}{\sum_{p=0}^{P(t)-1} |a_p(t)|^2}. \tag{2.25}$$

Mean Excess Delay

The mean excess delay $\overline{\tau}_e$ is defined as the difference between the mean delay $\overline{\tau}$ and the first path delay τ_0

$$\overline{\tau}_e(t) = \overline{\tau}(t) - \tau_0(t) = \frac{\mathbb{E}_\tau\left[|h(\tau;t)|^2\right]}{\mathbb{E}_1\left[|h(\tau;t)|^2\right]} - \tau_0(t) = \frac{\sum_{p=0}^{P(t)-1} |a_p(t)|^2 \left(\tau_p(t) - \tau_0(t)\right)}{\sum_{p=0}^{P(t)-1} |a_p(t)|^2}. \tag{2.26}$$

Maximum Excess Delay

The maximum excess delay $\tau_{\max}$ is defined as the time delay difference between the longest path still above a threshold power $\gamma_{\tau_{\max}}$ and the first path

$$\tau_{\max}(t) = \max_p \left\{\tau_p(t) : |a_p(t)|^2 \geq \gamma_{\tau_{\max}}\right\} - \tau_0(t). \tag{2.27}$$

Root Mean Square Delay

The Root Mean Square (RMS) delay is defined by

$$\tau_{\text{RMS}}(t) = \sqrt{\frac{\mathbb{E}_{\tau^2}\left[|h(\tau;t)|^2\right]}{\mathbb{E}_1\left[|h(\tau;t)|^2\right]}} = \sqrt{\frac{\sum_{p=0}^{P(t)-1} |a_p(t)|^2 \tau_p^2(t)}{\sum_{p=0}^{P(t)-1} |a_p(t)|^2}}. \tag{2.28}$$

For channel responses with a long propagation delay, the overall propagation delay τ_0 will be large and so the RMS delay. Without the knowledge of the first path delay τ_0, this metric does not allow to characterize a channel in terms of multipath propagation.

Delay Spread

The delay spread is defined as the standard deviation or square root of the second (central) moment of the power delay profile

$$\sigma_\tau(t) = \sqrt{\frac{\mathbb{E}_{(\tau-\overline{\tau})^2}\left[|h(\tau;t)|^2\right]}{\mathbb{E}_1\left[|h(\tau;t)|^2\right]}} = \sqrt{\frac{\mathbb{E}_{\tau^2}\left[|h(\tau;t)|^2\right]}{\mathbb{E}_1\left[|h(\tau;t)|^2\right]} - \left(\frac{\mathbb{E}_\tau\left[|h(\tau;t)|^2\right]}{\mathbb{E}_1\left[|h(\tau;t)|^2\right]}\right)^2} = \sqrt{\tau^2_{\mathrm{RMS}}(t) - \overline{\tau}^2(t)}$$
$$= \sqrt{\frac{\sum_{p=0}^{P(t)-1} |a_p(t)|^2 \left(\tau_p(t) - \overline{\tau}(t)\right)^2}{\sum_{p=0}^{P(t)-1} |a_p(t)|^2}}. \tag{2.29}$$

It is a measure for the temporal dispersion of the channel. Different propagation environments can be characterized by different delay spreads as depicted in Table 2.3.

Delay Profile Kurtosis

The Kurtosis [MGWW10] is defined as the fourth central moment of the amplitude delay profile

$$\kappa_\tau(t) = \frac{\mathbb{E}_1\left[\left(|h(\tau;t)| - \mathbb{E}_1\left[|h(\tau;t)|\right]\right)^4\right]}{\left(\mathbb{E}_1\left[\left(|h(\tau;t)| - \mathbb{E}_1\left[|h(\tau;t)|\right]\right)^2\right]\right)^2} \tag{2.30}$$

and it is a metric capturing the tailedness [Pea05] of the Channel Impulse Response (CIR).

Rise Time

The rise time [MGWW10] measures the steepness of the rising edge in the amplitude delay profile

$$t_{\mathrm{rise}}(t) = t_{\mathrm{H}}(t) - t_{\mathrm{L}}(t), \tag{2.31}$$

where

$$t_{\mathrm{L}}(t) = \min_p \left\{\tau_p(t) : |a(t)| \geq \gamma_{a_{\mathrm{L}}}\, \sigma_n\right\}, \tag{2.32a}$$
$$t_{\mathrm{H}}(t) = \min_p \left\{\tau_p(t) : |a(t)| \geq \gamma_{a_{\mathrm{H}}}\, h_{\max}(t)\right\}, \tag{2.32b}$$

with noise floor σ_n, $\gamma_{a_{\mathrm{L}}} > 0$ and $0 < \gamma_{a_{\mathrm{H}}} \leq 1$.

2.3.3.2 Multipath Spread

Based on the low-pass channel impulse response $h(\tau;t)$, the autocorrelation function can be defined, according to [Pro01] as

$$\Omega_{h,h}(\tau_1, \tau_2; \Delta t) = \frac{1}{2}\mathbb{E}\left[h^*(\tau_1;t)h(\tau_2;t+\Delta t)\right]. \tag{2.33}$$

For uncorrelated scattering, i.e. when amplitude and phase shifts of delay τ_1 are uncorrelated with those of delay τ_2, (2.33) simplifies to

$$\frac{1}{2}\mathbb{E}\left[h^*(\tau_1;t)h(\tau_2;t+\Delta t)\right] = \Omega_{h,h}(\tau_1;\Delta t)\delta\left(\tau_1 - \tau_2\right) \tag{2.34}$$

and with $\Delta t = 0$, the autocorrelation function is called multipath intensity profile or delay power spectrum

$$\Omega_{h,h}(\tau) = \Omega_{h,h}(\tau_1;0). \tag{2.35}$$

The multipath spread T_{m} is defined as the range of delays τ for which $\left|\Omega_{h,h}(\tau)\right| > 0$. Multipath spread T_{m} and delay spread σ_τ are empirically proportional, as they measure the same physical phenomenon.

2.3.3.3 Coherence Bandwidth

Analog to the multipath spread, the spaced-frequency, spaced-time correlation function of the channel transfer function $H(f;t)$ can be defined, according to [Pro01] as

$$\Omega_{H,H}(\Delta f;\Delta t) = \frac{1}{2}\mathbb{E}\left[H^*(f;t)H(f+\Delta f;t+\Delta t)\right]. \tag{2.36}$$

Considering $\Delta t = 0$, (2.36) simplifies to the spaced-frequency correlation function

$$\Omega_{H,H}(\Delta f) = \Omega_{H,H}(\Delta f;0). \tag{2.37}$$

The relationship between (2.35) and (2.37) is given by Fourier transform. Subsequently, the coherence bandwidth can be defined by

$$B_{\text{coh}} = \frac{1}{T_{\text{m}}}, \tag{2.38}$$

corresponding to the bandwidth over which the channel transfer function has an approximately constant amplitude and a linear phase shift. It can be deduced from (2.38), that coherence bandwidth B_{coh} and delay spread σ_τ are equally, empirically inverse proportional. Common definitions [Rap+96] are

$$B_{\text{coh}}^{0.9} = \frac{1}{50\sigma_\tau}, \qquad \text{for} \quad |\Omega_{H,H}(\Delta f)| \geq 0.9, \tag{2.39a}$$

$$B_{\text{coh}}^{0.5} = \frac{1}{5\sigma_\tau}, \qquad \text{for} \quad |\Omega_{H,H}(\Delta f)| \geq 0.5. \tag{2.39b}$$

For signal and system bandwidths smaller than the coherence bandwidth, the channel is frequency flat, whereas bandwidths larger than the coherence bandwidth require adequate channel estimation to compensate the frequency selective fading. This can be achieved i.e. in Orthogonal Frequency Division Multiplexing (OFDM) systems through subcarriers that are modulated with pilot symbols for channel estimation.

2.3.3.4 Coherence Time

Considering (2.36) with $\Delta f = 0$ allows to establish the spaced-time correlation function [Pro01]

$$\Omega_{H,H}(\Delta t) = \Omega_{H,H}(0;\Delta t), \tag{2.40}$$

from which the coherence time T_{coh} can be defined as the time over which the spaced-time correlation function is above a certain level. The coherence time is the period over which the channel can be considered as time invariant.

2.3.3.5 Doppler Spread

Temporal variations in the channel impulse response are the result of movements in either transmitter position, receiver position or the propagation environment, or a combination of the aforementioned. The time variant channel is characterized by the Doppler power spectrum [Pro01]

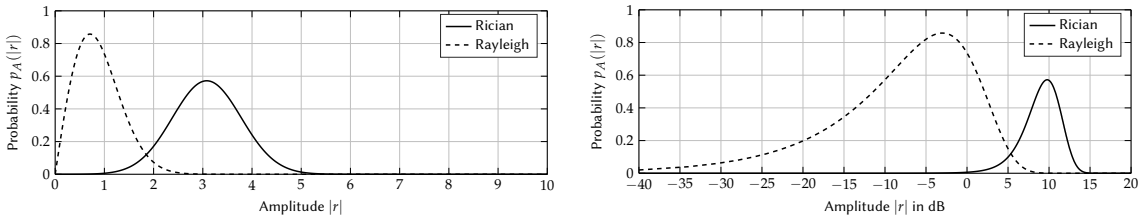
$$S_D(f) = \int_{-\infty}^{\infty} \Omega_{H,H}(0,\Delta t)e^{-j2\pi f\Delta t}d\Delta t. \tag{2.41}$$

The Doppler spread B_{d} is defined as as the range f for which $|S_D(f)| > 0$. As (2.40) and (2.41) are linked by Fourier transform, Doppler spread and coherence time are related by

$$B_{\text{d}} = \frac{1}{T_{\text{coh}}}. \tag{2.42}$$

2.3.4 Fading Channels

The amplitudes of the different path components are varying due to different physical phenomena such as attenuation on a reflecting object or obstacle to pass. This so-called large-scale fading depends on macroscopic variations in the environment. Furthermore, multiple paths of similar delays combine in constructive or destructive



(a) *Linear representation.* (b) *Logarithmic representation.*

FIGURE 2.10 – *Amplitude probability distribution for Rician and Rayleigh fading with* $\overline{\mathcal{E}} = 1$ *and* $\overline{\mathcal{E}}_{LoS} = 9$.

manner depending on their carrier phase shift (see Chapter 2.3.6.1). This phenomenon is called small-scale fading as caused by variations on the carrier wavelength scale.

Transmitting an unmodulated carrier $s(t) = e^{j2\pi f_w t}$ through a multipath channel, results in the received signal

$$r(t) = s(t) * h(\tau; t) = e^{j2\pi f_w t} \underbrace{\sum_{p=0}^{P-1} a_p(t) e^{-j2\pi f_w \tau_p(t)}}_{|r(t)|}, \tag{2.43}$$

when noise n is neglected.

For a sufficient large number of paths P, the amplitude of the received signal $|r(t)|$ can be modeled, according to the central limit theorem, as Gaussian process:

- **Rician fading**: In the presence of multipath, i.e. the channel has a non-fading LoS path, called specular component. Subsequently, the in phase I and quadrature Q component can be modeled by statistically independent Gaussian random variables of mean μ_I and μ_Q, respectively. The average specular, LoS power gain is given by $\overline{\mathcal{E}}_{LoS} = \mu_I^2 + \mu_Q^2$. Consequently, the amplitude probability distribution is given, according to the so-called Rician distribution, by

$$p_A(|r|) = \frac{2|r|}{\overline{\mathcal{E}}} e^{\left(-\frac{|r|^2 + \overline{\mathcal{E}}_{LoS}}{\overline{\mathcal{E}}}\right)} I_0\left(\frac{2|r|\sqrt{\overline{\mathcal{E}}_{LoS}}}{\overline{\mathcal{E}}}\right), \tag{2.44}$$

  with average channel power gain $\overline{\mathcal{E}}$ according to (2.22) and modified 0^{th}-order Bessel function of first kind I_0.

- **Rayleigh fading**: In the case of NLoS propagation, the specular component is not present and (2.44) simplifies to a Rayleigh distribution given by

$$p_A(|r|) = \frac{2|r|}{\overline{\mathcal{E}}} e^{\left(-\frac{|r|^2}{\overline{\mathcal{E}}}\right)}. \tag{2.45}$$

Figure 2.10 illustrates the amplitude distribution functions for both Rician and Rayleigh fading.

2.3.5 Typical Outdoor Channel Models for LPWA Networks

For the design, benchmarking and comparison of telecommunication systems, i.e. signal waveform, modulation or error correction schemes, numerical simulations are a crucial step before implementation and field trials. For this purpose, channel models are used to simulate the real propagation environment with different degrees of complexity and realness. These channel models are obtained through theoretical considerations or in-situ channel measurements/sounding.

Typical outdoor channel models suited for sub-GHz communication scenarios and hence applicable to LPWA networks are:

- The 3rd Generation Partnership Project (3GPP) Extended Typical Urban (ETU) channel model is designed for benchmarking mobile communication systems [3GP08].
- The European Telecommunications Standards Institute (ETSI) European Co-Operation in the field of Scientific and Technical research 259 (COST 259) channel models are designed for usage in Universal Mobile Telecommunication System (UMTS) systems [ETS10]. Typical but simplified realization of the COST 259 channel model are:
  - The Typical urban (Tux) channel model comprising a single cluster of Rayleigh fading paths.

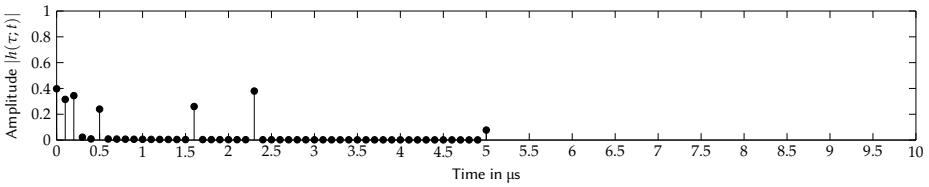
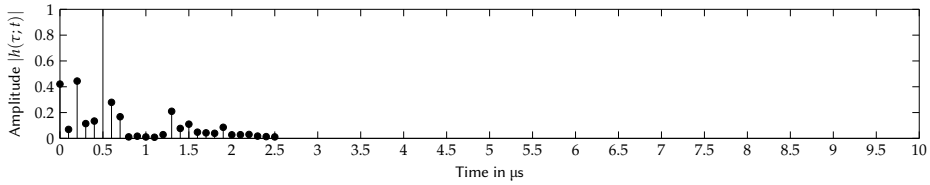
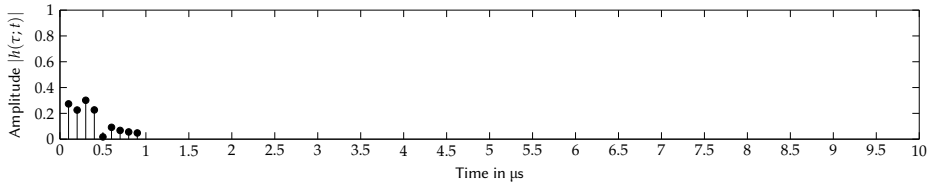


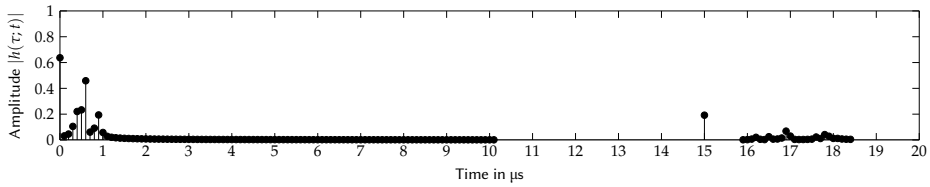
FIGURE 2.11 – *3GPP ETU channel model realization [3GP08].*



(a) *Typical urban (Tux).*



(b) *Rural area (Rax).*



(c) *Hilly terrain (HTx).*

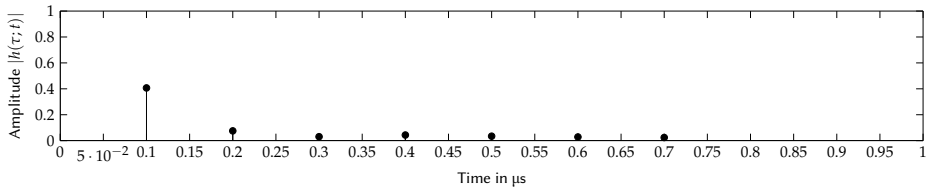
FIGURE 2.12 – *Simplified ETSI COST 259 channel model realizations [ETS10].*

  - The Rural area (Rax) channel model comprising a single cluster of Rayleigh fading paths and a Rician fading path.
  - The Hilly terrain (HTx) channel model comprises two clusters of Rayleigh fading paths.
- The WINNER channel model offers besides the tapped delay line model equally modeling of angular information [BR07].

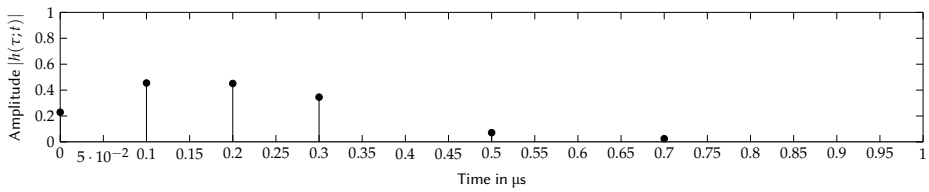
The aforementioned channel models can be compared to channel models used for GNSS and indoor i.e. UWB systems, in order to illustrate the different channel imposed limitations for localization:

- GNSS channels vary largely depending on the terrestrial environment and the satellite elevation angle. LoS and NLoS scenarios are possible and large delay spreads up to 15 µs are observed [JBH96].
- The International Telecommunication Union (ITU) indoor models A (low delay spread) and B (median delay spread) are designed for the 2 GHz frequency band and indoor office environments [ITU97].
- The channel model adopted by the IEEE 802.15.4a standard [Mol+06] has denser multipath profiles and hence presents harsher conditions than the ITU models. [Mol+06]

Figure 2.11, Figure 2.12 and Figure 2.13 show realizations for the aforementioned channel models, while Table 2.3 gives an overview on the macroscopic characteristics. It can be concluded that UWB systems usually profit from short delay spreads compared to LPWA scenarios with strong multipath or even NLoS communication inducing large delay spreads. GNSS and terrestrial LPWA both face large delay spreads. However, because high elevation satellites are typically in LoS condition, GNSS channels are characterized by Rician fading, while LPWA channels will most likely be of Rayleigh type.



(a) *Indoor A.*



(b) *Indoor B.*

FIGURE 2.13 – *ITU indoor office environment channel model realizations [ITU97].*

Channel model	**Mean Excess Delay $\overline{\tau}_e$ in µs**	**Delay Spread σ_τ in µs**	**Coherence Bandwidth $B_{\text{coh}}^{0.5}$ in kHz**
ETU	0.561	0.991	202
HTx	0.894	3.040	66
Tux	0.500	0.500	400
Rax	0.089	0.100	2000
Indoor A	0.024	0.037	5402
Indoor B	0.068	0.099	2015

TABLE 2.3 – *Overview on macroscopic characteristics for LPWA, GNSS and indoor propagation channel models.*

2.3.6 Propagation Channel Impact on Localization Metrics

In the following, the impact of channel limitations on typical LPWA localization methods is outlined with the aim to summarize the challenges for LPWA radio signal based localization and to sketch up the research questions as well as the hypotheses made in the following chapters.

2.3.6.1 RSSI

Parametric, model based RSSI ranging/localization will be feasible in close to free-space propagation scenarios. However, finding a generally valid path loss model is difficult due to obstruction causing large offsets in the path loss

$$L_{\text{path}} = \frac{P_{\text{r}}}{P_{\text{t}} G_{\text{t}} G_{\text{r}}}. \tag{2.46}$$

Moreover, small-scale fading due to constructive and destructive combination of paths with similar delay result in large RSSI variations over short-range variations in the order of the wavelength.

Considering a two-ray propagation scenario as depicted in Figure 2.14 with a base station antenna at height h_{b} and a mobile node antenna at height h_{m}, the received signal can be given by

$$\begin{aligned} r(t) = \quad & s_0\left(t-\tau_0(d)\right)\; e^{j2\pi f_{\text{w}}\left(t-\tau_0(d)\right)}\; a(\tau_0(d)) \\ & + s_0\left(t-\tau_1(d)\right)\; e^{j2\pi f_{\text{w}}\left(t-\tau_1(d)\right)}\; a(\tau_1(d)), \end{aligned} \tag{2.47}$$

with attenuation a according to Friis law (1.1), delays τ_i depending on antenna height and distance d. Considering

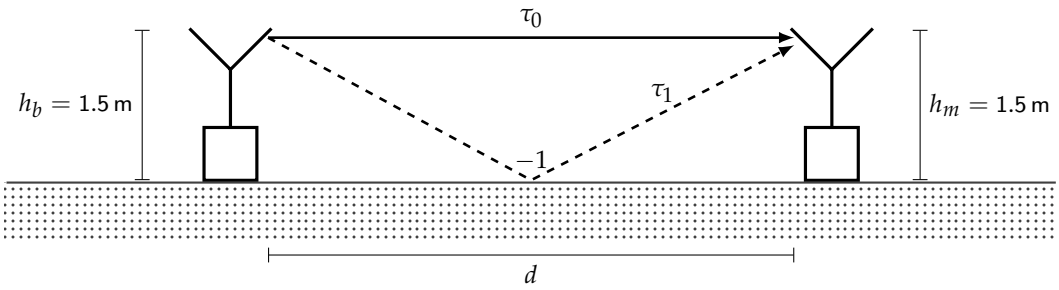


FIGURE 2.14 – *Two-ray propagation model.*

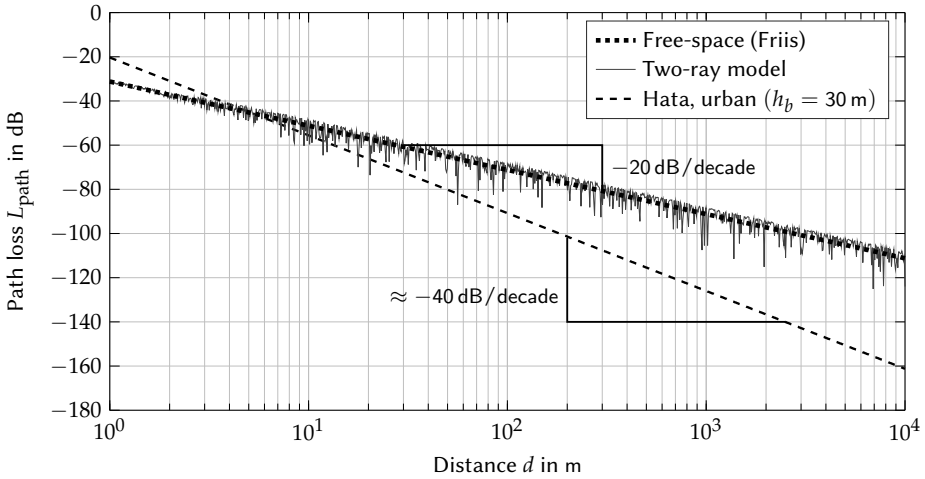


FIGURE 2.15 – *Propagation path loss at* 868 MHz*, considering the scenario given in Figure 2.14 unless otherwise specified.*

the baseband signal s_0 to be sufficient narrowband, i.e. $s_0\left(t-\tau_0(d)\right) \approx s_0\left(t-\tau_1(d)\right)$, (2.47) can be simplified to

$$r(t) = \underbrace{s_0\left(t-\tau_0(d)\right)\, e^{j2\pi f_{\mathrm{w}}(t-\tau_0(d))}}_{\text{Transmit signal}}\ \underbrace{a(\tau_0(d))\,\left\{1+\frac{a(\tau_1(d))}{a(\tau_0(d))}\, e^{j2\pi f_{\mathrm{w}}(\tau_0(d)-\tau_1(d))}\right\}}_{\text{Two-ray propagation impact} \rightarrow L_{\mathrm{path}}}. \tag{2.48}$$

Figure 2.15 illustrates the path loss

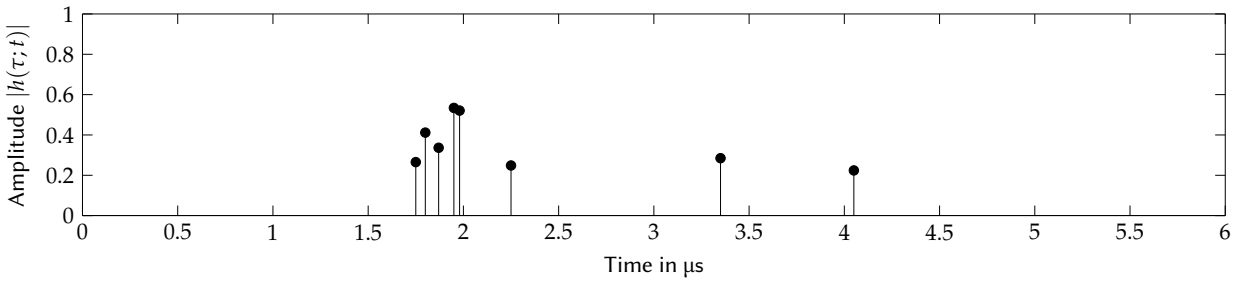
$$L_{\mathrm{path}} = \left| a(\tau_0(d))\,\left\{1+\frac{a(\tau_1(d))}{a(\tau_0(d))}\, e^{j2\pi f_{\mathrm{w}}(\tau_0(d)-\tau_1(d))}\right\}\right|, \tag{2.49}$$

over transmitter to receiver distance d for the two-ray propagation model, considering perfect ground reflection, as well as for free-space propagation according to Friis law with a path loss exponent $\gamma_L = 2$ and the Hata model [Hat80].

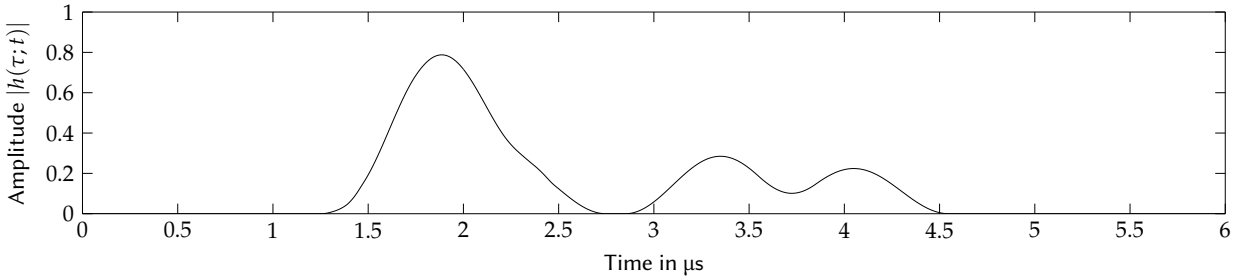
The two-ray model illustrates how constructive interference of the two paths adds 3 dB compared to free-space propagation, while destructive interference causes fading signals. The path loss according to the empirical Hata model has a path loss exponent $\gamma_L \approx 4$. Deriving ranging information for the RSSI requires prior knowledge of the present propagation scenario type/parameters, *e.g.* γ_L, in order to derive appropriate algorithms and associated parametrization. While parametric estimation suffers from arbitrary obstruction and small-scale fading, these features can be exploited in fingerprinting like approaches, which profit from large variations in the RSSI. However, fingerprinting methods require up to date RSSI maps, which is a challenge in time variant environments, i.e. varying obstruction through moving vehicles or the construction of buildings.

2.3.6.2 ToA

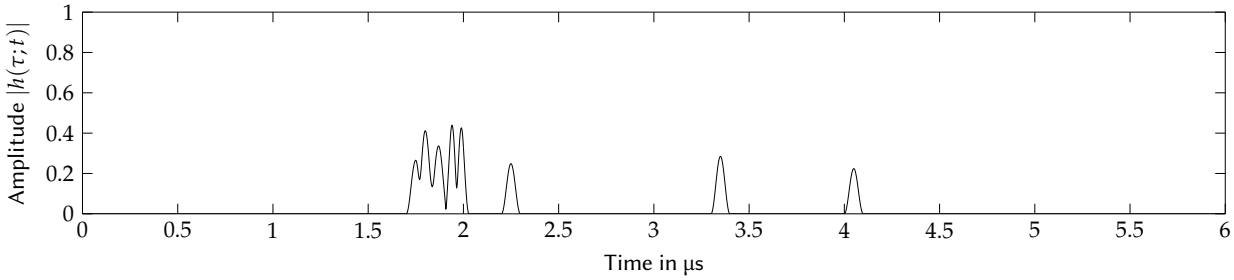
Free-space propagation is the ideal case for time based ranging methods, as the propagation delay is directly linked to the inter-node range. Multipath propagation adds further paths to the channel impulse response that, because of small-scale fading, can have larger amplitudes than the direct path despite their longer path. The ability to resolve the different paths in the channel impulse response depends on the signal bandwidth. Figure 2.16 illustrates the same radio channel, once sounded with a narrowband waveform and once with a wideband signal. The latter, results in a clear distinction of the multiple paths. However, in the case of the narrowband waveform, neighboring



(a) *Multipath channel realization according to the 3GPP ETU channel model [3GP08].*



(b) *Narrowband channel response ($B = 1\,\mathrm{MHz}$).*



(c) *Wideband channel response ($B = 10\,\mathrm{MHz}$).*

FIGURE 2.16 – *Time resolution for ToA estimation in a multipath channel.*

paths overlap and are superposed in the resulting channel response estimation. High-resolution algorithms [Sch86; PRK85; RK89] allow reducing the impact of multipath components on the estimation of the first path.

NLoS propagation, where the first path is strongly attenuated or completely absent, results in large ranging biases as only the delay of longer multipath components can be measured. Direct path prediction can be achieved in mobile scenarios based on the temporal evolution of multipath components [MDDU17]. Other methods include prior knowledge of the reflecting environment in a geometric approach to derive position in first path denied scenarios [Mei14]. These methods however require sufficient temporal resolution to track multipath components. Demonstrations in real setups are limited to (indoor) scenarios with UWB waveforms. Considering the positioning process, if more ranging estimates than the required minimum are available, a subset of unbiased ranging estimates can be selected to exclude NLoS measurements.

2.3.6.3 PoA

Phase shifts and propagation delays are proportional. In a free-space propagation scenario, range can be directly deduced from phase measurements considering ambiguity-resolving strategies as introduced in Chapter 1.5.2.8. In the case of coherent multi-channel ranging, i.e. pushing the ambiguity further away, the bandwidth is virtually increased through a sequential frequency hopping scheme Chapter 3.1, offering an improved temporal resolution of multipath components. As the concept is based on the extraction of range information from phase differences sequentially obtained over multiple frequencies, a time invariant scenario is required. Mobility during the sequential frequency hopping will result in additional contributions to the phase differences. Considering indoor LoS propagation with no/weak multipath, these additional phase terms can be linked to the node mobility and the estimated range/position corresponds to the temporal average during the frequency hopping process [PSSV09b;

Sch11]. The additional phase terms most likely become random in outdoor scenarios with strong multipath and subsequently range estimation fails in mobile scenarios.

Resolving the ambiguity by determining the number of carrier cycles between the node and the base station, as *e.g.* in phase based GNSS systems, requires almost free-space or LoS propagation with weak multipath. Strong multipath and obstructed visibility through nearby trees result in random phase shifts and makes carrier phase based positioning with centimeter-level accuracy very challenging [SD07].

2.3.7 Time Variant Channels

The time variation of the propagation channel can be beneficial as it allows statistical averaging of multiple measurements, *e.g.* RSSI measurements can be averaged to mitigate small-scale fading. However, phase based techniques, require either static conditions or a tractable mobility model combined with tight tracking of phase variations as phase information becomes otherwise random and useless. In the case of GNSS positioning, performing tight tracking of the carrier phase, satellite mobility helps algorithms to converge during the step of integer ambiguity resolution (see Chapter 1.5.2.8).

2.3.8 Interference, Immunity and Security

The radio channel considered so far is characterized by multipath propagation and thermal noise. Furthermore, real systems need to deal with different types of interference:

- Involuntary electromagnetic emissions, *e.g.* through electric motors or badly screened electrical devices.
- Other communication or Radio Detection and Ranging (RADAR) systems emitting in the same frequency band.

Involuntary emissions are regulated through Electromagnetic Compatibility (EMC) standards, while the cohabitation of multiple systems on the same spectrum resource aims at maximized spectrum usage and hence interference becomes unavoidable. Especially in the license free SRD and ISM bands where many LPWA systems operate alongside others, coordinated spectrum resource allocation between different, independent systems and operators is missing. This makes interference unavoidable [Zhe+19; BFT19]. Regulation (see Chapter 2.1.5) imposes techniques such as duty cycle limitations and LBT strategies that aim reducing interference and to guarantee to each user a fair access to the spectrum resource.

Considering radio signal based ranging and localization techniques, interference can be viewed as additional noise degrading the SNR of the useful signal, deteriorating localization metrics. In the case of too strong interference, the useful signal becomes unavailable and so the ranging/localization estimation. In the worst case, interference alters the radio signals in such a manner, that wrong positioning information is extracted, while the user is possibly not aware of this situation. Such altered position information can occur accidentally or intentionally through attacks. In GNSS systems different levels of voluntary interference [KH06] are called:

- Jamming: Voluntarily making the actual radio signal unavailable, i.e. through emissions of *e.g.* random, Continuous Wave (CW) or chirp waveforms with sufficient power compared to the useful signal power.
- Spoofing: Intentionally transmitting altered radio signals misleading the user, i.e. through the construction of radio signals corresponding to a different position.
- Meaconing: As spoofing requires the exact knowledge of the signal structure and their generation, meaconing simply replays previously recorded radio signals.

These techniques are equally relevant for LPWA localization. Integrity and security is also of concern for Internet of Things (IoT) applications and is hence widely studied for LPWA communication [ODDM17; ARLH17] and positioning [AEY10].

2.3.9 Choice of the Frequency Band

When designing a communication system, the choice of the frequency band needs to be considered. Different frequency bands can be compared under several technical, commercial and marketing criteria. Table 2.4 summarizes such a comparison.

The SRD and ISM frequency bands offer the advantage of license free and hence low-cost operation. The unavoidable interference in these crowded bands can be tackled with appropriate transceiver and waveform design, but also by adequate MAC layers. Antennas can be smaller in the SRD 868 MHz band and ISM 2.4 GHz band in comparison to the low frequency bands. Finally, the SRD 868 MHz band offers a long-range and an outdoor LPWA systems suited compromise, in terms of antenna size, free-space attenuation, building penetration and available

Frequency band	**ISM** 169 MHz	**ISM** 443 MHz	**SRD** 868 MHz	**GSM** 900 MHz	**ISM** 2.4 GHz
Wavelength $\lambda_W \propto$ Antenna size	1773.37 mm	692.15 mm	345.27 mm	333.33 mm	124.88 mm
Free-space attenuation $(C_{st0})^{dBm}$ at $d_0 = 1$ m	−16.99 dB	−25.17 dB	−31.21 dB	−31.53 dB	−40.05 dB
Maximum transmit power $(P_t)_{max}$	27 dBm	10 dBm	14 dBm	33 dBm	20 dBm
Propagation conditions	Sufficient obstacle/building penetration				
Interference	Myriad of unlicensed devices, *e.g.* temperature sensors, remote controls, interphones			No	WiFi, Bluetooth
Licensed	No	No	No	Yes	No
Existing LPWA solutions	LoRa SX127x [Sem16], Si446x [Sil16]				SX1280 [Sem17b]
	CC1125 [Tex16]			NB-IoT	
		S2_LP [STM16]			
Specificities			Easy transfer to the GSM 900 MHz band		

TABLE 2.4 – *Comparison of different frequency bands for LPWA technologies and localization.*

existing LPWA transceiver and network solutions. Another argument for this frequency band lies in its proximity to the 900 MHz Global System for Mobile Communications (GSM) band. This proximity offers network operators the easy option of migrating an entire LPWA network from the license free SRD or ISM band to the licensed spectrum in order to address interference issues. In the optimum case, this only requires a software reconfiguration of the network and the associated nodes.

Based on these arguments, the thesis focuses on the SRD 868 MHz band. The studied concepts can however be equally applied to other frequency bands. Utilizing the multi-channel technique, *e.g.* in the ISM 2.4 GHz band is especially appealing as a total of 80 MHz of license free spectrum are available offering increased temporal resolution.

2.4 Motivation and Thesis Orientation

The IoT aims at connecting all sorts of objects to the internet. Many of these things are either mobile or in remote locations requiring a wireless data transfer over several hundred meters to several ten kilometers. Furthermore, these objects are constraint in power consumption and need to be low-cost and low-complexity. Wireless connectivity to this type of objects is typically provided with radio transceivers belonging to the so-called LPWA networks.

Various applications require not only a wireless data transfer between the internet and the objects, but also knowledge about location of the latter. Obtaining positioning information for wirelessly connected objects can be achieved by different means. A multitude of technical solutions to determine the location of a device is known in the state of the art. Most likely and especially when precise positioning information is required, objects are equipped with a GNSS module.

GNSSs offer worldwide coverage and are hence suited to LPWA applications, as no individual infrastructure needs to be setup. Although meter-level accuracy is achievable by adding an extra GNSS receiver to the object,

use cases are limited to outdoor environments with clear sky visibility. Adding a GNSS receiver increases power consumption, hardware complexity and cost considerably.

These drawbacks are the main motivation why current research and development seeks to provide precise and accurate position information to LPWA networks by other means. Utilizing the data carrying radio signals transmitted by the LPWA transceivers of connected objects to the base station infrastructure, or vice-versa, is appealing in terms of complexity, cost and power consumption, especially on the objects. The existing base station infrastructure can be used for radio signal based trilateration or triangulation techniques.

However, radio localization with LPWA signals and the corresponding hardware poses several challenges. If precise position information is to be derived from LPWA signals transmitted over long ranges, parametric, amplitude based approaches can be excluded as ranging precision theoretically increases proportional with range. Mapping methods, i.e. fingerprinting, allows improving precision, but require the construction of geo-referenced amplitude maps. Temporal variations in the propagation environment and small-scale fading make meter-level precision impossible.

Consequently, LPWA radio signal based techniques for precise localization have to rely on time or phase metrics as GNSSs do, which achieve meter- or even centimeter-level precision. LPWA signals are typically narrowband to enable long-range communication. This makes radio localization challenging as precision is inverse proportional to available bandwidth. If narrowband transmissions are considered as an inevitable system constraint, multi-channel techniques can be employed to increase bandwidth sequentially by coherently grouping multiple signals of instantaneously narrow bandwidth.

The multi-channel technique has been applied to other radio technologies and standards, such as "Wireless Fidelity" (WiFi), Radio Frequency Identification (RFID) and Zigbee. There, it has been shown that the multi-channel approach improves precision compared to single channel time based positioning techniques. Its application to LPWA networks yet remains open and it is very appealing to implement multi-channel methods with LPWA signals. The technique allows combining sequentially transmitted narrowband to UNB transmissions for long-range communication with a large as well as scalable virtual bandwidth to improve localization precision.

Several challenges need to be addressed when applying the multi-channel principle to LPWA systems. Inter-device synchronization in time, frequency and phase has to be achieved and faces clock offsets, drifts and phase noise of low-cost oscillators. If all these hardware dependent challenges are mastered, the propagation channel remains as positioning accuracy and precision limiting factor. Multipath scenarios impede the geometric relationship between the position and measurable localization metrics. The multi-channel method provides an increased temporal resolution for the propagation channel estimation and allows hence an improved resolution of multipath components compared to single channel measurements. If this channel estimation does not provide accurate localization metrics, the quality information can at least be used to weight the metrics accordingly in the location solving process.

Moreover, device mobility or dynamics in the propagation channel can have an impact on localization metrics. The impact of mobility is expected to be an even greater issue when considering long transmission times due to narrowband waveforms and multiple sequentially transmitted packets.

The research in this thesis is oriented to investigate the feasibility of applying the multi-channel positioning technique to LPWA networks and addresses the aforementioned challenges. Trilateration based localization techniques rely on range measurements for position estimation. The quality of the final position estimate is directly linked to the accuracy and precision of multiple underlying range measurements. Hence, this thesis investigates the performances of multi-channel ranging between two LPWA devices, which then allows extrapolating the achievable positioning quality in LPWA networks. Advanced and prospective range estimation algorithms taking advantage of multi-channel transmissions are designed. These innovative algorithms aim at extracting the maximum positioning information from available LPWA signals.

The methodological approach of this thesis combines the derivation of theoretical ranging precision bounds with numerical simulation, hardware experimentation and field trials in real propagation scenarios. Considering this complete scope from theory to field trials allows studying all aspects and gives full understanding through iterating between these different steps. Developing a detailed signal model and deriving theoretical performance bounds provides transceiver hardware requirements and absolute lower limits of precision. Simulations allow confirming the signal model and allow benchmarking the performances of range estimation algorithms. The implementation of multi-channel ranging on a Software Defined Radio (SDR) based transceiver platform allows full flexibility and rapid prototyping. Experiments in a cabled and hence controlled propagation channel validate hypotheses made concerning transceiver hardware. Field trials are typically used for final validation and demonstration of a system and its features under real conditions. Hence, outdoor field trials complete this global approach and demonstrate the practical feasibility of multi-channel ranging with narrowband waveforms for accurate and precise localization of wireless connected objects in LPWA networks.

Bibliography of Chapter 2

[3GP08] 3GPP. *Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); Base Station (BS) radio transmission and reception (Release 8)*. 3rd Generation Partnership Project (3GPP), 2008.

[All83] D. W. Allan. *Clock characterization tutorial*. National Aeronautics, Space Administration, Office of Management, Scientific, and Technical Information Division, 1983.

[AEY10] W. Ammar, A. ElDawy, and M. Youssef. "Secure Localization in Wireless Sensor Networks: A Survey". In: *CoRR* abs/1004.3164 (2010). URL: http://arxiv.org/abs/1004.3164.

[ARLH17] E. Aras, G. S. Ramachandran, P. Lawrence, and D. Hughes. "Exploring the Security Vulnerabilities of LoRa". In: *2017 3rd IEEE International Conference on Cybernetics (CYBCONF)*. 2017, pp. 1–6.

[BFT19] M. A. Ben Temim, G. Ferre, and R. Tajan. "Analysis of the Coexistence of Ultra Narrow Band and Spread Spectrum Technologies in ISM Bands". In: *5th International Symposium on Ubiquitous Networking (UNet)*. 2019.

[BR07] Y. d. J. Bultitude and T. Rautiainen. "IST-4-027756 WINNER II D1. 1.2 V1. 2 WINNER II Channel Models". In: *EBITG, TUI, UOULU, CU/CRC, NOKIA, Tech. Rep., Tech. Rep* (2007).

[CEP18] CEPT. *ERC Recommendation 70-03*. Aug. 2018.

[Dec15] DecaWave. *DWM1000 Ultra Wideband (UWB) transceiver IC*. http://www.decawave.com/sites/default/files/resources/dwm1000-datasheet-v1.3.pdf. Accessed: 2020/07/31. 2015.

[Dem06] A. Demir. "Computing Timing Jitter From Phase Noise Spectra for Oscillators and Phase-Locked Loops With White and 1/f Noise". In: *IEEE Transactions on Circuits and Systems I: Regular Papers* 53.9 (2006), pp. 1869–1884. URL: http://ieeexplore.ieee.org/document/1703773/.

[DCM18] I. Dotlic, A. Connell, and M. McLaughlin. "Ranging Methods Utilizing Carrier Frequency Offset Estimation". In: *2018 15th Workshop on Positioning, Navigation and Communications (WPNC)*. 2018, pp. 1–6.

[ETS10] ETSI. *Universal Mobile Telecommunications System (UMTS); Deployment aspects (3GPP TR 25.943 version 9.0.0 Release 9)*. European Telecommunications Standards Institute (ETSI), 2010.

[ETS17] ETSI. *LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) radio transmission and reception (3GPP TS 36.101 version 13.6.1 Release 13)*. European Telecommunications Standards Institute (ETSI), 2017.

[Fed02] Federal Communications Commission (FCC). *Revision of Part 15 of the Commission's Rules Regarding Ultra-Wideband Transmission Systems* First Report and Order. Feb. 2002.

[Hat80] M. Hata. "Empirical Formula for Propagation Loss in Land Mobile Radio Services". In: *IEEE Transactions on Vehicular Technology* 29.3 (1980), pp. 317–325.

[ITU97] ITU. *Rec. ITU-R M.1225 1, Recommendation ITU-R M.1225, Guidelines For Evaluation Of Radio Transmission Technologies For IMT-2000*. International Telecommunication Union (ITU), 1997.

[JBH96] A. Jahn, H. Bischl, and G. Heiss. "Channel Characterisation for Spread Spectrum Satellite Communications". In: *Proceedings of ISSSTA'95 International Symposium on Spread Spectrum Techniques and Applications*. Vol. 3. 1996, 1221–1226 vol.3.

[KH06] E. Kaplan and C. Hegarty. *Understanding GPS: Principles and Applications*. Second Edition. Artech House, 2006.

[Lor] Lora Alliance. *What is the LoRaWAN Specification?* https://lora-alliance.org/about-lorawan. Accessed: 2020/07/31.

[LoR18] LoRaAlliance. *Geolocation Whitepaper*. https://lora-alliance.org/resource-hub/lora-alliance-geolocation-whitepaper. Accessed: 2020/07/31. 2018.

[MDDU17] J. Maceraudi, F. Dehmas, B. Denis, and B. Uguen. "Multipath-Aided Direct Path ToA Reconstruction for Integrated UWB Receivers in Generalized NLoS". In: *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)*. 2017, pp. 1–5.

[MGWW10] S. Marano, W. M. Gifford, H. Wymeersch, and M. Z. Win. "NLOS Identification and Mitigation for Localization based on UWB Experimental Data". In: *IEEE Journal on Selected Areas in Communications* 28.7 (2010), pp. 1026–1035.

[Mei14] P. Meissner. “Multipath-Assisted Indoor Positioning”. PhD thesis. Graz University of Technology, 2014.

[Mol+06] A. F. Molisch et al. “A Comprehensive Standardized Model for Ultrawideband Propagation Channels”. In: *IEEE Transactions on Antennas and Propagation* 54.11 (2006), pp. 3151–3166.

[ODDM17] B. Oniga, V. Dadarlat, E. De Poorter, and A. Munteanu. “Analysis, design and implementation of secure LoRaWAN sensor networks”. In: *2017 13th IEEE International Conference on Intelligent Computer Communication and Processing (ICCP)*. 2017, pp. 421–428.

[PRK85] A. Paulraj, R. Roy, and T. Kailath. “Estimation Of Signal Parameters Via Rotational Invariance Techniques- Esprit”. In: *Nineteeth Asilomar Conference on Circuits, Systems and Computers, 1985.* 1985, pp. 83–89.

[Pea05] K. Pearson. “Das Fehlergesetz Und Seine Verallgemeinerungen Durch Fechner Und Pearson. A Rejoinder”. In: *Biometrika* 4.1-2 (1905), pp. 169–212.

[PSSV09b] M. Pichler, S. Schwarzer, A. Stelzer, and M. Vossiek. “Positioning with moving IEEE 802.15.4 (ZigBee) transponders”. In: *2009 IEEE MTT-S International Microwave Workshop on Wireless Sensing, Local Positioning, and RFID*. 2009, pp. 1–4.

[Pro01] J. G. Proakis. *Digital Communications*. Ed. by F. Edition. McGraw-Hill Higher Education, 2001.

[Rap+96] T. S. Rappaport et al. *Wireless Communications: Principles and Practice*. Vol. 2. prentice hall PTR New Jersey, 1996.

[RK89] R. Roy and T. Kailath. “ESPRIT-Estimation of Signal Parameters Via Rotational Invariance Techniques”. In: *IEEE Transactions on Acoustics, Speech, and Signal Processing* 37.7 (1989), pp. 984–995.

[SGG08] Z. Sahinoglu, S. Gezici, and I. Guvenc. “Ultra-Wideband Positioning Systems”. In: *Cambridge, New York* (2008).

[Sch86] R. Schmidt. “Multiple Emitter Location and Signal Parameter Estimation”. In: *IEEE Transactions on Antennas and Propagation* 34.3 (1986), pp. 276–280.

[SD07] S. Schon and F. DilBner. “Challenges for GNSS-based high precision positioning – some geodetic aspects”. In: *2007 4th Workshop on Positioning, Navigation and Communication*. 2007, pp. 229–237.

[Sch11] S. Schwarzer. “Entwicklung eines industriellen Funkortungssystems basierend auf der kohaerenten Kombination von Kommunikationssignalen mit IEEE-802.15.4-Geraeten”. PhD thesis. Technischen Universitaet Clausthal, 2011.

[Sema] Semtech. *SX1257 - Low Power Digital I and Q RF Multi-PHY Mode Analog Front End 860-1000 MHz*. https://www.semtech.com/uploads/documents/DS_SX1257_V1.2.pdf. Accessed: 2020/07/31.

[Semc] Semtech. *SX1301 - Digital Baseband Chip for outdoor LoRaWAN macro gateways*. https://www.semtech.com/uploads/documents/sx1301.pdf. Accessed: 2020/07/31.

[Sem16] Semtech. *SX1276/77/78/79 - 137 MHz to 1020 MHz Low Power Long Range Transceiver*. http://www.semtech.com/images/datasheet/sx1276.pdf. Accessed: 2020/07/31. Aug. 2016.

[Sem17b] Semtech. *SX1280/SX1281 Long Range, Low Power, 2.4 GHz Transceiver with Ranging Capability*. 2017.

[Sig] Sigfox. *Sigfox, a 0G Network*. https://www.sigfox.com/. Accessed: 2020/07/31.

[Sil16] Silicon Labs. *High-Performance, Low-Current Transceiver: Si4464/63/61/60*. 2016.

[Sit+11] Y. L. Sit et al. “The OFDM Joint Radar-Communication System: An Overview”. In: *The Third International Conference on Advances in Satellite and Space Communications, Budapest, Hungary* (2011).

[Sit17] Y. L. Sit. “MIMO OFDM Radar-Communication System with Mutual Interference Cancellation”. PhD thesis. Karlsruhe Institute of Technology, 2017.

[STM16] STMicroelectronics. *S2-LP Ultra-low power, high performance, sub-1GHz transceiver*. http://www.st.com/content/ccc/resource/technical/document/datasheet/group3/bd/26/62/81/3d/86/4d/15/DM00339133/files/DM00339133.pdf/jcr:content/translations/en.DM00339133.pdf. Nov. 2016.

[Tex16] Texas Instruments. *CC1125 Ultra-High Performance RF Narrowband Transceiver*. http://www.ti.com/lit/ds/swrs120e/swrs120e.pdf. 2016.

[Ubl] Ublox. *High precision GNSS performance for the mass market: NEO-M8P series*. https://www.u-blox.com/en/product/neo-m8p-series. Accessed: 2020/07/31.

[Vig16] J. R. Vig. *Quartz Crystal Resonators and Oscillators - For Frequency Control and Timing Applications - A Tutorial*. https://ieee-uffc.org/download/quartz-crystal-resonators-and-oscillators-for-frequency-control-and-timing-applications-a-tutorial-2/. Accessed: 2020/07/31. 2016.

[WA86] F. L. Walls and D. W. Allan. "Measurements of Frequency Stability". In: *Proceedings of the IEEE* 74.1 (1986), pp. 162–168.

[Zhe+19] C. Zheng et al. "Copula-Based Interference Models for IoT Wireless Networks". In: *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*. 2019, pp. 1–6.

3

Coherent Multi-Channel Ranging

"La science est un effort vers la Création. La religion est un effort vers le Créateur."

— Édouard Branly (1844 – 1940)

Chapter contents

Multi-channel ranging allows combining narrowband instantaneous transmissions with large virtual bandwidths for precise positioning and is hence compatible with Low Power Wide Area (LPWA) transceivers. The principle of multi-channel ranging is discussed and a detailed signal model presented. Based on this signal model, hardware requirements are deducted and theoretical performance bounds derived. Range estimation algorithms are constructed and initial simulation results in an Additive White Gaussian Noise (AWGN) channel are presented.

3.1 Principle of Multi-Channel Ranging

Narrowband LPWA signals do not allow getting precise time based ranging/positioning as outlined in Chapter 2.1.1. The fundamental limit for the ranging precision is given by the Cramer Rao Lower Bound (CRLB) from (1.43) as

$$\sqrt{\mathrm{Var}\left(\widehat{t_{\mathrm{A}}}\right)} = \sqrt{\frac{1}{4\pi^2 \frac{E_{\mathrm{S}}}{N_0} B_{\mathrm{RMS}}^2}}, \tag{3.1}$$

with the so-called Root Mean Square (RMS) bandwidth conditioning the CRLB according to Appendix B.2

$$B_{\mathrm{RMS}} = \sqrt{\int_{-\infty}^{\infty} f^2 \left|S_0(f)\right|^2 df \Big/ \int_{-\infty}^{\infty} \left|S_0(f)\right|^2 df}, \tag{3.2}$$

where $S_0(f)$ represents the spectrum of the waveform s_0.

Time based ranging systems employ signals covering a possibly large instantaneous bandwidth B, *e.g.* Ultra-Wide Band (UWB) ranging systems. Considering a rectangular shape of the spectrum S_0 as depicted in Figure 3.1a, the RMS bandwidth is given by

$$B_{\mathrm{RMS}} = \sqrt{\int_{-B/2}^{B/2} f^2 \left|S_0\right|^2 df \Big/ \int_{-B/2}^{B/2} \left|S_0\right|^2 df} = \frac{B}{\sqrt{12}}. \tag{3.3}$$

Increasing bandwidth B improves ranging precision. It is inversely possible to optimize the ranging precision and simultaneously minimize the instantaneous occupied bandwidth B by modifying the spectrum shape $S_0(f)$. Intuitively, the solution to this optimization is given by two spectral peaks with an infinite spacing. Theoretically, instantaneous bandwidth is zero, i.e. $B = 0$. Infinite spacing is technically not possible as frequencies cannot be arbitrary high. Restricting the spacing to a maximum allowed spectum excursion B_{virt}, results in the spectrum occupation depicted in Figure 3.1b with two spectral peaks at $\pm B_{\mathrm{virt}}/2$. The RMS bandwidth evaluates to

$$B_{\mathrm{RMS}} = \sqrt{\left[\left(-\frac{B_{\mathrm{virt}}}{2}\right)^2 \left|S_0\right|^2 + \left(\frac{B_{\mathrm{virt}}}{2}\right)^2 \left|S_0\right|^2\right] \Big/ \left[\left|S_0\right|^2 + \left|S_0\right|^2\right]} = \frac{B_{\mathrm{virt}}}{2}. \tag{3.4}$$

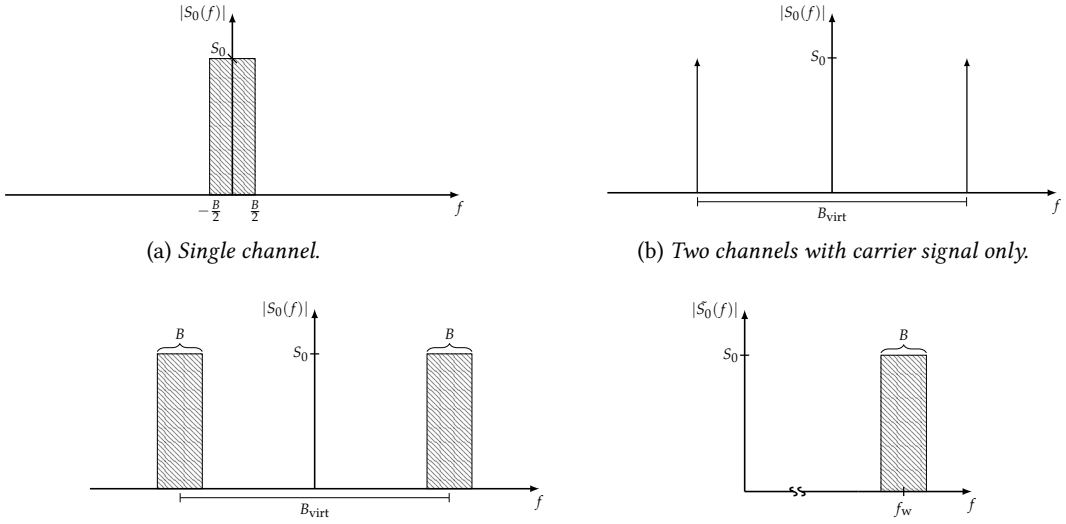
In the case that these spectral peaks correspond to narrowband transmissions of bandwidth B as illustrated in Figure 3.1c, the RMS bandwidth is given by

$$B_{\mathrm{RMS}} = \sqrt{\frac{B^2 + 3B_{\mathrm{virt}}^2}{12}}. \tag{3.5}$$

Comparing (3.3) and (3.5), it can be concluded that for equal ranging precision, it is not necessary to occupy a contiguous spectrum, but it is sufficient to have a maximum excursion. Furthermore, there is no temporal condition on when these spectral rays need to be transmitted. Simultaneous or sequential transmission are possible. However, to maintain $S_0(f)$ as a whole, relative phase coherence between the spectral peaks needs to be guaranteed (see Chapter 3.2.3). This relative phase coherence is defined by the relative phase rotation, bound in the interval $[0, 2\pi]$, of the spectral peaks in the complex plane.

So far, the baseband spectrum $S_0(f)$ has been considered, where relative phase coherence within the spectrum is required. Absolute phase relation is obtained by phase ambiguity resolution, i.e. determining the integer number of 2π phase rotations. If this absolute phase relation is guaranteed, the RMS bandwidth is given by

$$B_{\mathrm{RMS}} = \sqrt{\frac{B^2}{12} + f_{\mathrm{w}}^2}, \tag{3.6}$$



(a) *Single channel.* (b) *Two channels with carrier signal only.*

(c) *Two channels with signal of bandwidth B.* (d) *RTK-GPS.*

FIGURE 3.1 – *Signal spectrum S_0 of the radio ranging waveform s_0 for different ranging precisions.*

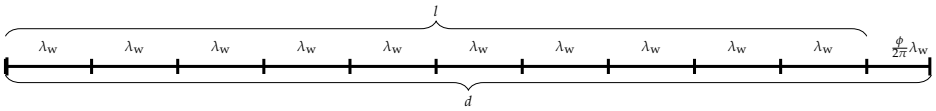


FIGURE 3.2 – *Relation between real range d, phase measurement ϕ and 2π ambiguity.*

with passband spectrum $\tilde{S_0}$ of bandwidth B and carrier frequency f_{w} as depicted in Figure 3.1d. Consequently, ranging precision on the carrier wavelength scale can be achieved. This technique is applied by the Real-Time Kinematic GPS (RTK-GPS), where absolute phase relation between transmitter and receiver is established by resolving the integer ambiguity (see Chapter 1.5.2.8). Centimeter ranging precision is achievable with a decimeter-level carrier wavelength λ_{w} (see Table 1.8).

Obtaining a large RMS bandwidth through a peak spectrum as depicted in Figure 3.1c, and hence improved ranging precision is compatible with the LPWA system constraint of instantaneously narrowband transmissions to achieve long-range communication. Such a LPWA compatible peak spectrum can be generated by sequentially transmitting multiple narrowband transmissions on different frequencies.

Transmitting a signal with a spectrum $S_0(f)$ containing spectral peaks at frequencies f_c can be interpreted as sampling the channel transfer function $H(f)$ at these frequencies f_c. For sufficiently narrowband signals representing the spectral peak, an amplitude and a phase measurement at the carrier frequency f_{w} characterizes the channel transfer function.

The two-way phase measurement between two nodes spaced by a distance $\widehat{d}_{\text{PoF}}$ is given according to (1.65) by

$$\widehat{\phi_{\text{A}c}} = -4\pi f_c \frac{\widehat{d}_{\text{PoF}}}{c_0} + 2\pi l. \tag{3.7}$$

The 2π ambiguity of a phase measurement is taken into account with the integer cycle ambiguity l. The relationship between phase measurement, actual range and integer ambiguity is depicted in Figure 3.2.

Solving (3.7) is not possible due to the two unknown variables $\widehat{d}_{\text{PoF}}$ and l which cannot be obtained from a single phase observation. Assuming an arbitrary l, *e.g.* $l = 0$ allows determining distance $\widehat{d}_{\text{PoF}}$ with an ambiguity on the wavelength scale. For sub-GHz frequencies, this distance estimation has hence a decimeter-level ambiguity.

However, considering two phase measurements at different frequencies f_1 and f_2, results in the equation set

$$\widehat{\phi_{\text{A}1}} = -4\pi f_1 \frac{\widehat{d}_{\text{PoF}}}{c_0} + 2\pi l_1, \tag{3.8a}$$

$$\widehat{\phi_{\text{A}2}} = -4\pi f_2 \frac{\widehat{d}_{\text{PoF}}}{c_0} + 2\pi l_2. \tag{3.8b}$$

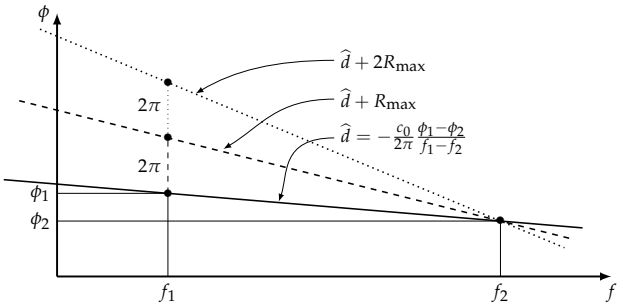


FIGURE 3.3 – *Relation between the 2π ambiguity on phase measurements and the resulting range ambiguity $R_{\max}$ for multi-channel ranging.*

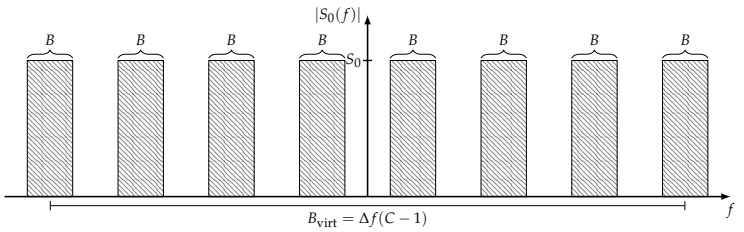


FIGURE 3.4 – *Signal spectrum S_0 of the radio ranging waveform s_0 for multi-channel ranging with C channels and a channel spacing Δf.*

Calculating the phase difference and resolving for $\widehat{d}_{\text{PoF}}$ results in

$$\widehat{d}_{\text{PoF}} = c_0 \frac{\widehat{\phi_{\text{A1}}} - \widehat{\phi_{\text{A2}}}}{-4\pi\,(f_1 - f_2)} + c_0 \frac{l_1 - l_2}{2\,(f_1 - f_2)}. \tag{3.9}$$

For sufficiently close frequencies f_1 and f_2, the ranging ambiguity can be increased. Figure 3.3 illustrates how 2π periodicity and range ambiguity are related. Large virtual bandwidth $B_{\text{virt}} = |f_1 - f_2|$ is required on one hand for large RMS bandwidth and high ranging precision. On the other hand, range ambiguity is proportional to the virtual wavelength defined by the spacing of adjacent channel frequencies. Sufficiently large virtual wavelength is required for large range ambiguity, so that the latter can be resolved by other means, *e.g.* through time based range estimation (see (1.74), [SVPS08]).

Maintaining the total virtual bandwidth and increasing range ambiguity can be achieved by inserting further peaks in the spectrum as depicted in Figure 3.4. Subsequently, for a total of C spectral peaks with an uniform spacing Δf, range resolution ΔR and range ambiguity $R_{\max}$ are given by

$$\Delta R = \frac{c_0}{2B_{\text{virt}}} = \frac{c_0}{2\Delta f(C-1)}, \tag{3.10a}$$

$$R_{\max} = \frac{c_0}{2\Delta f}, \tag{3.10b}$$

with virtual bandwidth $B_{\text{virt}} = \Delta f(C-1)$. The RMS bandwidth for this case can be obtained by generalizing (3.5) and is given by

$$B_{\text{RMS}} = \sqrt{\frac{B^2 + \Delta f^2(C^2-1)}{12}}. \tag{3.11}$$

Sequentially transmitting multiple narrowband signals between two LPWA nodes can be realized in a two-way ranging protocol as depicted in Figure 3.5.

Adding supplementary peaks, i.e. inserting additional sampling points on $H(f)$, gives not only an increased range ambiguity but allows also reconstructing more complex channel transfer functions as illustrated in Figure 3.6.

In the case of multipath propagation the phase measurement can be modelled by

$$\widehat{\phi_{\text{A}c}} = -4\pi f_c \frac{\widehat{d}_{\text{PoF}}}{c_0} + 2\pi l + \varphi_c, \tag{3.12}$$

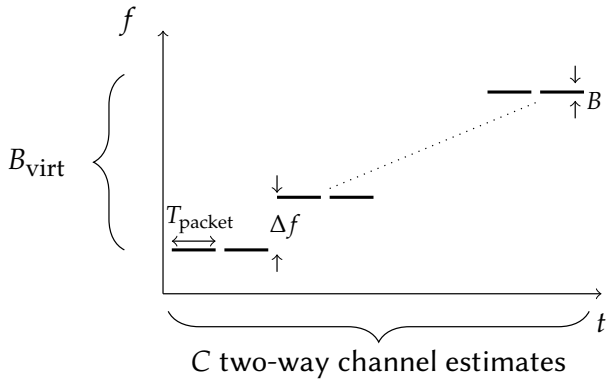
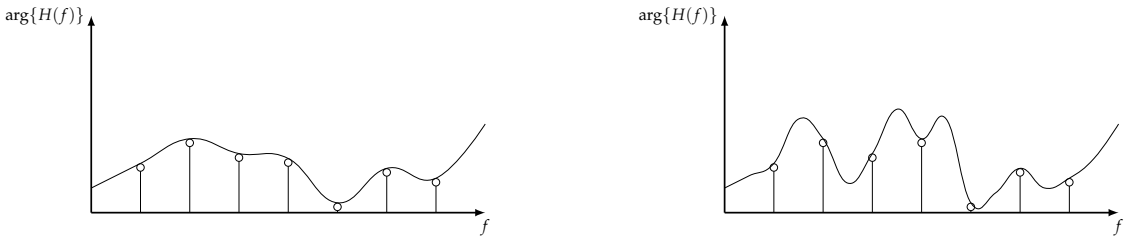


FIGURE 3.5 – *Time-frequency plan for two-way multi-channel ranging with C narrowband signals of instantaneous bandwidth B and a channel spacing Δf.*



(a) *Channel spacing $\Delta f < B_{\text{coh}}$.* (b) *Channel spacing $\Delta f > B_{\text{coh}}$ (undersampling).*

FIGURE 3.6 – *Sampling the channel transfer function $H(f)$ at discrete frequencies.*

with the multipath induced phase shift φ_c. For a channel spacing Δf sufficiently small, *e.g.* smaller than the channel coherence bandwidth B_{coh}, adjacent channels will experience similar multipath dependent phase shifts

$$\varphi_c \approx \varphi_{c+1}, \quad \text{if } \Delta f < B_{\text{coh}}, \tag{3.13}$$

allowing to cancel their contribution by calculating the difference $\widehat{\varphi_{\text{A}c}} - \widehat{\varphi_{\text{A}c+1}}$. In fact, this condition is equivalent to the Shannon sampling theorem [Sha48].

The Shannon sampling theorem in time domain requires at least two sampling points per signal period. Equivalent the sampling frequency must be larger than the spectral occupation. Likewise, the Shannon theorem in frequency domain requires at least two channel measurements within the coherence bandwidth according to (3.13). Utilizing the definition of the coherence bandwidth from (2.38), allows rewriting (3.13) as

$$\Delta f < B_{\text{coh}} = \frac{1}{T_{\text{m}}} \underset{\sim}{\propto} \frac{1}{\tau_{\text{max}}}, \tag{3.14}$$

with empircal proportionality between multipath spread T_{m} and the maximum excess delay τ_{max}. A small frequency spacing Δf needs to be chosen such that the temporal support of the Channel Impulse Response (CIR) is larger than the longest significant multipath component. Multipath components undergo temporal aliasing if this condition is not fulfilled.

RTK-GPS positioning in contrast to multi-channel ranging relies on a phase measurement on a single frequency and resolves the integer ambiguity through iterative processing in order to converge to an unique solution and through more than the required minimum number of satellites. RTK-GPS operation in multipath scenarios adds the supplementary unknown φ_c to the already underdetermined set of equations, which explains why resolving integer ambiguities in multipath propagation scenarios is unfeasible.

Multi-channel ranging according to Figure 3.4 and Figure 3.5 can be compared to Step Frequency RADAR (SF-RADAR) or channel estimation in multi-carrier communication systems *e.g.* Orthogonal Frequency Division Multiplexing (OFDM). Channel estimation for communication purposes aims at overcoming frequency selective fading, *e.g.* through channel equalization. Contrarily to multi-channel ranging, absolute time delay between transmitter and receiver are not of interest, requiring no specific synchronization procedure such as two-way ranging. In monostatic Radio Detection and Ranging (RADAR) systems, transmitter and receiver are co-located, which simplifies synchronization issues. Furthermore, range estimation is performed with a passive target, which is not required to be coordinated in terms of an active two-way exchange.

In the following, the general signal model for coherent multi-channel ranging is presented.

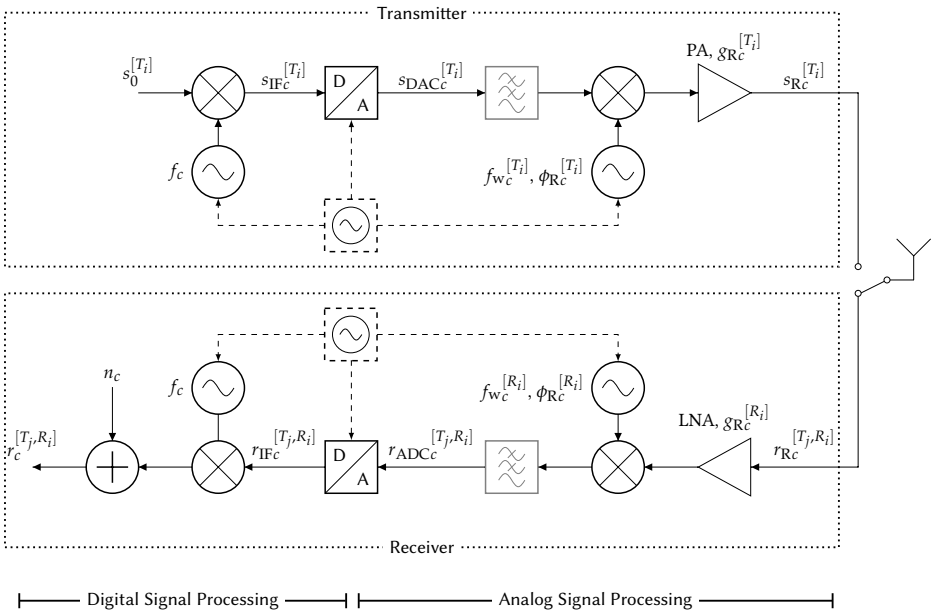


FIGURE 3.7 – *General radio transceiver architecture adapted to multi-channel ranging.*

3.2 Ranging Signal Model

3.2.1 General Radio Transceiver Signal Model

Developing a general radio transceiver signal model for multi-channel ranging, allows the in-depth study of performance bounds such as the CRLBs as well as simulating radio signals to benchmark ranging metric extraction algorithms under various conditions. Furthermore, implementation related hardware requirements can be illustrated based on the signal model.

The following signal model considers a general radio transceiver structure comprising a digital signal-processing unit adapted to multi-channel ranging as well as digital to analog conversion and baseband to pass band frequency translation through an analog mixing stage. Figure 3.7 illustrates such a general transceiver architecture, where the baseband signal is up- and down-converted in both, a numerical and an analog stage to maintain the required phase coherence.

The signal model and the underlying notation have been inspired by [PSSV09a; Sch11] and are modified for the purpose of LPWA ranging.

The transmitter and the receiver of node i are denoted T_i and R_i respectively. Physical quantities assigned to a transmitter or receiver X are denoted $(\cdot)^{[X]}$ and variables concerning a transmission from transmitter X to receiver Y are denoted $(\cdot)^{[X,Y]}$.

Furthermore, the following hypotheses are made:

- Analog signals and sampling are derived from a common clock source, implicating that Sampling Frequency Offset (SFO) and Carrier Frequency Offset (CFO) are linked (see (3.18) and (3.20)).
- Quantification of numerical signals is not taken into account by the model. Quantification noise can however be integrated into the final noise term $n_c^{[T,R]}$ (see (3.28)).
- Radio frequency blocks such as filters, Power Amplifiers (PAs), Low Noise Amplifiers (LNAs) and switches are assumed to have a deterministic behavior which can be summarized in a complex gain $g_{\mathrm{R}c}^{[X]}$ for a given frequency f_c/channel c as LPWA signals are assumed sufficiently narrowband (see (3.21) and (3.25)).
- The transmitted waveform s_0 is sufficiently narrowband, so that frequency flat fading can be assumed and the radio channel can be characterized approximately by a time variant complex amplitude $A_c^{[T,R]}(t)$ at f_c or $f_c\left(1+\delta_f^{[T]}\right)$ integrating a multipath scenario (see (3.24)).
- Interference is not considered in this signal model and AWGN is added on the final baseband received signal (see (3.27)).

The signal model in Chapter 3.2.1.1 gives the step by step explanation details for all processing blocks from Figure 3.7. The final signal model and parameters are presented in Chapter 3.2.1.2.

3.2.1.1 Signal Model Derivation

The samples of the baseband transmit waveform are described by $s_0\left[k'\right]$ with $k' \in [0, K_S - 1]$ and a total of K_S samples. The nominal sampling period is given by T_{Samp}. Considering a zero-order interpolation in digital to analog conversion, the continuous version of the baseband waveform with transmission start time instant, i.e. the Time of Departure (ToD) $t_D^{[T]}$, is given by

$$s_0^{[T]}(t) = \sum_{k'=0}^{K_S-1} \Pi_{T_{\text{Samp}}}\left(t - t_D^{[T]} - k' T_{\text{Samp}}\right) s_0\left[k'\right], \tag{3.15}$$

with a rectangular window

$$\Pi_{T_{\text{Samp}}}(t) = \begin{cases} 1, & \text{for } t \in [0, T_{\text{Samp}}), \\ 0, & \text{else.} \end{cases} \tag{3.16}$$

The waveform $s_0\left[k'\right]$ is a priori known to both the transmitter T and the receiver R. If the waveform constitutes the preamble of a LPWA packet, the receiver knows this preamble for synchronization purposes. If the waveform contains the entire packet, the receiver can first demodulate the packet and then reconstruct the transmit waveform under the hypothesis that demodulation can be achieved free of error.

For the channel c, the baseband waveform is numerically up-converted to channel Intermediate Frequency (IF) f_c by

$$s_{\text{IF}c}^{[T]}[k] = s_0^{[T]}\left(kT_{\text{Samp}}\right) e^{j2\pi f_c k T_{\text{Samp}}} \quad \text{or} \quad s_{\text{IF}c}^{[T]}(t) = s_0^{[T]}(t)\, e^{j2\pi f_c t}. \tag{3.17}$$

It has to be noted, that no phase shift term is added in this up-conversion since it is a pure numerical process.

For digital to analog conversion, the local time scale of transmitter/receiver X integrating time offset and time dilatation, is given by

$$t^{[X]} = \left(1 + \delta_f^{[X]}\right) t + t_0^{[X]}, \tag{3.18}$$

with global time t, normalized frequency offset $\delta_f^{[X]}$ and time offset $t_0^{[X]}$.

Using (3.18) to pass from local to global time base and for ideal digital to analog conversion, the analog IF signal is given by

$$s_{\text{DAC}c}^{[T]}(t) = s_{\text{IF}c}^{[T]}\left(t^{[T]}\right) = s_{\text{IF}c}^{[T]}\left(\left(1 + \delta_f^{[T]}\right) t + t_0^{[T]}\right). \tag{3.19}$$

This analog IF signal is finally up-mixed with an oscillator of instantaneous phase

$$\begin{aligned} \phi_c^{[T]}(t) &= 2\pi \int_0^t f_{\text{w}c}\left(1 + \delta_f^{[T]} + \delta_f'^{[T]}(\gamma)\right) d\gamma + \phi_{\text{PN}}^{[T]}(t) \\ &= 2\pi \underbrace{\left(1 + \delta_f^{[T]}\right) f_{\text{w}c}}_{f_{\text{w}c}^{[T]}} t + \underbrace{\phi_{\text{R}c}^{[T]} + 2\pi f_{\text{w}c} \int_0^t \delta_f'^{[T]}(\gamma)\, d\gamma + \phi_{\text{PN}}^{[T]}(t)}_{\tilde{\phi}_{\text{R}c}^{[T]}(t)}, \end{aligned} \tag{3.20}$$

according to (2.4). The Radio Frequency (RF) signal is given in complex notation by

$$s_{\text{R}c}^{[T]}(t) = g_{\text{R}c}^{[T]}\, s_{\text{DAC}c}^{[T]}(t) e^{j\left(2\pi f_{\text{w}c}^{[T]} t + \tilde{\phi}_{\text{R}c}^{[T]}(t)\right)}, \tag{3.21}$$

with actual carrier frequency $f_{\text{w}c}^{[T]}$, which is together with sampling, derived from the same clock source. For the general case, carrier frequency can be different for every channel c, inducing a different initial oscillator phase $\phi_{\text{R}c}^{[T]}$ *e.g.* through reprogramming of the Phase-Locked Loop (PLL). RF gains and phase shifts are summarized in $g_{\text{R}c}^{[T]}$, these are deterministic and can be calibrated.

The RF signal is transmitted over the wireless radio channel and received by receiver R. The received signal, omitting AWGN, is given by

$$r_{\mathrm{R}c}^{[R]}(t) = s_{\mathrm{R}c}^{[T]}(t) * h^{[T,R]}(\tau;t), \tag{3.22}$$

with CIR $h^{[T,R]}(\tau;t)$ between transmitter T and receiver R as defined by (2.18). Under the assumption of a narrowband signal $s_0(t)$, the radio channel at frequency $\left(1+\delta_f^{[T]}\right)\left(f_{\mathrm{w}c}^{[T]}+f_c\right)$ can be summarized as complex coefficient $A_c^{[T,R]}$ and the received signal is given by

$$r_{\mathrm{R}c}^{[T,R]}(t) = A_c^{[T,R]}(t)\, s_{\mathrm{R}c}^{[T]}\left(t-\tau_0^{[T,R]}\right), \tag{3.23}$$

with

$$A_c^{[T,R]}(t) = \alpha_c^{[T,R]}(t)e^{j\varphi_c^{[T,R]}(t)} = \sum_{p=0}^{P^{[T,R]}(t)-1} a_p^{[T,R]}(t)e^{-j2\pi\left(1+\delta_f^{[T]}\right)(f_{\mathrm{w}c}+f_c)\left(\tau_p^{[T,R]}(t)-\tau_0^{[T,R]}(t)\right)}, \tag{3.24}$$

according to (2.18). The propagation delay between transmitter T and receiver R is denoted $\tau_0^{[T,R]} = d^{[T,R]}/c_0$ with transmitter to receiver distance $d^{[T,R]}$ and radio wave propagation velocity c_0.

After down-conversion, the analog IF signal is given by

$$r_{\mathrm{ADC}c}^{[T,R]}(t) = g_{\mathrm{R}c}^{[R]}\, r_{\mathrm{R}c}^{[T,R]}(t)e^{-j\left(2\pi f_{\mathrm{w}c}^{[R]}t+\tilde{\phi}_{\mathrm{R}c}^{[R]}(t)\right)}, \tag{3.25}$$

with $g_{\mathrm{R}c}^{[R]}$, $f_{\mathrm{w}c}^{[R]}$ and unknown phase $\tilde{\phi}_{\mathrm{R}c}^{[R]}(t)$ equivalent to those defined at the transmitter.

Analog to digital conversion on receiver local time scale $t^{[R]}$ yields

$$r_{\mathrm{IF}c}^{[T,R]}\left(t^{[R]}\right) = r_{\mathrm{ADC}c}^{[T,R]}\left(\frac{t^{[R]}-t_0^{[R]}}{1+\delta_f^{[R]}}\right). \tag{3.26}$$

The samples at $t^{[R]} = kT_{\mathrm{Samp}}$ are finally numerically down-converted to baseband and adding AWGN n_c to consider noise of all stages, gives the final received signal

$$r_c^{[T,R]}[k] = r_{\mathrm{IF}c}^{[T,R]}\left(kT_{\mathrm{Samp}}\right)e^{-j2\pi f_c kT_{\mathrm{Samp}}} + n_c^{[T,R]}[k]. \tag{3.27}$$

The received signal in (3.27) can be expressed as function of the baseband waveform s_0, by combining (3.15) to (3.26).

3.2.1.2 Final Signal Model

In summary, the received signal on channel c yields

$$r_c^{[T,R]}[k] = g_{\mathrm{R}c}^{[T]}\, g_{\mathrm{R}c}^{[R]}\, \alpha_c^{[T,R]}\left(\frac{kT_{\mathrm{Samp}}-t_0^{[R]}}{1+\delta_f^{[R]}}\right)\left\{\sum_{k'=0}^{K_{\mathrm{S}}-1}\Pi_{T_{\mathrm{Samp}}}\left(\delta_{\mathrm{T}}^{[T,R]}\left(kT_{\mathrm{Samp}}-t_{\mathrm{A}c}^{[T,R]}\right)-k'T_{\mathrm{Samp}}\right)s_0\left[k'\right]\right\}$$
$$\cdot e^{j\left(2\pi\delta_f^{[T,R]}(f_{\mathrm{w}c}+f_c)kT_{\mathrm{Samp}}+\phi_{\mathrm{A}c}^{[T,R]}[k]\right)} + n_c^{[T,R]}[k], \tag{3.28}$$

with the following parameters given by:

- **Hardware gains** $g_{\mathrm{R}c}^{[T]}$ and $g_{\mathrm{R}c}^{[R]}$: Various filter, amplifier and mixer gains are summarized in the complex gains, which depend on the actual frequency and are hence channel and implementation dependent. The complex gains can be determined and compensated in a calibration step.
- **Channel amplitude**

$$\alpha_c^{[T,R]}(t) = \left|A_c^{[T,R]}(t)\right| = \left|\sum_{p=0}^{P^{[T,R]}(t)-1} a_p^{[T,R]}(t)e^{-j2\pi\left(\left(1+\delta_f^{[T]}\right)f_{\mathrm{w}c}+f_c\right)\left(\tau_p^{[T,R]}(t)-\tau_0^{[T,R]}(t)\right)}\right|, \tag{3.29}$$

  as frequency flat fading can be assumed on each channel c due to narrowband transmissions. The channel amplitude varies on every channel, taking multipath propagation into account (3.24).

- **Time dilatation**

$$\delta_{\mathrm{T}}^{[T,R]} = \frac{1+\delta_f^{[T]}}{1+\delta_f^{[R]}}, \tag{3.30}$$

  accounts for stretching or compressing of sampling time.

- **Time of Arrival (ToA)**: In receiver time basis the ToA is given by

$$t_{\mathrm{A}c}^{[T,R]} = \left(1+\delta_f^{[R]}\right)\tau_0^{[T,R]} + t_0^{[R]} + \frac{1+\delta_f^{[R]}}{1+\delta_f^{[T]}}\left(t_{\mathrm{D}}^{[T]} - t_0^{[T]}\right). \tag{3.31}$$

  The ToA estimate will be greater for a larger propagation delay $\tau_0^{[T,R]}$, the receiver being started earlier $t_0^{[R]}$ or a later transmission by the transmitter on $t_{\mathrm{D}}^{[T]}$. A transmission being started at an earlier $t_0^{[T]}$ reduces the ToA.

- **Frequency offset**

$$\delta_f^{[T,R]} = \frac{\delta_f^{[T]} - \delta_f^{[R]}}{1+\delta_f^{[R]}}. \tag{3.32}$$

- **Phase of Arrival (PoA)**

$$\begin{aligned}\phi_{\mathrm{A}c}^{[T,R]}[k] = &-2\pi\left(1+\delta_f^{[T]}\right)\left(f_{\mathrm{w}c}+f_c\right)\tau_0^{[T,R]} + \varphi_c^{[T,R]}\left(\frac{kT_{\mathrm{Samp}} - t_0^{[R]}}{1+\delta_f^{[R]}}\right)\\ &+ 2\pi f_c t_0^{[T]} - 2\pi\left(\frac{\left(\delta_f^{[T]} - \delta_f^{[R]}\right)f_{\mathrm{w}c} + \left(1+\delta_f^{[T]}\right)f_c}{1+\delta_f^{[R]}}\right)t_0^{[R]}\\ &+ \tilde{\phi}_{\mathrm{R}}{}_c^{[T]}\left(\frac{kT_{\mathrm{Samp}} - t_0^{[R]}}{1+\delta_f^{[R]}} - \tau_0^{[T,R]}\right) - \tilde{\phi}_{\mathrm{R}}{}_c^{[R]}\left(\frac{kT_{\mathrm{Samp}} - t_0^{[R]}}{1+\delta_f^{[R]}}\right).\end{aligned} \tag{3.33}$$

  The phase term comprises the phase rotation due to the propagation delay, phase offsets due to time offsets between transmitter and receiver t_0, as well as initial phase, integrating frequency drift and phase noise according to (3.20).

- **Noise** $n_c^{[T,R]}$, comprising thermal noise, quantification noise and as noise considered interference.

For the purpose of communication the receiver aims estimating $s_0[k']$ from the received signal $r_c^{[T,R]}[k]$ in (3.28), compensating the parameters given in (3.29) to (3.33). In contrast to communication, for ranging and localization, the receiver, knowing $s_0[k']$, extracts the parameters, i.e. localization metrics given by (3.29) to (3.33) from (3.28). Localization metric extraction algorithms are presented in Chapter 3.4.1 and the estimates from such algorithms can be described by:

$$\widehat{\alpha_c}^{[T,R]}(t) = \alpha_c^{[T,R]}(t) + \epsilon_{\widehat{\alpha_c}(t)}^{[T,R]}, \tag{3.34a}$$

$$\widehat{\delta_{\mathrm{T}}}^{[T,R]} = \delta_{\mathrm{T}}^{[T,R]} + \epsilon_{\widehat{\delta_{\mathrm{T}}}}^{[T,R]}, \tag{3.34b}$$

$$\widehat{t_{\mathrm{A}c}}^{[T,R]} = t_{\mathrm{A}c}^{[T,R]} + \epsilon_{\widehat{t_{\mathrm{A}c}}}^{[T,R]}, \tag{3.34c}$$

$$\widehat{\delta_f}^{[T,R]} = \delta_f^{[T,R]} + \epsilon_{\widehat{\delta_f}}^{[T,R]}, \tag{3.34d}$$

$$\widehat{\phi_{\mathrm{A}c}}^{[T,R]}[k] = \phi_{\mathrm{A}c}^{[T,R]}[k] + \epsilon_{\widehat{\phi_{\mathrm{A}c}}[k]}^{[T,R]}, \tag{3.34e}$$

where $\epsilon_{(\cdot)}^{[T,R]}$ denotes the estimation error on a given localization metric.

3.2.1.3 Comparison of the Signal Model to Previous Work in the State of the Art

The signal model introduced in this thesis, aiming at LPWA applications, differs in several points from the transceiver signal model presented in [PSSV09a; Sch11] which is designed for ZigBee systems.

The work in [PSSV09a; Sch11] assumes a frequency synthesis for the local oscillator which guarantees deterministic phase relation between the clock reference for digital signal generation and the carrier signal. This can be achieved with an integer PLL and it ensures that the carrier to reference clock phase relation is time invariant for a given carrier frequency. Furthermore, the signal model assumes constant and identical time intervals between every channel and a specific symmetric up-down hopping scheme, which allows combining two phase measurements on the same channel so that frequency offset related errors cancel. These hardware requirements and a restricted hopping scheme, moreover allow estimating $H(f)$ from $H^2(f)$ by determining the 2^C-state error function due to the fact that the square-root of a complex number has two solutions [SS10]. Estimating $H(f)$ instead of $H^2(f)$ improves temporal resolution by a factor 2, as well as it avoids phantom propagation paths that arise in $H^2(f)$ (see Chapter 3.4.2.3).

The signal model of this thesis does not make any hypothesis on the type of frequency synthesis, as phase coherence between different points in time for a same channel is not required. Cancellation of frequency offset related errors is achieved by classical CFO estimation.

In the LPWA context, where packet transmissions can last up to one second, it is advantageous or even necessary to avoid restrictions regarding equal time intervals for packet transmissions. This degree of freedom, required for low-power operation and in order to be regulation compliant, is traded against the ability to reconstruct $H(f)$.

Furthermore, the signal model directly integrates multipath propagation modeling which allows deriving lower bounds on the ranging precision in these scenarios (see Chapter 3.3).

Temporal frequency drift is integrated into the signal model to investigate its impact on LPWA transmissions which last longer that Zigbee packets. Phase noise is equally integrated so that oscillator specifications can be given as function of the required ranging precision.

3.2.2 Two-Way Ranging Signal Model

Performing an unique packet transmission between two nodes, does not allow estimating the propagation delay τ_0, as (3.31) contains also the time offsets between the two nodes. Therefore a Time of Flight (ToF) protocol is applied in order to cancel unknown time offsets.

In the following, two protocols are presented. First, a protocol with an initiating node, sending a packet to a node that responds after the reception of the initiating packet. The second protocol assumes that nodes are coarsely aligned to timeslots via a Medium Access Control (MAC) protocol. Both two-way protocols are depicted in Figure 3.8 and the resulting localization metrics are detailed in the following.

For the purpose of simplification, the following restrictive hypotheses are made:

- Transmitter and receiver signals of a node i are derived from the same clock source

$$t_0^{[T_i]} = t_0^{[R_i]}, \tag{3.35a}$$
$$\delta_f^{[T_i]} = \delta_f^{[R_i]}. \tag{3.35b}$$

- Node 1 is assumed to be aligned to global time

$$t_0^{[T_1]} = t_0^{[R_1]} = 0, \qquad t_0^{[T_2]} = t_0^{[R_2]} = t_0, \tag{3.36a}$$
$$\delta_f^{[T_1]} = \delta_f^{[R_1]} = 0, \qquad \delta_f^{[T_2]} = \delta_f^{[R_2]} = \delta_f. \tag{3.36b}$$

- The radio channel is assumed to be reciprocal and time invariant

$$a_p^{[T_1,R_2]}(t) = a_p^{[T_2,R_1]}(t) = a_p, \tag{3.37a}$$
$$\tau_p^{[T_1,R_2]}(t) = \tau_p^{[T_2,R_1]}(t) = \tau_p, \tag{3.37b}$$
$$A_c^{[T,R]}(t) = A_c^{[T,R]}. \tag{3.37c}$$

- Clock source frequency drift and oscillators phase noise are neglected

$$\tilde{\phi}_{\mathrm{R}\,c}^{[X]}(t) = \phi_{\mathrm{R}c}^{[X]}. \tag{3.38}$$

3.2.2.1 Ping-Pong Two-Way Ranging Protocol

According to Figure 3.8a, node 1 initiates the ranging process by sending a packet at local transmission time instant $t_{\mathrm{D}}^{[T_1]} = 0$, corresponding to $k = 0$. Node 2 receives the packet in its local time at time instant $t_{\mathrm{A}c}^{[T_1,R_2]}$ as $r_c^{[T_1,R_2]}[k]$. The node synchronizes to the packet and obtains the ToA estimation $\widehat{t_{\mathrm{A}c}}^{[T_1,R_2]}$. After reception, node 2 switches to transmit mode and sends the response packet at time instant

$$t_{\mathrm{D}}^{[T_2]} = \left\lceil \frac{\widehat{t_{\mathrm{A}c}}^{[T_1,R_2]}}{T_{\mathrm{Samp}}} \right\rceil T_{\mathrm{Samp}} + K_{\mathrm{S}} T_{\mathrm{Samp}}, \tag{3.39}$$

corresponding to the next integer sampling point. Meanwhile, node 1 has completed transmission and switches after a sampling time $k = K_{\mathrm{S}}$ to reception mode. The return packet received by node 1 is described by $\tilde{r_c}^{[T_2,R_1]}[\tilde{k}] = r_c^{[T_2,R_1]}[\tilde{k} + K_{\mathrm{S}}]$.

The localization metrics (3.29) to (3.33) can be expressed for the two received signals $r_c^{[T_1,R_2]}[k]$ and $\tilde{r_c}^{[T_2,R_1]}[\tilde{k}]$ with the simplifications (3.35) to (3.38) as:

- **Channel amplitude**

$$\alpha_c^{[T_1,R_2]} \approx \alpha_c^{[T_2,R_1]} \approx \left| \sum_{p=0}^{P^{[T_2,R_1]}(t)-1} a_p e^{-j2\pi(f_{\mathrm{w}c}+f_c)(\tau_p-\tau_0)} \right|, \tag{3.40}$$

  where frequency offset is neglected as the channel is assumed sufficiently frequency flat fading.

- **Time dilatation**

$$\delta_{\mathrm{T}}^{[T_1,R_2]} = \frac{1}{1+\delta_f}, \tag{3.41a}$$

$$\delta_{\mathrm{T}}^{[T_2,R_1]} = 1 + \delta_f. \tag{3.41b}$$

- **ToA**

$$t_{\mathrm{A}c}^{[T_1,R_2]} = \left(1+\delta_f\right)\tau_0 + t_0, \tag{3.42a}$$

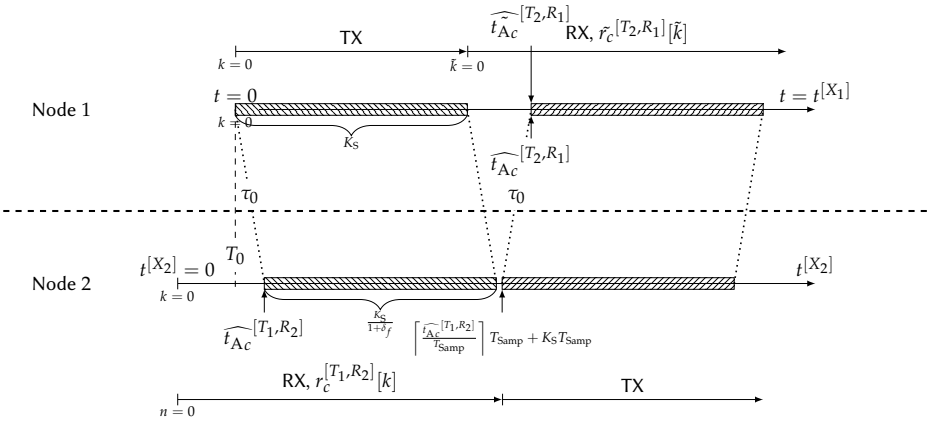
$$\begin{aligned} \tilde{t_{\mathrm{A}c}}^{[T_2,R_1]} &= \tau_0 + \frac{1}{1+\delta_f}\left(t_{\mathrm{D}}^{[T_2]} - t_0\right) - K_{\mathrm{S}} T_{\mathrm{Samp}} \\ &= \tau_0 + \frac{1}{1+\delta_f}\left(\left\lceil \frac{\widehat{t_{\mathrm{A}c}}^{[T_1,R_2]}}{T_{\mathrm{Samp}}} \right\rceil T_{\mathrm{Samp}} + K_{\mathrm{S}} T_{\mathrm{Samp}} - t_0\right) - K_{\mathrm{S}} T_{\mathrm{Samp}} \\ &= 2\tau_0 - \frac{\delta_f}{1+\delta_f} K_{\mathrm{S}} T_{\mathrm{Samp}} + \frac{1}{1+\delta_f}\epsilon_{\widehat{t_{\mathrm{A}c}}}^{[T_1,R_2]}. \end{aligned} \tag{3.42b}$$

  The propagation delay τ_0 can be extracted from (3.42b) under the knowledge of frequency offset δ_f, in order to compensate the second term corresponding to the fact that node 1 does not know the actual response time of node 2 (see Chapter 2.2.1). The last term comprises the uncertainty in ToA estimation at node 2 and the timing error arising from discrete time. For sufficient high sampling frequency, this error is negligible compared to the ToA estimation error which depends on signal bandwidth and symbol energy to noise spectral density ratio (see Chapter 3.3.1).

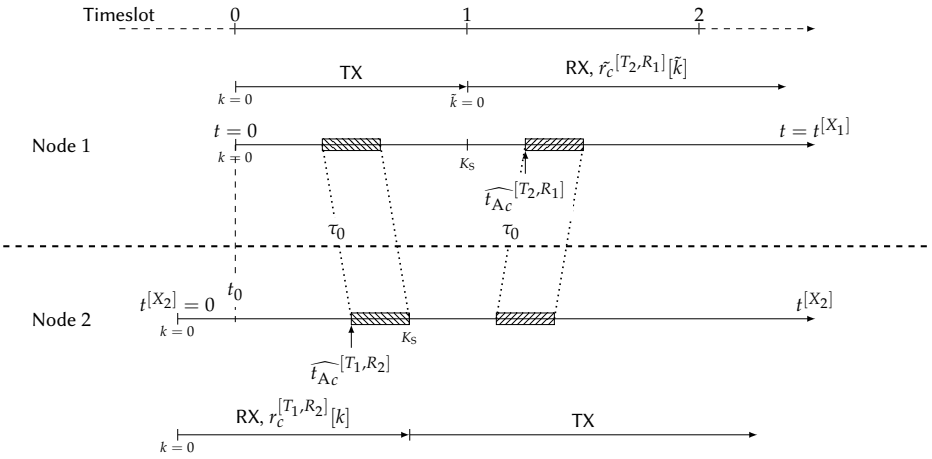
- **Frequency offset**

$$\delta_f^{[T_1,R_2]} = -\frac{\delta_f}{1+\delta_f}, \tag{3.43a}$$

$$\delta_f^{[T_2,R_1]} = \delta_f. \tag{3.43b}$$



(a) *Ping-pong two-way ranging protocol.*



(b) *Timeslot two-way ranging protocol.*

FIGURE 3.8 – *Two-way ranging protocols.*

- **PoA**

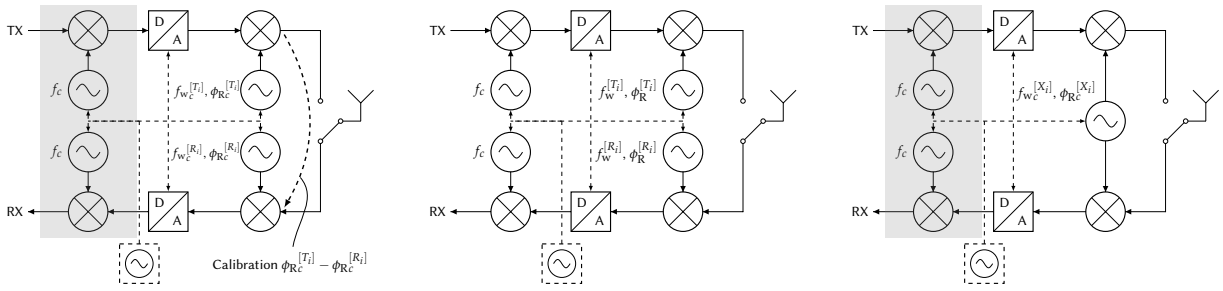
$$\phi_{\mathrm{A}c}^{[T_1,R_2]} = -2\pi\left(f_{\mathrm{w}c}+f_c\right)\tau_0 \quad +\varphi_c - 2\pi\left(\frac{-\delta_f f_{\mathrm{w}c}+f_c}{1+\delta_f}\right)t_0 \quad +\phi_{\mathrm{R}c}^{[T_1]}-\phi_{\mathrm{R}c}^{[R_2]}, \tag{3.44a}$$

$$\begin{aligned}\tilde{\phi_{\mathrm{A}c}}^{[T_2,R_1]} = &-2\pi\left(1+\delta_f\right)\left(f_{\mathrm{w}c}+f_c\right)\tau_0 \quad +\varphi_c+2\pi f_c t_0 \quad +\phi_{\mathrm{R}c}^{[T_2]}-\phi_{\mathrm{R}c}^{[R_1]}\\ &+2\pi\delta_f^{[T_2,R_1]}\left(f_{\mathrm{w}c}+f_c\right)K_\mathrm{S}T_\mathrm{Samp}.\end{aligned} \tag{3.44b}$$

3.2.2.2 Timeslot Two-Way Ranging Protocol

In the timeslot two-way ranging protocol depicted in Figure 3.8b, both nodes are coarsely aligned to common timeslots. It is assumed without loss of generality, that node 1 is the reference node perfectly aligned to these timeslots, i.e. node 1 can be the base station serving as network coordinator scheduling the MAC layer timeslots. Every node transmits or receives in its assigned slots, independently from any events, contrarily to the ping-pong two-way protocol.

Localization metrics are the same as for the ping-pong two-way protocol with the difference of the ToA estimate at node 1, as node 2 transmits at $t_\mathrm{D}^{[T_2]} = K_\mathrm{S}T_\mathrm{Samp}$. Hence, the ToA is given by:



(a) *Transmitter to receiver phase sum-difference calibration on each channel.*

(b) *Unknown but constant absolute phase sum-difference.*

(c) *Common Local Oscillator (LO) for transmitter and receiver, no phase sum-difference.*

FIGURE 3.9 – *Radio transceiver hardware architecture requirements for multi-channel ranging.*

- **ToA**

$$t_{\mathrm{A}c}^{[T_1,R_2]} = \left(1+\delta_f\right)\tau_0 + t_0, \tag{3.45a}$$

$$\begin{aligned} \tilde{t_{\mathrm{A}c}}^{[T_2,R_1]} &= \tau_0 + \frac{1}{1+\delta_f}\left(t_{\mathrm{D}}^{[T_2]} - t_0\right) - K_{\mathrm{S}}T_{\mathrm{Samp}} \\ &= \tau_0 + \frac{1}{1+\delta_f}\left(T_{\mathrm{Samp}}K_{\mathrm{S}} - t_0\right) - K_{\mathrm{S}}T_{\mathrm{Samp}} \\ &= \tau_0 - \frac{1}{1+\delta_f}t_0 - \frac{\delta_f}{1+\delta_f}K_{\mathrm{S}}T_{\mathrm{Samp}}. \end{aligned} \tag{3.45b}$$

In order to obtain the propagation delay τ_0, (3.45a) and (3.45b) have to be summed and in the ideal case, i.e. without CFO and for perfect ToA estimation the time offset t_0 cancels and the ToF yields

$$\text{Ideal case} \qquad t_{\mathrm{A}c}^{[T_1,R_2]} + \tilde{t_{\mathrm{A}c}}^{[T_2,R_1]} = 2\tau_0. \tag{3.46}$$

The detailed ToF expression taking ToA estimation errors and CFO into account is given in Chapter 3.4.2.1.

3.2.3 Radiotransceiver Hardware Architecture Requirements

Multi-channel ranging reconstructs an estimation of the channel transfer function H based on amplitude estimations $a_c^{[T,R]}$ and phase estimates $\varphi_c^{[T,R]}$ given by (3.40) and (3.44) respectively. However, as it is the case with time estimates $t_{\mathrm{A}c}^{[T,R]}$, phase estimates depend on the unknown time offset t_0, which can be cancelled by summing $\phi_{\mathrm{A}c}^{[T_1,R_2]}$ and $\phi_{\mathrm{A}c}^{[T_2,R_1]}$ equivalent to multiplying $\widehat{H}_{\mathrm{PoA}_c}^{[T_1,R_2]}$ with $\widehat{H}_{\mathrm{PoA}_c}^{[T_2,R_1]}$ to obtain an estimation of $\widehat{H}_{\mathrm{PoF}_c}$.

The argument $\arg\left(\widehat{H}_{\mathrm{PoF}_c}\right)$ is given by the sum of (3.44a) and (3.44b). In the ideal case, i.e. without CFO and for perfect PoA estimation the time offset term $2\pi f_c t_0$ cancels and the Phase of Flight (PoF) yields

$$\begin{aligned} \text{Ideal case} \qquad \arg\left(\widehat{H}_{\mathrm{PoF}_c}\right) &= \phi_{\mathrm{A}c}^{[T_1,R_2]} + \tilde{\phi_{\mathrm{A}c}}^{[T_2,R_1]} \\ &= -2\pi\, 2\left(f_{\mathrm{w}c} + f_c\right)\tau_0 + 2\varphi_c + \underbrace{\phi_{\mathrm{R}c}^{[T_1]} - \phi_{\mathrm{R}c}^{[R_2]} + \phi_{\mathrm{R}c}^{[T_2]} - \phi_{\mathrm{R}c}^{[R_1]}}_{\Sigma\Delta\phi_{\mathrm{R}c}}. \end{aligned} \tag{3.47}$$

The detailed PoF expression taking PoA estimation errors and CFO into account is given in Chapter 3.4.2.2.

The sum-difference of initial oscillator phases $\Sigma\Delta\phi_{\mathrm{R}c} = \phi_{\mathrm{R}c}^{[T_1]} - \phi_{\mathrm{R}c}^{[R_2]} + \phi_{\mathrm{R}c}^{[T_2]} - \phi_{\mathrm{R}c}^{[R_1]}$ needs either to be known or constant over different channels c, so that ranging information τ can be extracted.

Different transceiver realizations can achieve these requirements:

1. **Independent transmitter and receiver local oscillators combined with phase difference calibration**: The transceiver allows estimating $\phi_{\mathrm{R}c}^{[T_i]} - \phi_{\mathrm{R}c}^{[R_i]}$ and its contribution on $\arg\left(\widehat{H}_{\mathrm{PoF}_c}\right)$ in (3.47) can be subtracted, i.e. $\Sigma\Delta\phi_{\mathrm{R}c}$ is known. Calibration can be performed by exploiting the unwanted but unavoidable transmitter to receiver leakage on a radio transceiver chip. Figure 3.9a illustrates the corresponding architecture where transmitter or receiver PLL can be reprogrammed between channels but require to be continuously running between calibration and operation phase.

2. **Independent transmitter and receiver local oscillators and numerical IF mixing by a numerical local oscillator common to transmitter and receiver branch**: Maintaining carrier frequency $f_{\mathrm{w}c} = f_{\mathrm{w}} = \text{const.}$ over all channels c and running local oscillators without interruption during the entire multi-channel two-way ranging protocol implies that there is only one initial phase per oscillator, i.e. $\phi_{\mathrm{R}c}^{[X]} = \phi_{\mathrm{R}}^{[X]}$. Figure 3.9b illustrates this case where $\Sigma\Delta\phi_{\mathrm{R}c} = \Sigma\Delta\phi_{\mathrm{R}} = \text{const.}$ is a constant phase rotation of the multi-channel transfer function estimation $\widehat{H}_{\mathrm{PoF}_c}$.
3. **Common local oscillator for transmitter and receiver**: When transmitter and receiver share a common oscillator as in Figure 3.9c, initial phases cancel as $\phi_{\mathrm{R}c}^{[T_i]} = \phi_{\mathrm{R}c}^{[R_i]}$, i.e. $\Sigma\Delta\phi_{\mathrm{R}c} = 0$.

The transceiver realizations 1 and 3 equally allow switching the multi-channel frequency by changing the carrier frequency $f_{\mathrm{w}c}$ and keeping $f_c = \text{const.}$. This is possible as $\Sigma\Delta\phi_{\mathrm{R}c}$ is calibrated (realization 1) or zero (realization 3) for every channel. Performing multi-channel frequency switching only in analog domain, simplifies the transceiver architecture as the numerical IF mixing stage can be omitted.

It is difficult to state whether commercially available LPWA transceivers (see Table 1.3) fulfill the radio transceiver architecture requirements for two-way multi-channel ranging. In-depth study and testing is necessary to determine the compatibility of chipsets with the requirements regarding phase coherence and access to the localization metrics. Reverse engineering has to be applied when constructors do not disclose relevant information.

3.3 Theoretical Performance Bounds

3.3.1 Introduction to Theoretical Performance Bounds

Estimating an unknown parameter θ based on a given observation $\tilde{R}(\theta)$ can be described with tools from estimation theory [Kay93]. In real-world systems the observation $\tilde{R}(\theta)$ is not ideal, *e.g.* noisy or biased. The statistics of an observation $\tilde{R}(\theta)$ for a given θ can be described by the probability distribution function $p\left(\tilde{R}(\theta)|\theta\right)$. Based on this conditional probability, statistical lower bounds on the estimation quality of the unknown parameter θ can be derived. The so-called CRLB [VT04] or the Ziv Zakai Lower Bound (ZZLB) [CZZ75] can be used for this purpose.

While the CRLB is straightforward to derive, it is not tight in the strong noise regime. The ZZLB provides a tighter bound in such a case, however it is more complex to derive.

3.3.1.1 CRLB and ZZLB for ToA Estimation

Considering ToA estimation, the noisy observation is given by the received signal r which is a delayed version of the transmit signal s_0

$$r(t,\tau) = s_0(t-\tau) + n(t), \tag{3.48}$$

with ToA delay τ and noise n. Considering the noise n to be AWGN, the CRLB is given by (1.43) (see full derivation in Appendix B.2) and the ZZLB by [DW09] as

$$\sqrt{\mathrm{Var}\left(\widehat{t_{\mathrm{A}}}\right)_{\mathrm{ZZLB}}} = \sqrt{\frac{1}{T}\int_0^T t(T-t)P_{\min}(t)dt}, \tag{3.49}$$

with observation window length T and

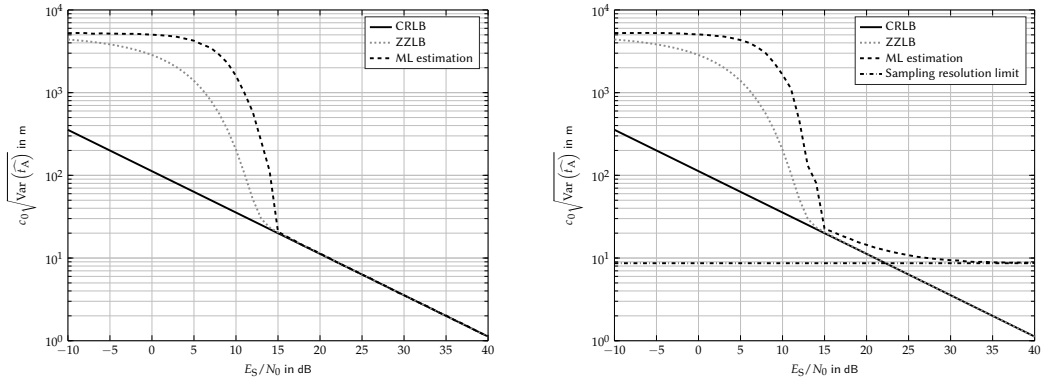
$$P_{\min}(t) = Q\left(\sqrt{\frac{E_{\mathrm{S}}}{N_0}\left[1-\tilde{\Omega}_{s_0,s_0}(t)\right]}\right), \tag{3.50}$$

with normalized autocorrelation function $\tilde{\Omega}_{s_0,s_0}$ of the transmit signal s_0 of energy E_{S}.

Figure 3.10a illustrates the CRLB, the ZZLB as well as a numerical simulation of ToA estimation through the Maximum Likelihood (ML) estimator. The transmit signal s_0 is given by a Gaussian pulse of width $T_{\mathrm{pulse}} = 1\,\mu\mathrm{s}$ corresponding to a bandwidth $B = 1\,\mathrm{MHz}$. Simulations are performed with a sampling frequency $f_{\mathrm{Samp}} = 1000\,\mathrm{MHz}$.

For low E_{S}/N_0, the ZZLB gives the tighter bound to predict ToA precision. It actually takes into account that the ToA estimation error is uniformly distributed in $[0,T)$. Practically, the observation window T will be sufficiently limited *e.g.* by the MAC layer.

Figure 3.10b shows the same simulation results for a lower sampling frequency $f_{\mathrm{Samp}} = 10\,\mathrm{MHz}$, showing a level out of the simulated ToA precision. In fact, ToA precision is no longer bound by the observation noise n but



(a) *Sampling frequency* $f_{\mathrm{Samp}} = 1000\,\mathrm{MHz}$. (b) *Sampling frequency* $f_{\mathrm{Samp}} = 10\,\mathrm{MHz}$.

FIGURE 3.10 – *ToA CRLB, ZZLB and ML estimation for a Gaussian pulse of bandwidth* $B = 1\,\mathrm{MHz}$.

by the uniform distributed sampling resolution error [LZP11]

$$\epsilon_{T_{\mathrm{Samp}}} = \frac{1}{\sqrt{12} f_{\mathrm{Samp}}}. \tag{3.51}$$

The following study only considers the CRLB due to the straightforward derivation. This is justified by the fact that technically relevant E_S/N_0 levels for ToA estimation lie in the zone where the CRLB is tight.

3.3.1.2 General CRLB Formulation with AWGN

In the case of observations with AWGN the CRLB can be calculated in a simplified form [Kay93]. The unknown estimation parameter is given by $\boldsymbol{\theta} = \left[\theta_0, \cdots, \theta_{P-1}\right]^T$ and the observation in the form $\tilde{\boldsymbol{R}}(\boldsymbol{\theta}) = \left[\tilde{R}_0(\boldsymbol{\theta}), \cdots, \tilde{R}_{K-1}(\boldsymbol{\theta})\right]^T$. For AWGN follows

$$\tilde{\boldsymbol{R}}(\boldsymbol{\theta}) \sim \mathcal{N}\left(\boldsymbol{R}(\boldsymbol{\theta}), \boldsymbol{\Sigma}_{\boldsymbol{R}}\right), \tag{3.52}$$

with observation model $\boldsymbol{R}(\boldsymbol{\theta})$ and noise covariance matrix $\boldsymbol{\Sigma}_{\boldsymbol{R}}$. The CRLB on estimators of the unknown estimation parameter $\boldsymbol{\theta}$ is given by

$$\mathrm{Var}\left(\widehat{\boldsymbol{\theta}}\right) \geq \mathrm{trace}\left[\boldsymbol{I}^{-1}(\boldsymbol{\theta})\right], \tag{3.53}$$

with Fisher Information Matrix (FIM)

$$\boldsymbol{I}(\boldsymbol{\theta}) = \boldsymbol{J}^T(\boldsymbol{\theta})\, \boldsymbol{\Sigma}_{\boldsymbol{R}}^{-1}\, \boldsymbol{J}(\boldsymbol{\theta}) \tag{3.54}$$

and Jacobian Matrix (JM)

$$\boldsymbol{J}(\boldsymbol{\theta}) = \begin{pmatrix} \frac{\partial R_0(\boldsymbol{\theta})}{\partial \theta_0} & \cdots & \frac{\partial R_0(\boldsymbol{\theta})}{\partial \theta_{P-1}} \\ \vdots & & \vdots \\ \frac{\partial R_{K-1}(\boldsymbol{\theta})}{\partial \theta_0} & \cdots & \frac{\partial R_{K-1}(\boldsymbol{\theta})}{\partial \theta_{P-1}} \end{pmatrix}. \tag{3.55}$$

In the case that prior information on the unknown estimation parameter $\boldsymbol{\theta}$ is available, the CRLB from (3.53) can be modified and is given by

$$\mathrm{Var}\left(\widehat{\boldsymbol{\theta}}\right) \geq \mathrm{trace}\left(\left(\boldsymbol{I}(\boldsymbol{\theta}) + \boldsymbol{\Sigma}_{\boldsymbol{\theta}}^{-1}\right)^{-1}\right), \tag{3.56}$$

with prior information covariance matrix $\boldsymbol{\Sigma}_{\boldsymbol{\theta}}$ on the unknown estimation parameter $\boldsymbol{\theta}$. This covariance matrix allows modelling *e.g.* constraints or other information available on the parameters θ_p, prior to estimation of $\boldsymbol{\theta}$.

3.3.2 CRLB Formulation for Multi-Channel Ranging

In the following, the CRLB for multi-channel ranging according to the timeslot two-way ranging protocol from Chapter 3.2.2.2 is derived. Without loss of generality, the bounds are calculated for the radio transceiver architecture with independent transmit and receive local oscillator and a common IF mixing stage (see Figure 3.9b).

Nodes 2 and 1 obtain respectively the set of C received signals $r_c^{[T_1,R_2]}$ and $r_c^{[T_2,R_1]}$ according to (3.28). With parameters given by (3.40), (3.41), (3.45), (3.43) and (3.44). The signals received by one node on C channels are combined into

$$\boldsymbol{r}^{[T,R]}[k] = \tilde{\boldsymbol{r}}^{[T,R]}[k] + \tilde{\boldsymbol{n}}^{[T,R]}[k], \tag{3.57}$$

with noise free received signal

$$\tilde{\boldsymbol{r}}^{[T,R]}[k] = \begin{pmatrix} \mathcal{R}\left\{\tilde{r}_0^{[T,R]}[k]\right\} \\ \mathcal{I}\left\{\tilde{r}_0^{[T,R]}[k]\right\} \\ \vdots \\ \mathcal{R}\left\{\tilde{r}_{C-1}^{[T,R]}[k]\right\} \\ \mathcal{I}\left\{\tilde{r}_{C-1}^{[T,R]}[k]\right\} \end{pmatrix} \in \mathbb{R}^{2C\times 1}, \tag{3.58}$$

separating real ($\mathcal{R}$, in-phase) and imaginary ($\mathcal{I}$, quadrature) part and noise

$$\tilde{\boldsymbol{n}}^{[T,R]}[k] = \begin{pmatrix} \mathcal{R}\left\{\tilde{n}_0^{[T,R]}[k]\right\} \\ \mathcal{I}\left\{\tilde{n}_0^{[T,R]}[k]\right\} \\ \vdots \\ \mathcal{R}\left\{\tilde{n}_{C-1}^{[T,R]}[k]\right\} \\ \mathcal{I}\left\{\tilde{n}_{C-1}^{[T,R]}[k]\right\} \end{pmatrix} \in \mathbb{R}^{2C\times 1}. \tag{3.59}$$

The overall noise free observation vector combining the two-way exchange yields

$$\boldsymbol{R}[k] = \begin{pmatrix} \tilde{\boldsymbol{r}}^{[T_1,R_2]}[k] \\ \tilde{\boldsymbol{r}}^{[T_2,R_1]}[k] \end{pmatrix} \in \mathbb{R}^{4C\times 1}. \tag{3.60}$$

The observation $\boldsymbol{R}$ depends on the known system parameters

sampling period	T_{Samp},	
transmit waveform	s_0,	
number of samples	K_{S},	
number of channels	C,	
LO carrier frequency	f_{w}	and
IF channel frequencies	$\{f_0, f_1, \ldots, f_{C-1}\}$.	

(3.61)

Equally the observation $\boldsymbol{R}$ depends on the unknown estimation parameters

propagation delay	τ_0,	
channel amplitudes	$\{\alpha_0, \alpha_1, \ldots, \alpha_{C-1}\}$,	
channel phases	$\{\varphi_0, \varphi_1, \ldots, \varphi_{C-1}\}$,	
clock frequency offset	δ_f,	
time offset	t_0	and
initial LO phases	$\phi_{\text{R}}^{[T_1]}$, $\phi_{\text{R}}^{[R_2]}$, $\phi_{\text{R}}^{[T_2]}$, $\phi_{\text{R}}^{[R_1]}$.	

(3.62)

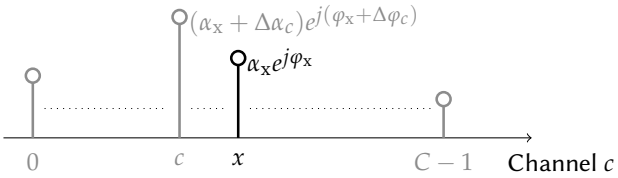


FIGURE 3.11 – *Relative channel coefficient definition.*

Considering (3.44) without inter-node delay ($\tau_0 = 0$) and perfect inter-node synchronization ($t_0 = 0$ and $\delta_f = 0$), phase estimations on $c \in [0, \ldots, C-1]$ channels are given by

$$\phi_{\mathrm{A}c}^{[T_1,R_2]} = \varphi_c + \phi_{\mathrm{R}}^{[T_1]} - \phi_{\mathrm{R}}^{[R_2]}, \tag{3.63a}$$

$$\tilde{\phi_{\mathrm{A}c}}^{[T_2,R_1]} = \varphi_c + \phi_{\mathrm{R}}^{[T_2]} - \phi_{\mathrm{R}}^{[R_1]}. \tag{3.63b}$$

For uncorrelated channel coefficients, which have to be assumed in the case of multipath propagation, follows

$$\mathrm{cov}\left[\varphi_i, \varphi_k\right] = 0, \quad \forall i,k \in [0, \ldots, C-1] \ \cap \ i \neq k. \tag{3.64}$$

The problem in (3.63) does not allow estimating the initial LO phases $\phi_{\mathrm{R}}^{[X]}$ separately. Only phase differences $\phi_{\mathrm{R}}^{[T]} - \phi_{\mathrm{R}}^{[R]}$ can be estimated. In order to ensure variable separability, a variable change is performed as follows.

As multi-channel ranging is based on the principle of relative phase differences on different frequencies, the channel coefficients are defined as relative amplitude and phase differences to a central channel $x = \left\lceil \frac{C}{2} \right\rceil - 1$ integrating initial LO phases

$$\alpha_x + \Delta\alpha_c \triangleq \alpha_c, \tag{3.65a}$$

$$\varphi_x + \Delta\varphi_c \triangleq \varphi_c + \phi_{\mathrm{R}}^{[T_1]} - \phi_{\mathrm{R}}^{[R_2]}, \tag{3.65b}$$

$$\Delta\phi_{\mathrm{R}} \triangleq \left(\phi_{\mathrm{R}}^{[T_2]} - \phi_{\mathrm{R}}^{[R_1]}\right) - \left(\phi_{\mathrm{R}}^{[T_1]} - \phi_{\mathrm{R}}^{[R_2]}\right). \tag{3.65c}$$

By definition, relative differences are zero on the central channel $c = x$

$$\Delta\alpha_{\left\lceil \frac{C}{2} \right\rceil - 1} = 0, \tag{3.66a}$$

$$\Delta\varphi_{\left\lceil \frac{C}{2} \right\rceil - 1} = 0. \tag{3.66b}$$

An illustration of this relative channel coefficient definition is depicted in Figure 3.11. Consequently, (3.63) can be rewritten as

$$\phi_{\mathrm{A}c}^{[T_1,R_2]} = \varphi_x + \Delta\varphi_c, \tag{3.67a}$$

$$\tilde{\phi_{\mathrm{A}c}}^{[T_2,R_1]} = \varphi_x + \Delta\varphi_c + \Delta\phi_{\mathrm{R}}. \tag{3.67b}$$

The equation set in (3.67) shows that the newly defined variables are separable and can be estimated from the given phase measurements. Consequently the unknown parameter estimation vector for the observation $\boldsymbol{R}$ in (3.60) with system parameters from (3.61) is given by (3.62), utilizing the definitions from (3.65)

$$\boldsymbol{\theta} = [\tau_0,\ \boldsymbol{A},\ \boldsymbol{\Phi},\ \delta_f,\ t_0,\ \Delta\phi_{\mathrm{R}}]^{\mathrm{T}} \in \mathbb{R}^{(2C+4)\times 1}, \tag{3.68}$$

with $\boldsymbol{A} = \left[\Delta\alpha_0 \ldots \Delta\alpha_{x-1}\ \alpha_{\mathrm{x}}\ \Delta\alpha_{x+1} \ldots \Delta\alpha_{C-1}\right]$ and $\boldsymbol{\Phi} = \left[\Delta\varphi_0 \ldots \Delta\varphi_{x-1}\ \varphi_{\mathrm{x}}\ \Delta\varphi_{x+1} \ldots \Delta\varphi_{C-1}\right]$.

In the following, AWGN $\tilde{\boldsymbol{n}}$ is considered, which allows applying (3.54) for straightforward CRLB derivation. The noise on successive samples is considered uncorrelated. The CRLB on the unknown estimation parameter $\boldsymbol{\theta}$ for the observation $\tilde{\boldsymbol{R}}$ is given according to (3.56) by

$$\mathrm{Var}\left(\widehat{\boldsymbol{\theta}}\right) \geq \mathrm{trace}\left(\left(\boldsymbol{I}_{\boldsymbol{R}}(\boldsymbol{\theta}) + \boldsymbol{\Sigma}_{\boldsymbol{\theta}}^{-1}\right)^{-1}\right), \tag{3.69}$$

with the overall FIM $\boldsymbol{I}_{\boldsymbol{R}}$ and prior information $\boldsymbol{\Sigma}_{\boldsymbol{\theta}}$ on the unknown estimation parameter. The overall FIM can be given as the sum of the sample specific FIM due to the noise independence

$$\boldsymbol{I}_{\boldsymbol{R}}(\boldsymbol{\theta}) = \sum_{k=0}^{K_{\mathrm{S}}-1} \boldsymbol{I}_{\boldsymbol{R}}(\boldsymbol{\theta}, k) = \sum_{k=0}^{K_{\mathrm{S}}-1} \boldsymbol{J}_{\boldsymbol{R}}^{\mathrm{T}}[k]\, \boldsymbol{\Sigma}_{\boldsymbol{R}}^{-1}\, \boldsymbol{J}_{\boldsymbol{R}}[k] \in \mathbb{R}^{(2C+4)\times(2C+4)}. \tag{3.70}$$

The sample specific JM $\boldsymbol{J}_{\boldsymbol{R}}[k]$ contains the partial derivatives of the observation $\boldsymbol{R}$ to the elements of the unknown estimation vector $\boldsymbol{\theta}$. Detailed derivation of the entries of the JM are given in Appendix C.

As the received signals $r_c^{[T,R]}$ are obtained sequentially on different channels, i.e. on successive LPWA packets, the noise on the observations can be considered as independent. Hence the observation noise covariance is given by the diagonal matrix

$$\begin{aligned}\boldsymbol{\Sigma}_{\boldsymbol{R}} = \operatorname{diag}\Bigg[&\left(\sigma_{\mathcal{R},0}^{[T_1,R_2]}\right)^2, \left(\sigma_{\mathcal{I},0}^{[T_1,R_2]}\right)^2, \ldots, \left(\sigma_{\mathcal{R},C-1}^{[T_1,R_2]}\right)^2, \left(\sigma_{\mathcal{I},C-1}^{[T_1,R_2]}\right)^2, \\ &\left(\sigma_{\mathcal{R},0}^{[T_2,R_1]}\right)^2, \left(\sigma_{\mathcal{I},0}^{[T_2,R_1]}\right)^2, \ldots, \left(\sigma_{\mathcal{R},C-1}^{[T_2,R_1]}\right)^2, \left(\sigma_{\mathcal{I},C-1}^{[T_2,R_1]}\right)^2\Bigg] \in \mathbb{R}^{4C\times 4C}.\end{aligned} \tag{3.71}$$

3.3.3 Ranging Precision Bounds in Free-space Propagation

The general CRLB formulation from (3.69) can be evaluated for the case of free-space propagation, i.e. frequency flat fading on C channels. In this scenario, all channel amplitudes α_c and phases φ_c are equal. This results in all amplitude and phase differences to be zero, i.e. $\Delta\alpha_c = 0$ and $\Delta\varphi_c = 0$ according to the definition in (3.65c). This knowledge on amplitude and phase differences in the estimation problem can be modeled as prior information in the covariance matrix

$$\boldsymbol{\Sigma}_{\boldsymbol{\theta}} = \begin{pmatrix} \sigma_{\tau_0}^2 & & & & \\ & \boldsymbol{\Sigma}_{\alpha_x,\Delta\alpha_c,\varphi_x,\Delta\varphi_c} & & \boldsymbol{0} & \\ & & \sigma_{\delta_f}^2 & & \\ & \boldsymbol{0} & & \sigma_{t_0}^2 & \\ & & & & \sigma_{\Delta\phi_{\mathrm{R}}}^2 \end{pmatrix}, \tag{3.72}$$

with channel coefficient covariance matrix $\boldsymbol{\Sigma}_{\alpha_x,\Delta\alpha_c,\varphi_x,\Delta\varphi_c}$. Amplitude and phase differences being zero is modeled by $\sigma_{\Delta\alpha_c}^2 = 0$ and $\sigma_{\Delta\varphi_c}^2 = 0$. The center channel coefficient and all other parameters have no prior information, i.e. $\sigma_{\tau_0}^2 = \sigma_{\alpha_{\mathrm{x}}}^2 = \sigma_{\varphi_{\mathrm{x}}}^2 = \sigma_{\delta_f}^2 = \sigma_{t_0}^2 = \sigma_{\Delta\phi_{\mathrm{R}}}^2 = \infty$.

Analytical derivation of the CRLB from (3.69) is very complex due to the complex structure of the JM. Therefore, analysis is based on the analytical expressions of the JM entries and numerical evaluation of the CRLB expression. Table 3.1 summarizes numerical values for the system parameters used in the following numerical evaluation.

Figure 3.12 compares the numerical evaluation of the CRLB of (3.69) with system parameters from Table 3.1 to a modified CRLB formulation without clock frequency offset, i.e. $\delta_f = 0$ and a reduced unknown estimation parameter $\boldsymbol{\theta} \to \boldsymbol{\theta} \setminus \delta_f$. Both bounds are compared to the analytical CRLB from (3.1) with RMS bandwidth from (3.11). Plots are given as function of single channel E_{S}/N_0 as the sequentially received signals need to be processed independently for communication purposes and to extract amplitude, ToA, PoA and CFO metrics. However, the ranging relevant signal energy to noise spectral density ratio is given by

$$\frac{E_{\mathrm{S,ranging}}}{N_0} = C\, \frac{E_{\mathrm{S}}}{N_0}. \tag{3.73}$$

Figure 3.12 shows the delay CRLB for a frequency flat channel considering a signal model with and without CFO. Delay τ_0 estimation in the two-way signaling scheme is not degraded by unknown CFO. Calculating the difference of (3.44a) and (3.44b) and neglecting the factor $\left(1+\delta_f\right)$ on the delay τ_0, allows separating delay and CFO estimation and hence there is theoretically no mutual degradation in two-way ranging. Figure 3.13 shows the analytical CRLB (1.46) for single channel ToF and multi-channel ToF as well as for multi-channel PoF ranging with RMS bandwidth (3.11) and $E_{\mathrm{S,ranging}}/N_0$.

The analytical CRLB is compared to the numerical evaluation of the CRLB in (3.69) on the detailed signal model. The CRLB for multi-channel ToF ranging, i.e. when only time estimates are available, can be obtained by considering

Parameter	Numerical value
Delay τ_0	uniform in $[0, 10]\text{km}/c_0$
Time offset t_0	uniform in $[-100, +100]\mu\text{s}$
Initial LO phase $\Delta\phi_\text{R}$	uniform in $[0, 2\pi)$
Carrier frequency f_W	868 MHz
CFO δ_f	uniform in $[-1, +1]$ppm
Waveform s_0	Hanning pulse
	B=1 kHz
Channel spacing Δf	400 kHz
Number of channels C	16
Virtual bandwidth B_virt	6 MHz
Maximum unambiguous range R_max	375 m
Range resolution ΔR	25 m
Sampling frequency f_Samp	16 kHz
Number of realizations	10^2

TABLE 3.1 – *Parameters for numerical CRLB evaluation.*

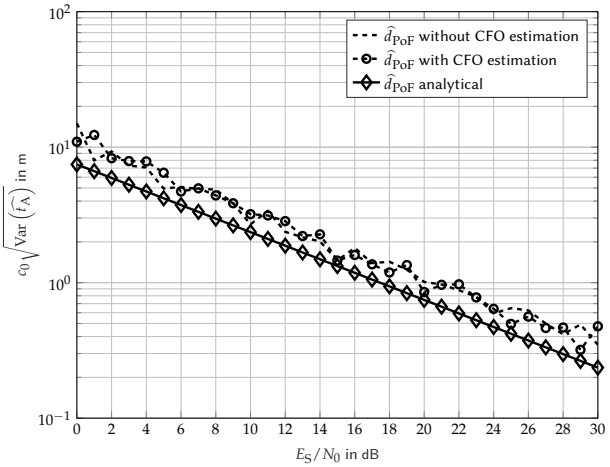


FIGURE 3.12 – *CRLB on delay τ_0 comparing analytical bound and numerical evaluation of the detailed multi-channel ranging CRLB with and without CFO δ_f in the estimation parameter $\boldsymbol{\theta}$.*

all initial LO phase to be random at each channel, i.e. $\phi_\text{R}^{[X]} \rightarrow \phi_{\text{R}c}^{[X]}$ which is equivalent to removing the prior information on the phase information $\sigma^2_{\Delta\varphi_c} = \infty$.

Figure 3.13 illustrates how the numerical evaluation of the multi-channel ToF and multi-channel PoF ranging CRLB match their analytical equivalent. This validates the CRLB formulation from (3.69).

At a technically typical $E_\text{S}/N_0 = 20\,\text{dB}$, single channel ToF ranging achieves 4 km precision, while multi-channel ToF ranging, *e.g.* averaging over C independent single channel ToF estimates improves by a factor $\sqrt{C} = 4$ to 1 km. Maintaining the narrow instantaneous bandwidth $B = 1\,\text{kHz}$, but virtually aggregating $B_\text{virt} = 6\,\text{MHz}$ through coherent processing, achieves meter-level precision for PoF ranging.

Figure 3.13 equally demonstrates the great advantage of multi-channel PoF ranging compared to time-based approaches. In both techniques, the same waveform is transmitted for the same duration with the same energy. The largely improved ranging precision for PoF ranging is obtained through phase estimation and the coherent processing to aggregate a virtually larger bandwidth. This advantage is payed-off by the hardware implications for coherent processing (see Chapter 3.2.3) and supplementary issues such as the ranging ambiguity.

3.3.4 Ranging Precision Bounds in Multipath Propagation

In the previous section the signal model has been validated with the numerical evaluation of the CRLB in a free-space propagation scenario. The feasibility of meter-level ranging precision with system parameters, which are realistic for LPWA systems, *e.g.* reasonable number of channels and adequate channel spacing (see Table 3.1) has been illustrated.

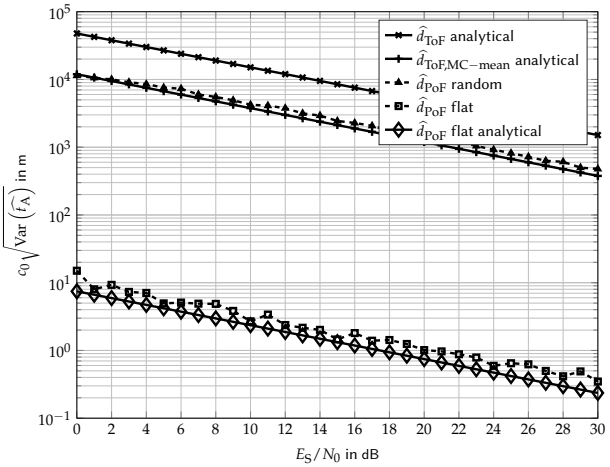


FIGURE 3.13 – *CRLB on delay τ_0 in a free-space propagation channel for an instantaneous signal bandwidth $B = 1\,\mathrm{kHz}$ and a multi-channel virtual bandwidth $B_{\mathrm{virt}} = 6\,\mathrm{MHz}$ with parameters from Table 3.1.*

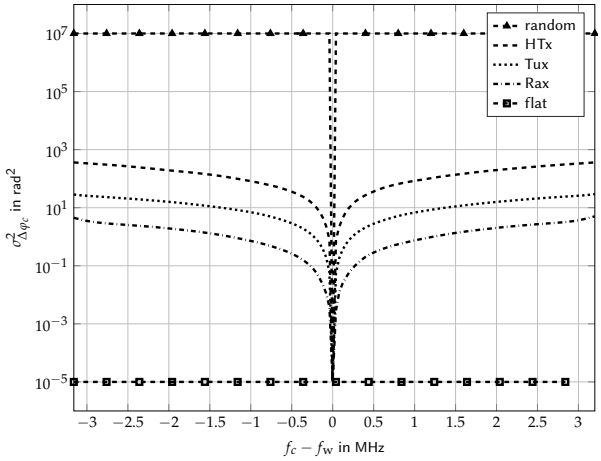


FIGURE 3.14 – *Phase difference variance according to* (3.74) *for typical ETSI channel models [ETS10].*

This section focuses on the numerical evaluation of the CRLB in the more general case of multipath propagation. CRLBs are given for the widely adopted European Telecommunications Standards Institute (ETSI) channel models [ETS10] presented in Chapter 2.3.5. This allows predicting the ranging precision in realistic LPWA channels as encountered in urban propagation scenarios.

To evaluate the CRLB from (3.69) for different propagation channel types, the prior information on the channel coefficients is modified. Instead of assuming a single channel coefficient φ_c for all channels, i.e. $\sigma^2_{\Delta\varphi_c} = 0$, the case of different channel coefficients φ_c has to be taken into account. This requires deriving

$$\boldsymbol{\Sigma}_{\alpha_x,\Delta\alpha_c,\varphi_x,\Delta\varphi_c} = \mathrm{cov}\left[\boldsymbol{A}\ \boldsymbol{\Phi}\right], \tag{3.74}$$

for each channel model. For this purpose 10^4 Rayleigh fading channel realizations are generated in frequency domain for each channel model. Amplitude and phase differences are calculated according to (3.65a) and (3.65b) and Figure 3.11 and used to obtain the covariance matrix $\boldsymbol{\Sigma}_{\alpha_x,\Delta\alpha_c,\varphi_x,\Delta\varphi_c}$. Figure 3.14 depicts the phase difference variance for the ETSI channel models with Rayleigh fading. By definition the center channel x has $\Delta\varphi_x = 0$ and hence a phase difference variance $\sigma^2_{\Delta\varphi_x} = 0$. Variances increase for channels further away from the center channel x. And as expected, channels with a smaller coherence bandwidth B_{coh} (see Table 2.3) exhibit larger phase variations at the same channel c with respect to the center channel x.

Figure 3.15 gives the CRLB for the system parameters from Table 3.1 and the channel statistics from (3.74). Precision in the frequency flat channel approaches the analytical multi-channel PoF ranging CRLB. For the ETSI channel models, precision degrades with growing RMS delay spread, i.e. with decreasing channel coherence bandwidth. For technical relevant E_{S}/N_0, the bounds are E_{S}/N_0 independent, showing that the propagation channel limits precision. The precision in the random channel, where no prior on the channel

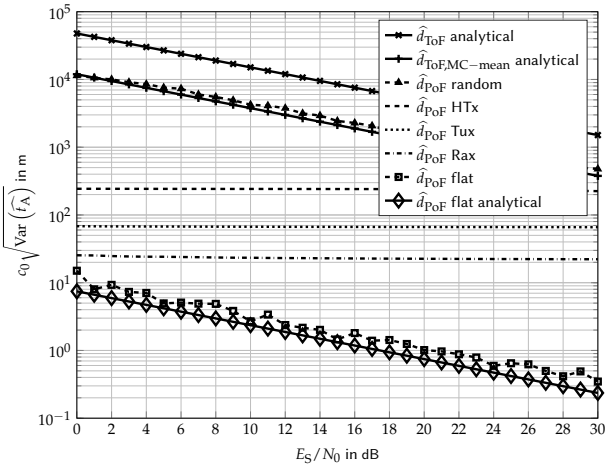


FIGURE 3.15 – *CRLB on delay τ_0 in the ETSI multipath propagation channels for an instantaneous signal bandwidth $B = 1\,\mathrm{kHz}$ and a multi-channel virtual bandwidth $B_{\mathrm{virt}} = 6\,\mathrm{MHz}$ with parameters from Table 3.1.*

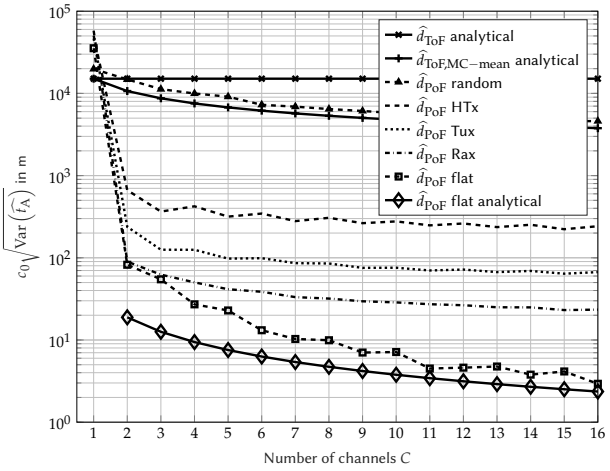


FIGURE 3.16 – *CRLB on delay τ_0 as function of virtual bandwidth $B_{\mathrm{virt}} = \Delta f(C-1)$, for an instantaneous signal bandwidth $B = 1\,\mathrm{kHz}$ with parameters from Table 3.1.*

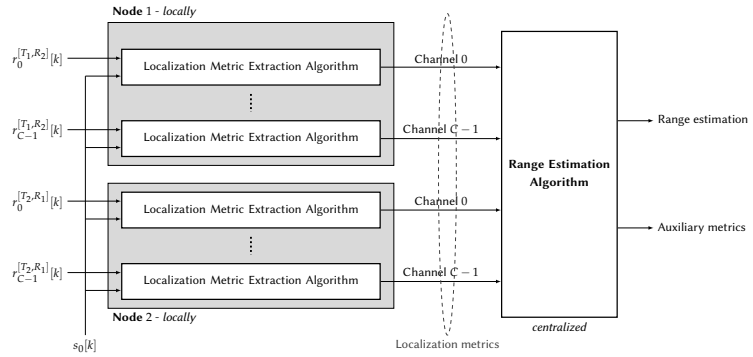
coefficients is available, matches the multi-channel ToF CRLB, reported by [Kar+11]. For the Typical urban (Tux) channel, attainable multi-channel ranging precision is $\sqrt{\mathrm{Var}\left(\widehat{d}_{\mathrm{PoF}}\right)} \leq 100\,\mathrm{m}$ at $E_{\mathrm{S}}/N_0 = 20\,\mathrm{dB}$, compared to $\sqrt{\mathrm{Var}\left(\widehat{d}_{\mathrm{ToF}}\right)} \approx \sqrt{C}\sqrt{\mathrm{Var}\left(\widehat{d}_{\mathrm{ToF,MC-mean}}\right)} \approx 4\,\mathrm{km}$ for a single channel.

3.3.5 Precision to Energy Consumption Trade-Off

Energy consumption is a crucial design limitation for LPWA systems. Communication protocols are optimized to reduce the required transmission and reception times to a minimum. Multi-channel ranging allows scaling the total transmission time by adjusting the number of channels C. Reducing the number of channels and keeping the channel spacing constant, decreases transmission time but equally reduces the RMS bandwidth and hence degrades ranging precision.

Figure 3.16 shows the CRLBs for the system parameters from Table 3.1 and the ETSI channel models as function of the number of channels C. In theory, the major precision improvement is achieved when passing from a single channel to the use of two channels, allowing coherent phase-based processing. For $C = 1$, the RMS bandwidth in (3.11) depends only on the instantaneous waveform bandwidth B, whereas for $C \geq 2$, the RMS bandwidth becomes scalable. Figure 3.16 also reveals that for equidistant channel spacing, precision improves in the frequency flat fading propagation channel by $1/C$ for $C \geq 2$ as the RMS bandwidth grows linearily.

The appropriate choice of C allows a trade-off between energy consumption and the required ranging precision, which are both application dependent and need to be adapted to the given propagation channel characteristics.



(a) *Received signal processing on the example of two-way ranging.*

(b) *Localization metric extraction algorithm.*

FIGURE 3.17 – *Signal processing flow diagram for range estimation with LPWA transceivers.*

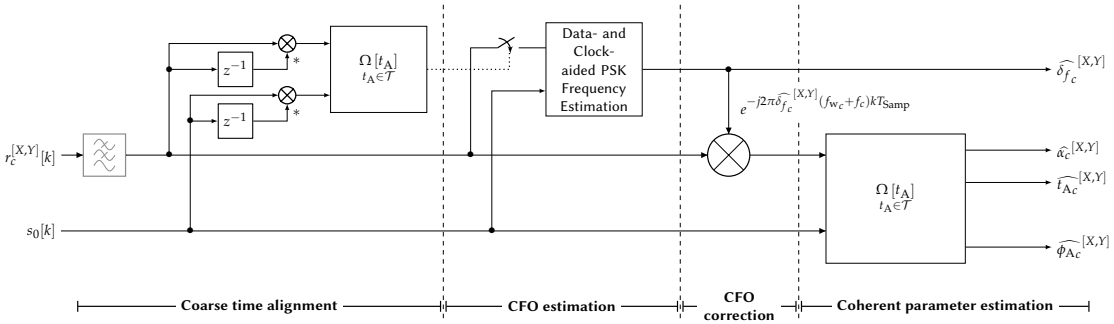


FIGURE 3.18 – *Localization metric extraction algorithm: Differential detection and coherent parameter estimation.*

3.4 Radio Signal Based Ranging

3.4.1 Localization Metric Extraction Algorithms

The receivers involved in multi-channel ranging hold upon reception the samples of the received signal $r_c^{[T,R]}$ according to (3.28).

Gathering the received signals on all channels and for both nodes in order to obtain (3.60) allows applying joint parameter estimation on the complete set of observations, *e.g.* by least-square optimization methods. Storing and centralizing all received signals is however not practical for LPWA systems which are constraint in resources. Therefore, each raw received signal $r_c^{[T,R]}$ is processed separately directly upon reception to extract the localization metrics such as amplitude (Received Signal Strength Indicator (RSSI)), time (ToA), phase (PoA) and auxiliary estimates such as CFO for correcting the localization metrics appropriately. In order to determine range or position information, the localization metrics on all channels and for both nodes, constituting much less data, are centralized and combined. This two-step approach is depicted in Figure 3.17a and is suited to LPWA transceivers. In the following, localization metric extraction algorithms are presented and range estimation algorithms are detailed in Chapter 3.4.2.

Three localization metric extraction algorithms are studied which all have the same inputs and outputs as depicted in Figure 3.17b. The algorithms vary in complexity and performance:

- **Differential detection and coherent parameter estimation**: A coarse time alignment through differential detection, allows the application of a low-complexity CFO estimation algorithm from [MM97]. Localization metrics are estimated on the CFO compensated received signal through correlation with the transmit signal.
- **Time-frequency search and coherent parameter estimation**: Differential detection and low-complexity CFO estimation are replaced by an exhaustive time and frequency search through two-dimensional correlation as employed in Global Positioning System (GPS) signal acquisition [KH06]. Localization metrics are estimated on the CFO compensated received signal through correlation with the transmit signal.
- **Time-frequency search with tracking**: Time frequency search through two-dimensional correlation directly serves for localization metric extraction. Computational complexity is reduced through a tracking procedure both in time and frequency over the set of C channels in order to reduce the search spaces.

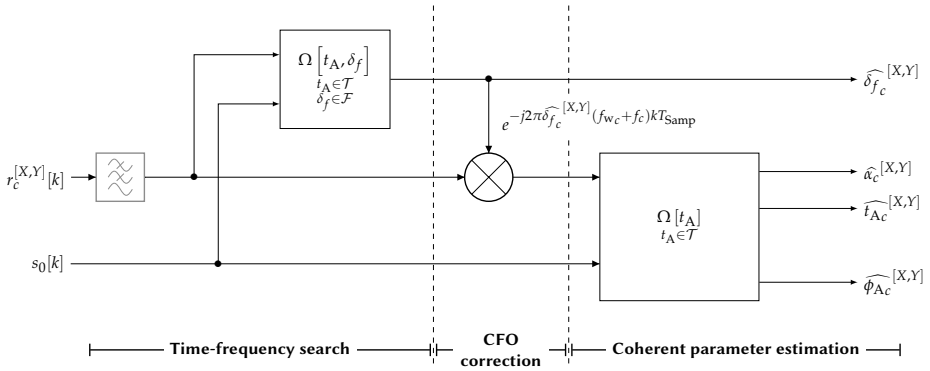


FIGURE 3.19 – *Localization metric extraction algorithm: Time-frequency search and coherent parameter estimation.*

3.4.1.1 Differential Detection and Coherent Parameter Estimation

The following algorithm depicted in Figure 3.18 is divided into three steps:

1. Coarse time alignment.
2. CFO estimation and compensation.
3. Coherent parameter estimation.

In order to extract the localization metrics through cross correlation of the transmit signal s_0 and the received signal $r_c^{[X,Y]}$, the latter needs to be compensated in CFO to allow coherent parameter estimation. Considering Phase Shift Keying (PSK) modulated signals s_0, such as Differential Binary Phase Shift Keying (DBPSK) in Sigfox, a low-complexity data- and clock-aided CFO estimation algorithm [MM97] can be used for this purpose. This algorithm estimates CFO through comparison of the received symbols with those initially transmitted. The received symbols are recovered through differential detection through cross correlation. The estimated CFO is then used to obtain a CFO compensated receive signal

$$r_{c\,\text{no CFO}}^{[T,R]}[k] = r_c^{[T,R]}[k]\, e^{-j2\pi\widehat{\delta}_{f_c}^{[T,R]}(f_w+f_c)kT_{\text{Samp}}}. \tag{3.75}$$

Based on the cross correlation between the CFO compensated received signal $r_{c\,\text{no CFO}}^{[T,R]}$ and the transmit signal s_0, localization metrics are extracted by calculating

$$\widehat{\alpha_c}^{[T,R]} = \max_{t_A \in \mathcal{T}} \left| \Omega_{r_{c\,\text{no CFO}}, s_0}^{[T,R]}[t_A] \right|, \tag{3.76a}$$

$$\widehat{t_{A_c}}^{[T,R]} = \arg\max_{t_A \in \mathcal{T}} \left| \Omega_{r_{c\,\text{no CFO}}, s_0}^{[T,R]}[t_A] \right|, \tag{3.76b}$$

$$\widehat{\phi_c}^{[T,R]} = \arg\left\{ \Omega_{r_{c\,\text{no CFO}}, s_0}^{[T,R]}\left[\widehat{t_{A_c}}\right] \right\}, \tag{3.76c}$$

with time search space $\mathcal{T}$ and cross correlation

$$\Omega_{r_{c\,\text{no CFO}}, s_0}^{[T,R]}[t_A] = \sum_{k=0}^{K_S-1} \left(r_{c\,\text{no CFO}}^{[T,R]}\left[k - \frac{t_A}{T_{\text{Samp}}}\right] \right)^* s_0[k]. \tag{3.77}$$

This algorithm has a moderate computational complexity, as it requires only two cross correlations. However, it is limited in its applicability to low Signal to Noise Ratio (SNR) signals due to the requirement of a sufficiently high (positive) SNR for the CFO estimation algorithm [MM97]. Moreover, initial differential detection degrades the SNR by up to 3 dB.

3.4.1.2 Time-frequency Search and Coherent Parameter Estimation

To overcome these limitations, differential detection and the low-complexity CFO estimation algorithm are replaced by an exhaustive time-frequency search, which is typically utilized in GPS signal acquisition [KH06]. The algorithm is illustrated in Figure 3.19. In order to jointly estimate the unknown delay and CFO, all possible

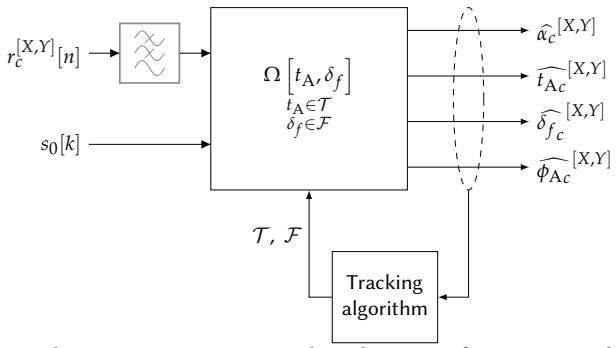


FIGURE 3.20 – *Localization metric extraction algorithm: Time-frequency search with tracking.*

hypotheses are tested through cross correlation of the received signal with a frequency shifted version of s_0

$$\widehat{\delta_{f_c}}^{[T,R]} = \arg\max_{\substack{\delta_f \\ t_A \in \mathcal{T} \\ \delta_f \in \mathcal{F}}} \left| \Omega_{r_c, s_0}^{[T,R]}[t_A, \delta_f] \right|, \tag{3.78}$$

with time search space $\mathcal{T}$, relative frequency offset δ_f in frequency search space $\mathcal{F}$ and cross correlation

$$\Omega_{r_c, s_0}^{[T,R]}[t_A, \delta_f] = \sum_{k=0}^{K_S-1} \left(r_c^{[T,R]}\left[k - \frac{t_A}{T_{\text{Samp}}} \right] \right)^* s_0[k]\, e^{-j2\pi\delta_f (f_w + f_c) k T_{\text{Samp}}}. \tag{3.79}$$

The CFO estimation is subsequently used for compensation of CFO induced errors before coherent parameter estimation according to (3.76). Due to the two-dimensional search process, complexity grows significantly. However, this approach overcomes the limitations of the previous algorithms as it allows improving the SNR on the receiving side. Signals with a low spectral efficiency, such as Direct Sequence Spread Spectrum (DSSS) allowing acquisition below the noise floor [KH06] may be employed. Furthermore, the algorithm is not specific to a certain type of waveform s_0.

3.4.1.3 Time-frequency Search with Tracking

The time-frequency search and coherent parameter estimation algorithm can be improved in two ways:

- The time-frequency search in (3.79) provides not only frequency offset estimation but also delay estimation. The coherent parameter estimation step is hence included and localization parameters can be directly obtained on (3.79) and are given by

$$\widehat{\alpha_c}^{[T,R]} = \max_{t_A, \delta_f} \left| \Omega_{r_c, s_0}^{[T,R]}[t_A, \delta_f] \right|, \tag{3.80a}$$

$$\widehat{t_{Ac}}^{[T,R]} = \arg\max_{t_A} \max_{t_A, \delta_f} \left| \Omega_{r_c, s_0}^{[T,R]}[t_A, \delta_f] \right|, \tag{3.80b}$$

$$\widehat{\delta_{f_c}}^{[T,R]} = \arg\max_{\delta_f} \max_{t_A, \delta_f} \left| \Omega_{r_c, s_0}^{[T,R]}[t_A, \delta_f] \right|, \tag{3.80c}$$

$$\widehat{\phi_{Ac}}^{[T,R]} = \arg\left\{ \Omega_{r_c, s_0}^{[T,R]}\left[\widehat{t_{Ac}}^{[T,R]}, \widehat{\delta_{f_c}}^{[T,R]} \right] \right\}. \tag{3.80d}$$

- Adequate tracking techniques allow reducing the time $\mathcal{T}$ and frequency $\mathcal{F}$ search spaces for the estimation of localization metrics on the set of C received signals on the different channels $[0, \ldots, C-1]$.

The following hypotheses need to be considered for this purpose:

- The time search space can be reduced if the time relation between the nodes remains constant over the multi-channel exchange, i.e. $t_0 = \text{const.}\ \forall c \in [0, C-1]$.
- The lower limit for the time search space is given by the ToA estimation uncertainty and sampling time drifts due to clock frequency offsets δ_f.

The frequency search space for $c = 0$ is designed to cover the maximum encountered and hence specified relative CFO. It can be reduced for $c > 0$ to testing adjacent hypotheses around the CFO estimate $\widehat{\delta_{f_c}}^{[T,R]}$ obtained due

to initial full search space. Temporal clock frequency drifts between successive channels need to be inferior to the tested adjacent hypotheses. This algorithm is depicted in Figure 3.20.

Computational complexity can be reduced compared to full time-frequency search and coherent parameter estimation, however tracking techniques need to properly adapt to *e.g.* time varying CFO or degraded reception conditions, *e.g.* through temporal signal loss.

Table 3.2 summarizes the features of the presented localization metric extraction algorithms.

	Differential Detection and Coherent Parameter Estimation	**Time-frequency Search and Coherent Parameter Estimation**	**Time-frequency Search with Tracking**
SNR operation range	$\gtrsim 0\,\mathrm{dB}$ [MM97]	Detection below noise floor possible (limitation: maximum coherent integration time)	
Waveform	PSK	any	
Complexity in cross correlations	2	$\mathcal{T} \times \mathcal{F} + 2$	acquisition: $\mathcal{T} \times \mathcal{F}$ tracking min.: 2×3
Requirements	high robustness		sophisiticated tracking required

Table 3.2 – *Overview on localization metric extraction algorithms.*

3.4.2 Range Estimation

Classical ToF ranging as well as multi-channel PoF range estimation can be performed based on the extracted localization metrics.

3.4.2.1 Time of Flight

The ToF estimation from timeslot two-way ranging is calculated by the sum of the two ToA estimates given by (3.34) with (3.45). ToA estimates are converted to a common time base with the available CFO estimation. The ToF is given by

$$\widehat{T_{\mathrm{ToF}c}}^{[1,2]} = \widehat{t_{\mathrm{A}c}}^{[T_1,R_2]} + \left(1+\widehat{\delta_f}\right)\widehat{t_{\mathrm{A}c}}^{[T_2,R_1]}. \tag{3.81}$$

Single channel ToF range estimation is given by

$$\widehat{d}_{\mathrm{ToF}c} = \frac{c_0}{2}\widehat{T_{\mathrm{ToF}c}}^{[1,2]} = \underbrace{c_0\tau_0}_{\text{Term I}} \underbrace{+c_0\frac{2\delta_f+\epsilon_{\widehat{\delta_f}}}{2}\tau_0}_{\text{Term II}} \underbrace{-c_0\frac{\epsilon_{\widehat{\delta_f}}}{2\left(1+\delta_f\right)}t_0}_{\text{Term III}} \underbrace{-c_0\frac{1+\delta_f+\epsilon_{\widehat{\delta_f}}}{2\left(1+\delta_f\right)}\delta_f K_{\mathrm{S}} T_{\mathrm{Samp}}}_{\text{Term IV}} \underbrace{+c_0\frac{\epsilon_{\widehat{t_{\mathrm{A}c}}}^{[T_1,R_2]}+\left(1+\delta_f+\epsilon_{\widehat{\delta_f}}\right)\epsilon_{\widehat{t_{\mathrm{A}c}}}^{[T_2,R_1]}}{2}}_{\text{Term V}} \tag{3.82}$$

- **Term I**: Range which is to be estimated.
- **Term II**: This error is due to the absence of an absolute clock reference. It can be neglected as $\delta_f \ll 1$ and the error hence much smaller than range to be estimated, *e.g.* $c_0\tau_0 = 1\,\mathrm{km}$ results in a 1 mm error for a 1 ppm CFO.
- **Term III**: This error depends on the CFO estimation quality and the timeslot alignment. Practically the timeslot alignment, controlled by the MAC layer, is in the order of magnitude of ToA estimation errors, i.e. $|t_0| \approx \left|\epsilon_{\widehat{t_{\mathrm{A}}}}\right|$. The term is due to $\epsilon_{\widehat{\delta_f}} \ll 1$ much smaller than the ToA estimation error Term V. Considering a timeslot alignment $t_0 = 1\,\mathrm{ms}$ and a CFO estimation error $\epsilon_{\widehat{\delta_f}} = 1\,\mathrm{ppm}$, this term evaluates to a 0.3 m range error.

- **Term IV**: This error arises due to the time duration between the two ToA estimations. For LPWA transmissions/packets, $K_S T_{\text{Samp}}$ can be in the order of seconds. In such a case the error of this term evaluates to $\approx 150\,\text{m}$ for $K_S T_{\text{Samp}} = 1\,\text{s}$ and a 1 ppm CFO. Depending on the ToA estimation precision this error can be significant compared to Term V and needs to be corrected. This is possible using a CFO estimation and the knowledge of the transmission time.
- **Term V**: ToA estimation uncertainty and noise.

Single channel ToF range estimates on different channels c can be combined to improve statistics. In the following, averaging and the median over the set of C channels is investigated

$$\widehat{d}_{\text{ToF,MC}-\text{mean}} = \underset{c}{\text{mean}}\left(\widehat{d}_{\text{ToF}c}\right), \tag{3.83a}$$

$$\widehat{d}_{\text{ToF,MC}-\text{median}} = \underset{c}{\text{median}}\left(\widehat{d}_{\text{ToF}c}\right). \tag{3.83b}$$

3.4.2.2 Phase of Flight - Phase Slope

The sets of phase estimates are given by (3.44a) and (3.44b) and their channel-wise sum analog to (3.81), considering conversion to a common time base yields the so-called PoF

$$\begin{aligned}
\widehat{\phi_{\text{PoF}c}}^{[1,2]} &= \left(1+\widehat{\delta_f}\right)\widehat{\phi_{\text{A}c}}^{[T_1,R_2]} + \widehat{\widetilde{\phi_{\text{A}c}}}^{[T_2,R_1]} \\
&= \underbrace{-2\pi\left(f_{\text{w}c}+f_c\right)\,2\tau_0 + 2\varphi_c}_{\text{Term I}} \quad \underbrace{-2\pi\left(f_{\text{w}c}+f_c\right)\left(2\delta_f+\epsilon_{\widehat{\delta_f}}\right)\tau_0 + \left(\delta_f+\epsilon_{\widehat{\delta_f}}\right)\varphi_c}_{\text{Term II}} \quad \underbrace{-2\pi f_c \frac{\epsilon_{\widehat{\delta_f}}}{1+\delta_f} t_0}_{\text{Term III}} \\
&\quad \underbrace{+2\pi\left(f_{\text{w}c}+f_c\right)\delta_f K_S T_{\text{Samp}}}_{\text{Term IV}} \quad \underbrace{+\left(1+\delta_f+\epsilon_{\widehat{\delta_f}}\right)\epsilon_{\widehat{\phi_{\text{A}c}}}^{[T_1,R_2]} + \epsilon_{\widehat{\phi_{\text{A}c}}}^{[T_2,R_1]}}_{\text{Term V}} \\
&\quad \underbrace{+2\pi f_{\text{w}c}\frac{1+\delta_f+\epsilon_{\widehat{\delta_f}}}{1+\delta_f}\delta_f t_0}_{\text{Term VI}} \quad \underbrace{+\left(1+\delta_f+\epsilon_{\widehat{\delta_f}}\right)\left(\phi_{\text{R}c}^{[T_1]}-\phi_{\text{R}c}^{[R_2]}\right)+\phi_{\text{R}c}^{[T_2]}-\phi_{\text{R}c}^{[R_1]}}_{\text{Term VII}}.
\end{aligned} \tag{3.84}$$

- **Term I**: Range information is included in the delay dependent phase shift and the multipath channel phase. This term is equivalent to its ToF analog.
- **Term II**: This error is due to the absence of an absolute clock reference. It can be neglected as $\delta_f \ll 1$ and the error hence much smaller than range to be estimated, *e.g.* $c_0\tau_0 = 1\,\text{km}$ results in a 1 mm error for a 1 ppm CFO. This term is equivalent to its ToF analog in (3.82).
- **Term III**: This error depends on the CFO estimation quality and the timeslot alignment. Practically the timeslot alignment, controlled by the MAC layer, is in the order of magnitude of ToA estimation errors, i.e. $|t_0| \approx \left|\epsilon_{\widehat{t_{\text{A}}}}\right|$. Considering a timeslot alignment $t_0 = 1\,\text{ms}$ and a CFO estimation error $\epsilon_{\widehat{\delta_f}} = 1\,\text{ppm}$, this term evaluates to a 0.3 m range error. This term is equivalent to its ToF analog in (3.82).
- **Term IV**: This error arises due to the time duration between the two PoA estimations. For LPWA transmissions/packets, $K_S T_{\text{Samp}}$ can be in the order of seconds. In such a case the error of this term evaluates to $\approx 150\,\text{m}$ for $K_S T_{\text{Samp}} = 1\,\text{s}$ and a 1 ppm CFO. In contrast to its equivalent ToF term in (3.82), this error needs correction as it is significant in comparison to the precision of PoF based range estimation, predicted with the CRLBs. Based on a CFO estimation and the knowledge of the transmission time this error can be corrected (see (3.93)).
- **Term V**: PoA estimation uncertainty and noise. This term is equivalent to its ToF analog in (3.82).
- **Term VI**: Error due to the quality of the timeslot alignment and CFO. This error is a constant phase rotation for all channels c considering $f_{\text{w}c} = \text{const.}$. So it has no impact on the range information included in the phase variation over the channels. For $f_{\text{w}c} \neq \text{const.}$ the variations of this error are neglegible with the same reasoning as in Term III.
- **Term VII**: Term regrouping the initial oscillator phases. Neglecting the CFO impact, this term is equivalent to $\Sigma\Delta\phi_{\text{R}c}$.

Considering one of the transceiver architectures from Figure 3.9 and the corresponding processing, $\Sigma\Delta\phi_{\mathrm{R}c}$ is known, constant or zero over all channels. Under the hypothesis of free-space propagation, i.e. $\varphi_c = \text{const.}$ over all channels, range information can be obtained by taking the average slope of (3.84) as

$$\widehat{d}_{\mathrm{PoF,Slope}} = -\frac{c_0}{2 \cdot 2\pi} \frac{1}{C} \sum_{c=0}^{C-2} \left(\frac{\widehat{\phi_{\mathrm{PoF}c}}^{[1,2]} - \widehat{\phi_{\mathrm{PoF}c+1}}^{[1,2]}}{(f_{\mathrm{w}c} + f_c) - (f_{\mathrm{w}c} + f_{c+1})} \right). \tag{3.85}$$

The slope can be calculated from only $\widehat{\phi_{\mathrm{PoF}0}}^{[1,2]}$ and $\widehat{\phi_{\mathrm{PoF}C-1}}^{[1,2]}$, which yields maximum RMS bandwidth and hence best ranging precision. However, it is not sufficient as the large resulting channel spacing introduces a small maximum unambiguous range. Averaging in (3.85) ensures increased maximum unambiguous range through smaller channel spacing.

Further restricting to the transceiver architecture in Figure 3.9b with constant f_{w} and numerical IF mixing, slopes can be calculated on (3.44a) and (3.44b) separately, which gives the estimation of $\tau_0 + t_0$ and $\tau_0 - t_0$. Their combination allows range estimation.

Although the phase slope approach is straightforward, it is not applicable to multipath environments where $\varphi_c \neq \text{const.}$ over all channels and hence the phase and range are no longer linearly related.

3.4.2.3 Phase of Flight - Channel Impulse Response Reconstruction

In the general case of multipath propagation, an estimation of the CIR gives detailed insight into the channel, *e.g.* through macroscopic propagation channel characteristics (see Chapter 2.3.3) and allows range estimation *e.g.* through detecting the first path.

The estimated round-trip channel transfer function at the frequencies f_c can be reconstructed based on (3.40) and (3.44) as

$$\widehat{H}_{\mathrm{PoF}_c}^{[1,2]} = \widehat{\alpha_c}^{[T_1,R_2]} \, \widehat{\alpha_c}^{[T_2,R_1]} \, e^{j \, \widehat{\phi_{\mathrm{PoF}c}}^{[1,2]}}. \tag{3.86}$$

It is the multiplication of the two one-way channel transfer functions

$$\widehat{H}_{\mathrm{PoF}_c}^{[1,2]} = \widehat{H}_{\mathrm{PoA}_c}^{[T_1,R_2]} \, \widehat{H}_{\mathrm{PoA}_c}^{[T_2,R_1]}, \tag{3.87}$$

which is required to eliminate the unknown time offset t_0.

The round-trip CIR is given by Inverse Discrete Fourier Transform (IDFT) of (3.86)

$$\widehat{h_{\mathrm{PoF}}}^{[1,2]}(kT_{\mathrm{resolution}}) = \widehat{h_{\mathrm{PoF}k}}^{[1,2]} = \frac{1}{K_{\mathrm{IDFT}}} \sum_{c=0}^{K_{\mathrm{IDFT}}-1} \widehat{H}_{\mathrm{PoF}_c}^{[1,2],0} \, e^{j \frac{2\pi ck}{K_{\mathrm{IDFT}}}}, \tag{3.88}$$

with a zero-padded channel transfer function $\widehat{H}_{\mathrm{PoF}_c}^{[1,2],0}$ of length K_{IDFT} and CIR time resolution $T_{\mathrm{resolution}} = 1/\left(2\Delta f(K_{\mathrm{IDFT}} - 1)\right)$. An illustration is given in Figure 3.21.

The round-trip CIR is a convolution of the reciprocal one-way CIR $\widehat{h_{\mathrm{PoA}}}^{[T,R]}$ with itself

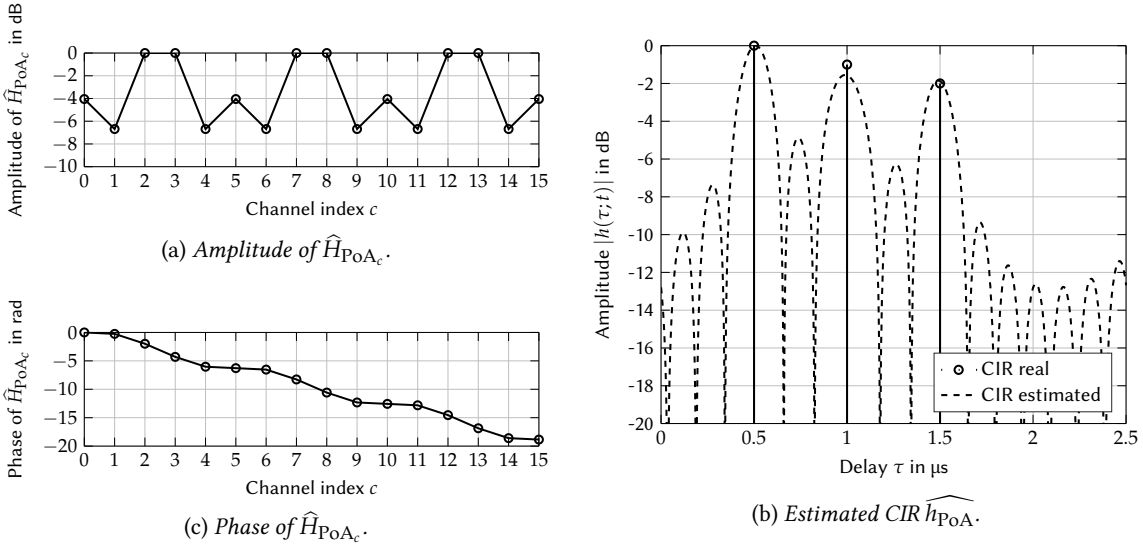
$$\widehat{h_{\mathrm{PoF}k}}^{[1,2]} = \widehat{h_{\mathrm{PoA}k}}^{[T_1,R_2]} * \widehat{h_{\mathrm{PoA}k}}^{[T_2,R_1]}. \tag{3.89}$$

Delays τ_p appear at twice their real distance and so-called phantom paths $\tau_i + \tau_k, \ \forall i \neq k$ arise due to this convolution.

For free-space and Line of Sight (LoS) weak multipath propagation, range estimation is given according to (2.24) by the maximum in the estimated CIR $\widehat{h_{\mathrm{PoF}}}^{[1,2]}$

$$\widehat{d}_{\mathrm{PoF,CIR-max}} = \frac{c_0}{2} \, \tau_{h_{\max}}. \tag{3.90}$$

However, LoS with strong multipath propagation scenarios require more adequate range estimation algorithms such as first path detection depicted in Figure 3.22. The first path which is assumed to be the direct path and hence corresponds to the inter-node range, is taken as shortest path within a certain range R_{first} and above a certain threshold γ_{first} relative to the path of maximum magnitude



(a) *Amplitude of* $\widehat{H}_{\mathrm{PoA}_c}$.

(c) *Phase of* $\widehat{H}_{\mathrm{PoA}_c}$.

(b) *Estimated CIR* $\widehat{h_{\mathrm{PoA}}}$.

FIGURE 3.21 – *CIR reconstruction.*

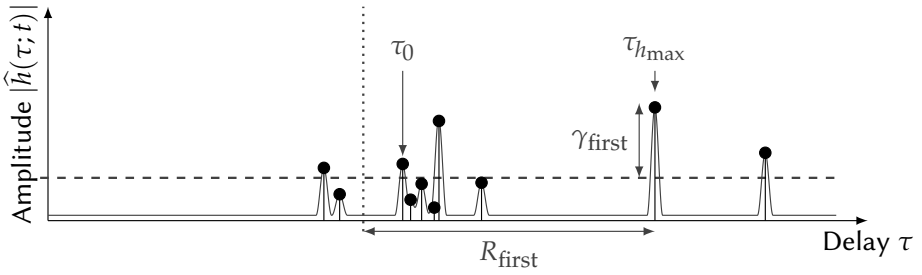


FIGURE 3.22 – *First path detection relative to the path of maximum amplitude.*

$$\widehat{d}_{\mathrm{PoF,CIR-first}} = \frac{c_0}{2} \min_{\tau} \left\{ \tau : \left(\frac{|h(\tau;t)|}{h_{\max}} \right)^2 \geq \gamma_{\mathrm{first}} \cap \left| \tau_{h_{\max}} - \tau \right| \leq \frac{R_{\mathrm{first}}}{c_0} \right\}. \tag{3.91}$$

The thresholds need to be adapted to the propagation channel characteristics and the ranging ambiguity. This is necessary as paths of long excess delays may appear before the actual first path due to circularity of the CIR.

It is desirable to remove the phantom paths between the actual paths as they degrade range resolution ΔR by a factor 2 [Sch11]. A possible strategy on how to obtain H from H^2 is investigated in [Sch11; SS10]. However, this requires transmitting packets twice in each channel, respecting a specific timing and channel-hopping scheme. These requirements make the application of this technique in the LPWA context less appealing.

Estimating $\tau_0 + t_0$ and $\tau_0 - t_0$ based on the one-way CIRs and summing them up as in the phase slope method is an alternative. However, it introduces the problem of estimating the first path in a circularly shifted CIR. This approach hence only works if the first path is the strongest path.

Other range estimation algorithms are possible:

- **Optimization approach**: Range estimation through minimization, *e.g.* by least-square optimization, of the error between estimated localization metrics and a model.
- **Multiple Signal Classification (MUSIC)**: The multi-channel delay estimation can be formulated MUSIC estimation problem. This method is investigated in Chapter 5.1.2.1.
- **Learning based approach**: Localization metrics, *e.g.* amplitude, time and phase can be fed directly to a learning algorithm, which outputs range estimates. These methods in contrast to parametric estimation require a training phase with labeled data, i.e. data with the ranging ground truth. These approaches are investigated in Chapter 5.1.2.2.

While the phase slope approach requires the strong hypothesis of free-space propagation, all other methods can be used in multipath propagation.

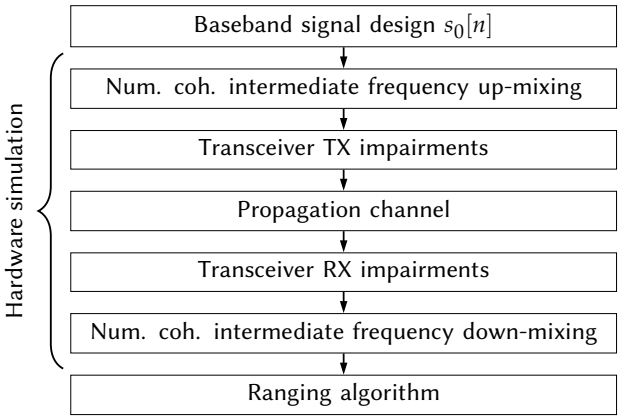


FIGURE 3.23 – *Signal processing steps in numerical simulation for ToF and PoF ranging techniques.*

3.5 Analysis by Simulations in an AWGN Channel

The following analysis by numerical simulation based on the timeslot two-way signal model (see Chapter 3.2.2.2) has multiple purposes:

- Validation of the signal model.
- Benchmarking of localization metric extraction algorithms given in Chapter 3.4.1 and comparison to the CRLB.
- Illustration of the performances for ToF and multi-channel PoF ranging.
- Providing design guidelines for the hardware implementation and dimensioning of system parameters.

Numerical simulations are limited to an AWGN channel in this chapter. Simulations considering multipath channel models are presented in Chapter 4.2.4.

3.5.1 Simulation Setup

The simulation setup is depicted in Figure 3.23 and detailed in the following:

- **Baseband signal design** s_0: For ranging purposes only the preamble is considered in the baseband waveform s_0. The preamble follows a Gold sequence of length 32 and is modulated as Binary Phase Shift Keying (BPSK) signal of a bandwidth $B = 10\,\text{kHz}$. This parameter choice is typical for LPWA physical layers and can be compared to *e.g.* Sigfox and compatible transceiver chips fromTable 1.3.
- **Numerical coherent IF up-mixing**: According to the transceiver architecture from Figure 3.9b, where channel switching is performed numerically, the baseband waveform is up-mixed to the set of channels $[0,\, C-1]$ with a total of $C = 16$ channels and an uniform channel spacing $\Delta f = 200\,\text{kHz}$. This results in a virtual bandwidth $B_{\text{virt}} = 3\,\text{MHz}$, a range resolution $\Delta R = 50\,\text{m}$ and a range ambiguity $R_{\max} = 750\,\text{m}$.
- **AD9361 TX impairments**: The transmitter impairments from the numerical IF stage to the antenna are simulated in the following.

  A constant clock frequency offset δ_f is considered. Typical offsets from $\pm 10\,\text{ppm}$ are taken into account. Digital to analog conversion is simulated by considering only SFO which is simulated by resampling the IF signal. The unknown time reference t_0 is simulated by an arbitrary time shift $|t_0| \leq 600\,\mu\text{s}$. An uniform distributed phase shift $\phi_{\text{R}} \in [0, 2\pi)$ is added to the resulting "analog" signal to simulate unknown initial LO phase. Constant CFO is simulated in baseband by introducing a frequency shift $\delta_f f_{\text{w}}$. This signal is then passed into the propagation channel.
- **Propagation channel**: The radio propagation channel is given by a frequency flat channel, i.e. free-space propagation. Delays τ_0 corresponding to ranges $[0 - 4\,\text{km}]$ are simulated.
- **AD9361 RX impairments**: Analog to the AD9361 TX impairments step, the same operations are performed in inverse order to simulate the equivalent behavior on the receiving side.
- **Numerical coherent IF down-mixing**: Equally analog to the numerical coherent IF up-mixing step.
- **Ranging Algorithm**: The resulting baseband received signals $r_c^{[T,R]}$ are processed with the localization metric extraction algorithm presented in Chapter 3.4.1.1. Range estimates for single channel (3.82) and

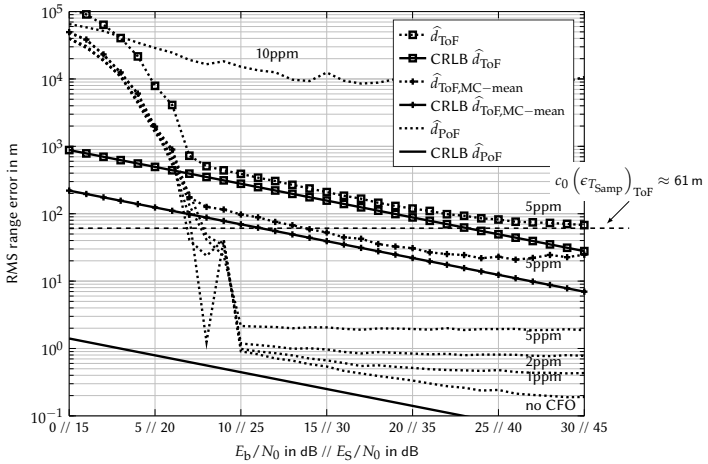


FIGURE 3.24 – *Simulated ranging error in a frequency flat channel with a signal bandwidth $B = 10\,\mathrm{kHz}$, $C = 16$ channels and a virtual multi-channel bandwidth $B_{\mathrm{virt}} = 3.0\,\mathrm{MHz}$ with parameters from Table 3.3.*

multi-channel (3.83a) ToF and multi-channel PoF (3.90) are compared.
Simulation results are given for 10^3 independent realizations. Table 3.3 summarizes the numerical values.

Parameter	**Numerical value**
Delay τ_0	uniform in $[0, 4]\mathrm{km}/c_0$
Time offset t_0	uniform in $[-600, +600]\mu\mathrm{s}$
Initial LO phase $\Delta\tilde{\phi}_{\mathrm{R}}$	uniform in $[0, 2\pi)$
Carrier frequency f_{W}	868 MHz
Waveform s_0	BPSK
	B=10 kHz
	Gold code of length $K_{\mathrm{code}} = 32$
Channel spacing Δf	200 kHz
Number of channels C	16
Virtual bandwidth B_{virt}	3 MHz
Maximum unambiguous range $R_{\max}$	750 m
Range resolution ΔR	50 m
IF sampling frequency $f_{\mathrm{Samp,IF}}$	20 MHz
Baseband sampling frequency $f_{\mathrm{Samp,BB}}$	1 MHz
Number of realizations	10^3

TABLE 3.3 – *Parameters for numerical simulations of ToF and PoF ranging.*

3.5.2 Simulation Results in Free-space Propagation

Figure 3.24 illustrates the RMS ranging error for the aforementioned setup. Single channel and multi-channel ToF ranging achieve for sufficient E_S/N_0, precisions close to the respective CRLB. For low $E_b/N_0 = E_S/N_0/K_{\mathrm{code}}$, CFO estimation with [MM97] fails and hence localization metric extraction. In the high E_S/N_0 regime, the precision is bound by the uniform distributed sampling resolution error, which evaluates here to

$$c_0\left(\epsilon_{T_{\mathrm{Samp}}}\right)_{\mathrm{ToF}} = \frac{c_0\left(\epsilon_{T_{\mathrm{Samp}}}\right)_{\mathrm{ToA}}}{\sqrt{2}} = \frac{c_0}{\sqrt{2}\sqrt{12}f_{\mathrm{Samp,BB}}} \approx 61\,\mathrm{m}. \tag{3.92}$$

Multi-channel PoF achieves the respective CRLB in the CFO free case, while increasing CFO degrades ranging precision. Meter-level precision can be achieved with 10 kHz signal bandwidth and a reasonable number of channels $C = 16$ and a total virtual bandwidth compliant with the authorized bandwidth in the SRD 868 MHz band.

As can be seen from Figure 3.24, CFO significantly limits precision for PoF ranging. Calculating the PoF includes the Term IV error according to (3.84). This error arises from the fact that the two phase estimations $\widehat{\phi_{\mathrm{A}c}}^{[T_1,R_2]}$ and $\widehat{\phi_{\mathrm{A}c}}^{[T_1,R_2]}$ are performed at time instances separated by the length of the transmission or packet $K_S T_{\mathrm{Samp}}$, as

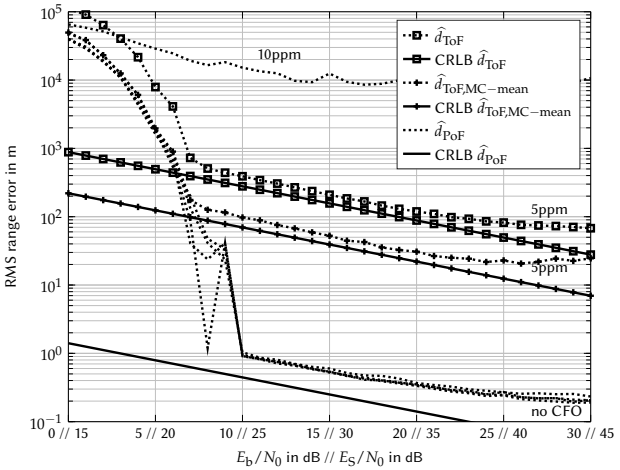


FIGURE 3.25 – *Simulated ranging error integrating the correction of CFO induced errors in a frequency flat channel with a signal bandwidth* $B = 10\,\mathrm{kHz}$, $C = 16$ *channels and a virtual multi-channel bandwidth* $B_{\mathrm{virt}} = 3.0\,\mathrm{MHz}$ *with parameters from Table 3.3.*

the two-way exchange is performed sequentially. For a maximum relative CFO of 10 ppm and a transmission or packet length $K_{\mathrm{code}}/B = 3.2\,\mathrm{ms}$, this error is given by $c_0\delta_f T_{\mathrm{Samp}} K_{\mathrm{S}} \approx 20\,\mathrm{m}$. This error is dominant compared to the other errors. However, it can be estimated and corrected. CFO estimation is available and the response time $K_{\mathrm{S}}T_{\mathrm{Samp}}$ is known, allowing compensating for this error by calculating

$$\widetilde{\widehat{\phi_{\mathrm{PoF}c}}}^{[1,2]} = \widehat{\phi_{\mathrm{PoF}c}}^{[1,2]} - 2\pi\widehat{\delta_{f_c}}^{[T_2,R_1]}\left(f_{\mathrm{w}} + f_c\right) K_{\mathrm{S}} T_{\mathrm{Samp}}. \tag{3.93}$$

Utilising (3.93) instead of (3.84) for CIR reconstruction, gives the results plotted in Figure 3.25. The simulation results show that CFO can be compensated and that the remaining CFO influence is negligible. Considering the aforementioned results, meter-level ranging precision can be achieved in free-space radio channels with LPWA compatible narrowband signals and reasonable E_{S}/N_0.

Considering the convergence point at $(E_{\mathrm{S}}/N_0)_0 = 25\,\mathrm{dB}$ as nominal operation point, receiver sensitivity is given by

$$\begin{aligned}\left(P_{\mathrm{req}}\right)^{\mathrm{dBm}} &= \left(\frac{E_{\mathrm{S}}}{N_0}\right)_0^{\mathrm{dB}} - \left(K_{\mathrm{code}}\right)^{\mathrm{dB}} + \left(k_{\mathrm{B}}\mathrm{Temp}\right)^{\mathrm{dBm/Hz}} + \left(B\right)^{\mathrm{dBHz}} + \left(N_{\mathrm{F}}\right)^{\mathrm{dB}} \\ &= 25\,\mathrm{dB} - 15\,\mathrm{dB} - 174\,\mathrm{dBm/Hz} + 40\,\mathrm{dBHz} + 2.5\,\mathrm{dB} \\ &= -121.5\,\mathrm{dBm}.\end{aligned} \tag{3.94}$$

According to (1.10), a transmit power $P_{\mathrm{t}} = 14\,\mathrm{dBm}$ leads to a link budget $L = 135.5\,\mathrm{dB}$. A coverage extrapolation with the Hata [Hat80] *suburban* and *rural* propagation conditions predicts a coverage of 2.5 km and 4 km respectively. These are LPWA typical coverages.

3.6 Conclusion and Perspectives

The principle of multi-channel ranging relies on sensing the radio channel with narrowband signals at different frequencies and retrieving amplitude and phase information. This channel estimation repeated at multiple frequencies, can be interpreted as sampling the channel transfer function in frequency domain at these frequencies. The number of channels and their spacing define the so-called virtual bandwidth, i.e. the equivalent bandwidth when sensing the propagation channel with a single signal of large instantaneous bandwidth. These parameters determine the performances of multi-channel ranging.

A detailed signal model has been developed which allows studying the complete processing chain, comprising the signal generation on the transmitter, the propagation channel and reception by the receiver. Based on the signal model, closed form expressions for localization metrics such as RSSI, ToA and PoA and their dependency on clock impairments and the propagation channel are given. The general signal model suited for both, ToF and Time Difference of Arrival (TDoA) like approaches is then developed for ping-pong and timeslot two-way ranging. Considering constant, time invariant clock offsets, the transceiver architecture requires sharing a common phase reference between the transmitter and the receiver branch. This can be achieved through intra-node calibration, a common local oscillator or a numerical intermediate frequency mixing stage to maintain phase coherence over the

multiple channels. Phase coherence between two nodes is established in a packet exchange following a round trip protocol.

The numerical evaluation of theoretical performance bounds shows that constant clock offsets are not impeding ranging precision. Theoretically multi-channel ranging achieves under AWGN conditions meter-level precision with Ultra-Narrow Band (UNB) 1 kHz signals, a virtual bandwidth covering the available 7 MHz in the SRD 868 MHz band and technically typical SNR levels. Modeling propagation channels as prior information allows evaluating the CRLB for multipath scenarios. Ranging precision significantly degrades, with a RMS error of 70 m in the ETSI Tux channel. Performances are bound by the channel coherence bandwidth.

Based on these promising results, a correlation based localization metric extraction algorithm is designed. This algorithm is equivalent to the synchronization process required in every wireless receiver for data reception. The proposed algorithm is hence compatible with existing LPWA transceivers with minor modifications to obtain estimated channel state information. The sequentially estimated channel transfer function is converted to an estimate of the CIR upon which the range between the nodes is estimated with a first path detection algorithm.

The algorithm is tested with AWGN simulations. For this purpose, the ranging algorithm is applied to received signals generated according to the presented signal model. The designed algorithm attains in simulation asymptotically the CRLB and the impact of CFO on the ranging precision can be corrected as predicted with the theoretical CRLB.

In order to get more detailed insight into expectable ranging performances in terms of accuracy and precision, the CRLB can be moreover evaluated *e.g.* for a two-path propagation model or for channel models with Rician fading, i.e. with a specular component for the direct LoS path. The IDFT based range estimator can be optimized with proper windowing to reduce side lobes, and hence improve in multipath performances.

Bibliography of Chapter 3

[CZZ75] D. Chazan, M. Zakai, and J. Ziv. "Improved Lower Bounds on Signal Parameter Estimation". In: *IEEE transactions on Information Theory* 21.1 (1975), pp. 90–93.

[DW09] D. Dardari and M. Z. Win. "Ziv-Zakai Bound on Time-Of-Arrival Estimation with Statistical Channel Knowledge at the Receiver". In: *2009 IEEE International Conference on Ultra-Wideband*. 2009, pp. 624–629.

[ETS10] ETSI. *Universal Mobile Telecommunications System (UMTS); Deployment aspects (3GPP TR 25.943 version 9.0.0 Release 9)*. European Telecommunications Standards Institute (ETSI), 2010.

[Hat80] M. Hata. "Empirical Formula for Propagation Loss in Land Mobile Radio Services". In: *IEEE Transactions on Vehicular Technology* 29.3 (1980), pp. 317–325.

[KH06] E. Kaplan and C. Hegarty. *Understanding GPS: Principles and Applications*. Second Edition. Artech House, 2006.

[Kar+11] Y. Karisan et al. "Range Estimation in Multicarrier Systems in the Presence of Interference: Performance Limits and Optimal Signal Design". In: *IEEE Transactions on Wireless Communications* 10.10 (2011), pp. 3321–3331.

[Kay93] S. M. Kay. *Fundamentals of Statistical Signal Processing: Estimation Theory*. 1993.

[LZP11] S. Lanzisera, D. Zats, and K. S. J. Pister. "Radio Frequency Time-of-Flight Distance Measurement for Low-Cost Wireless Sensor Localization". In: *IEEE Sensors Journal* 11.3 (2011), pp. 837–845.

[MM97] U. Mengali and M. Morelli. "Data-Aided Frequency Estimation for Burst Digital Transmission". In: *IEEE Transactions on Communications* 45.1 (1997), pp. 23–25.

[PSSV09a] M. Pichler, S. Schwarzer, A. Stelzer, and M. Vossiek. "Multi-Channel Distance Measurement With IEEE 802.15.4 (ZigBee) Devices". In: *IEEE Journal of Selected Topics in Signal Processing* 3.5 (2009), pp. 845–859.

[SVPS08] S. Schwarzer, M. Vossiek, M. Pichler, and A. Stelzer. "Precise distance measurement with IEEE 802.15.4 (ZigBee) devices". In: *2008 IEEE Radio and Wireless Symposium*. 2008, pp. 779–782.

[Sch11] S. Schwarzer. "Entwicklung eines industriellen Funkortungssystems basierend auf der kohaerenten Kombination von Kommunikationssignalen mit IEEE-802.15.4-Geraeten". PhD thesis. Technischen Universitaet Clausthal, 2011.

[SS10] S. Schwarzer and C. Saisenberger. "Verfahren zur Ortung von drahtlos kommunizierenden Funkteilnehmern". Pat. 10 2008 034 567. 2010.

[Sha48] C. Shannon. "A Mathematical Theory of Communication". In: *The Bell System Technical Journal* 27.3 (1948), pp. 379–423.

[VT04] H. L. Van Trees. *Detection, Estimation, and Modulation Theory*. John Wiley and Sons, 2004.

4

Experimentations and Field Trials

"Erfindungen, die die Welt verändern, werden nicht nur im dunklen Kämmerchen gemacht."

— Guglielmo Giovanni Maria Marconi (1874 – 1937)

Chapter contents

Simulations of multi-channel ranging revealing a significant performance gain compared to time based ranging techniques are validated with experimentation and field trials. For this purpose a multi-channel ranging enabled transceiver testbed is designed. Simulation results are compared to experimental measurements in a cabled Additive White Gaussian Noise (AWGN) channel. Several multi-channel ranging field trial measurement campaigns are performed in outdoor long-range propagation conditions. Performances are analyzed and strategies to combat multipath induced biases are proposed. Multi-channel ranging with the developed transceiver testbed is compared to an existing industrial LPWA ranging solution.

4.1 Multi-Channel Ranging Radio Transceiver Testbed

4.1.1 General Purpose and Specification

The main purpose of the multi-channel ranging radio transceiver testbed is, to transmit and receive LPWA signals according to the multi-channel ranging signal model presented in Chapter 3.2. The portable testbed is designed for experimental validation in the laboratory as well as for outdoor field trials. The radio transceiver testbed allowing performing multi-channel range estimation with Phase of Flight (PoF) measurements is hereafter referred to as Coherent Ranging On Narrowband Enabled Networks (CRONEN).

A transmitter allowing to send different waveforms s_0 offers the ability to flexibly test various configurations and LPWA physical layers. The straightforward approach combines MATLAB based waveform generation and a Radio Frequency (RF) transmitter capable of sending IQ samples. In order to get detailed insight into the performances of localization metric extraction algorithms and ranging estimators on real signals, data needs to be recorded for repeatable post-processing. This allows visualizing received waveforms and benchmarking of different algorithms on identical data for a fair comparison. For this purpose, the radio transceiver testbed is equally required to record raw IQ data for offline post-processing. This offers furthermore the flexibility of rapid algorithm prototyping and debugging with MATLAB instead of long development times for the implementation of embedded algorithms, *e.g.* with C language or Very High Speed Integrated Circuit Hardware Description Language (VHDL).

A popular choice for this type of requirements is the use of a Software Defined Radio (SDR). Developing a SDR based multi-channel ranging testbed is furthermore supported by the fact that the access to IQ data or at least to localization metrics such as Time of Arrival (ToA) and Phase of Arrival (PoA) is not granted on commercial LPWA radio chipsets (see Table 1.3).

State-of-the art SDRs are based on a Field Programmable Gate Array (FPGA) for rapid and flexible implementation as well as on a versatile radio front-end. Table 4.1 gives a non-exhaustive list of current state-of-the art SDRs according to [Cro17] and their features relevant for multi-channel ranging. For the implementation of the multi-channel ranging transceiver testbed CRONEN, a custom SDR, called FLEX board has been chosen. The FLEX board is based on a Xilinx Zynq-045 System on Chip (SoC) [Xil15] and an Analog Devices AD9361 radio-front end [Ana13]. Main criteria for this choice are the availability in the laboratory as well as existing FPGA designs that can be adapted for the purpose of this thesis. It is worth noting that the FLEX board and the Ettus B210 SDR are based on similar hardware.

The requirements for SDRs regarding multi-channel ranging are discussed in the following. Common SDRs are based on radio-front ends, such as the Analog Devices AD9361 chipset, that allow Frequency Division Duplex (FDD) operation mode which implies that transmitter and receiver path have independent Phase-Locked Loops (PLLs) for Local Oscillator (LO) frequency synthesis. This excludes the tranceiver architecture from Figure 3.9c with $\Sigma\Delta\phi_{\mathrm{R}c} = 0$. Consequently phase calibration or numerical Intermediate Frequency (IF) mixing according to Figure 3.9a or Figure 3.9b respectively, is required. For the realization of the multi-channel ranging transceiver testbed, the latter option has been chosen. This choice is rather arbitrary, but avoids supplementary processing to achieve phase calibration on each channel $f_{\mathrm{W}} + f_c$. Consequently channel switching f_c has to be performed in numerical domain, where phase coherence can be guaranteed.

Channel switching f_c can be realized during numerical offline waveform generation, i.e. with MATLAB by generating the two-way multi-channel transmit signal by joining the single channel transmit signals ${s_{\mathrm{IF}}}_c^{[T]} \in \mathbb{C}^{1\times K_{\mathrm{S}}}$

	FLEX board	**Ettus B210 (B200)** [Ett]	**LimeSDR** [Myr]	**HackRF One** [Gre]
FPGA	Xilinx Zynq-045 SoC	Spartan 6	Altera Cyclone IV	Xilinx CPLD (XC2C64A-7VQG100C)
PLGs	Full duplex FIFO buffer design 2×TX @32 kS 2×RX @64 kS	100 k (75 k)	40 k	64 macro-cells in CPLD
On board memory	512 MB RAM @2 MS/s	No		
Processor/ Operating system	ARM processor/ Embedded Linux	No		ARM processor (LPC4320FBD144)
Connectivity	USB 2.0 to host PC/ Ethernet	USB 3.0 to host PC		USB 2.0 to host PC
Radio front end	AD9361	AD9361 (AD9364)	LMS7002M	MAX5864 MAX2837 RFFC5072
Carrier frequency f_W	70 MHz − 6 GHz	70 MHz − 6 GHz	100 kHz − 3.8 GHz	1 MHz − 6 GHz
Bandwidth B	56 MHz	56 MHz	56 MHz	20 MHz
MIMO TX×RX	2 × 2	2 × 2 (1 × 1)	2 × 2	1 × 1
Transmit power P_t	0 dBm	10 dBm	10 dBm	−10 to 15 dBm
Oscillator stability	±0.5 ppm [Tai17]	±2 ppm	±2.5 ppm [Rak17]	±20 ppm
Phase coherence	Independent TX and RX LOs			Common TX and RX LO
Price	≈ 1500 $	≈ 1119 $ (686 $)	≈ 300 $	≈ 300 $

TABLE 4.1 – *Overview on current state-of-the-art SDRs.*

from (3.17) into the final signal

$$s_\mathrm{IF}^{[T_1]} = \left[s_{\mathrm{IF}_0}^{[T_1]}, \underbrace{(0,\ldots,0)}_{K_\mathrm{S}}, s_{\mathrm{IF}_1}^{[T_1]}, \underbrace{(0,\ldots,0)}_{K_\mathrm{S}}, \ldots, s_{\mathrm{IF}_{C-1}}^{[T_1]}, \underbrace{(0,\ldots,0)}_{K_\mathrm{S}} \right] \in \mathbb{C}^{1\times 2CK_\mathrm{S}},$$

$$s_\mathrm{IF}^{[T_2]} = \left[\underbrace{(0,\ldots,0)}_{K_\mathrm{S}}, s_{\mathrm{IF}_0}^{[T_2]}, \underbrace{(0,\ldots,0)}_{K_\mathrm{S}}, s_{\mathrm{IF}_1}^{[T_2]}, \underbrace{(0,\ldots,0)}_{K_\mathrm{S}}, \ldots, s_{\mathrm{IF}_{C-1}}^{[T_2]} \right] \in \mathbb{C}^{1\times 2CK_\mathrm{S}}, \tag{4.1}$$

with silence periods accounting for the reception in the timeslot when the other node is transmitting (see Chapter 3.2.2.2). This requires a minimum sampling frequency

$$f_\mathrm{Samp} \geq 2\max\left(|f_c|\right) \simeq B_\mathrm{virt}. \tag{4.2}$$

Analog to the transmitter, the receiver samples the entire virtual bandwidth B_virt and channel selection according to (3.27) is done in offline post-processing.

This approach, although offloading most signal processing to the offline, i.e. MATLAB domain, has the disadvantage of generating large data streams due to the combination of high sampling frequency for the aforementioned reasons and long LPWA transmission and reception durations.

For multi-channel ranging in the SRD 868 MHz band, a total virtual bandwidth of $(B_\mathrm{virt})_\mathrm{max} = 7\,\mathrm{MHz}$ can be used theoretically according to regulation [CEP18]. Considering the parameters from Table 3.3 and each I or Q value

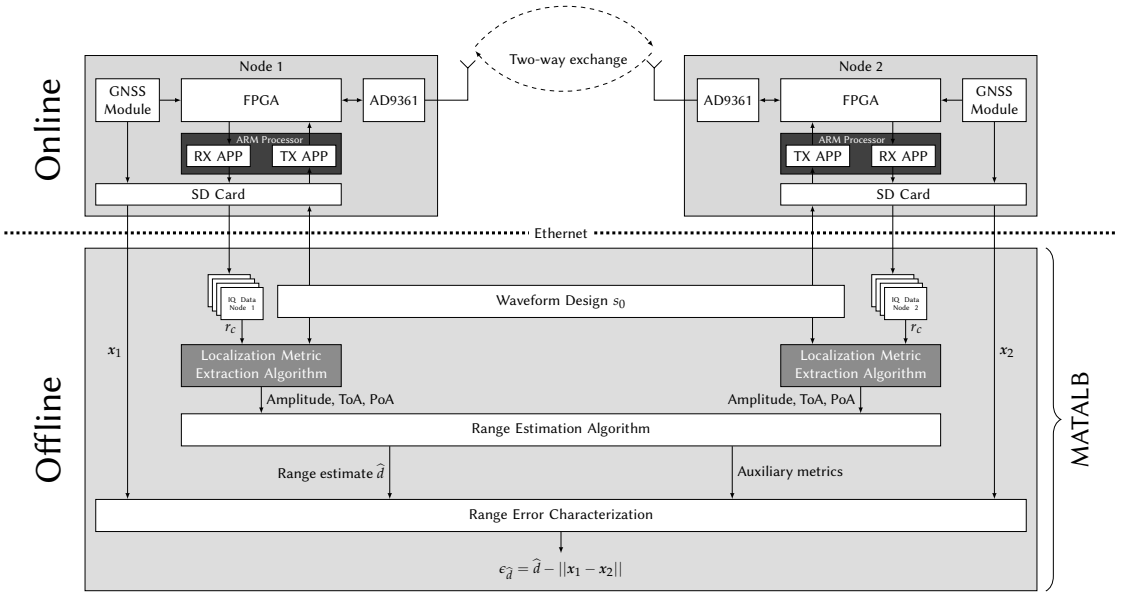


FIGURE 4.1 – *Overall system architecture and offline processing workflow for two-way multi-channel ranging.*

coded on $K_{\text{resolution}} = 16\,\text{bit}$, results in a total data size

$$F = \frac{K_{\text{code}}}{B} \cdot 2 \cdot C \cdot f_{\text{Samp,IF}} \cdot 2 \cdot K_{\text{resolution}} = \frac{32}{10\,\text{kHz}} \cdot 2 \cdot 16 \cdot 20\,\text{MHz} \cdot 2 \cdot 16\,\text{bit} = 8\,\text{MB}, \tag{4.3}$$

at a sampling frequency $f_S = 20\,\text{MHz} \gtrapprox 2 \cdot 7\,\text{MHz}$. Considering LPWA transmissions lasting up to $T_{\text{packet}} = 1\,\text{s}$ yields

$$F = T_{\text{packet}} \cdot 2 \cdot C \cdot f_{\text{Samp,IF}} \cdot 2 \cdot K_{\text{resolution}} = 1\,\text{s} \cdot 2 \cdot 16 \cdot 20\,\text{MHz} \cdot 2 \cdot 16\,\text{bit} = 2.6\,\text{GB}. \tag{4.4}$$

These large data streams cannot be stored in the Zynq-045 FPGA matrices. Direct Memory Access (DMA) architectures allow fast access and storing of the data on onboard Random Access Memory (RAM), while expensive high-speed Ethernet connections allow direct online offloading to a host processor [Dio+19].

At the time, when the multi-channel transceiver testbed was developed, DMA functions have not yet been implemented on the FLEX board and evaluated too time consuming to include into this work. Offloading IQ data to the RAM of the Advanced RISC Machine (ARM) processor, is implementation dependent limited to a maximum data rate of $\approx 2\,\text{MS/s}$ on the Advanced eXtensible Interface (AXI) bus between the ARM processor and the FPGA matrix. This limits the maximum virtual bandwidth to $B_{\text{virt}} \leq 2\,\text{MHz}/2 = 1\,\text{MHz}$. It is therefore inevitably to reduce data rate already in the FPGA before storage. With regard to multi-channel ranging, this is achieved by implementing the numerical IF up- and down-mixing function, i.e. (3.17) and (3.27) into the FPGA. Subsequently, data rate is adapted through up-sampling or decimation.

A baseband sampling frequency of 1 MHz is largely sufficient for LPWA waveforms and can be easily transferred over the AXI bus. The 512 MB RAM available on the FLEX board offers simultaneous storage of upto $512\,\text{MB}/(2 \cdot 32\,\text{bit/Sample}) \cdot 8\,\text{bit/byte} = 64\,\text{MSample}$, corresponding to $64\,\text{MSample}/1\,\text{MSample/s} = 64\,\text{s}$ transmit and receive streams of IQ samples on $2 \cdot 16\,\text{bit}$.

The implementation details are presented in the following.

4.1.2 Overall System Architecture

The overall system architecture for timeslot two-way multi-channel ranging and ranging error characterization is depicted in Figure 4.1. Each node, based on a FLEX board, comprises a SDR based on the Xilinx Zynq-045 SoC[1] [Xil15] and an Analog Devices AD9361 radio-front end [Ana13]. The Zynq-045 integrates an ARM processor running an embedded Linux operating system which is used for executing the transmission and reception applications which also configure the numerical IF up- and down-mixing stages in the FPGA matrix and the radio front-end. The MATLAB generated transmit waveform s_0 is once transferred via Ethernet to the SD card on the FLEX board. The transmission application reads the waveform IQ samples and transmits them, while the

[1] Xilinx Zynq XC7Z045-1FFG676.

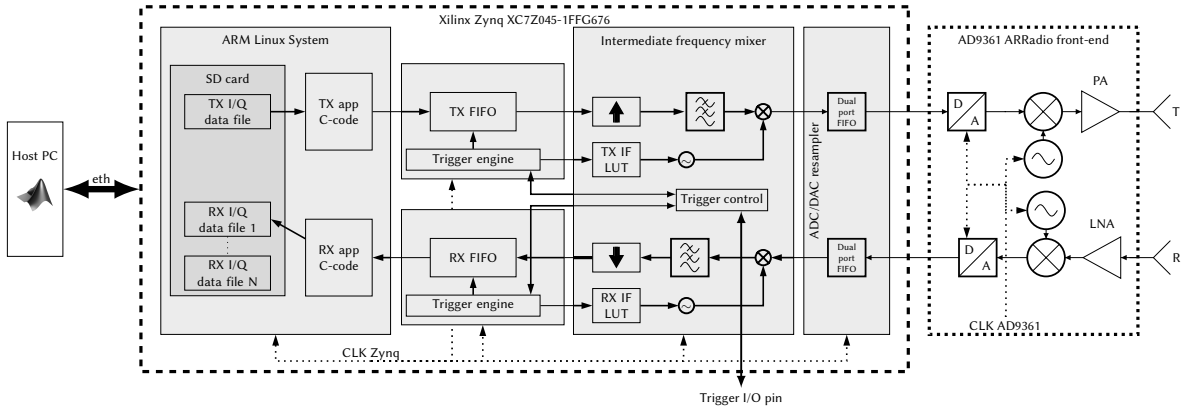


FIGURE 4.2 – *SDR based coherent multi-channel ranging transceiver testbed architecture.*

receive application stores IQ samples to the SD card. These IQ data files can then be offloaded via Ethernet to a host computer running MATLAB where localization metric extraction algorithms and range estimation (see Chapter 3.4) are performed.

Each node has an independent clock reference and hence nodes are not synchronized. This corresponds to the typical LPWA scenario where distant nodes and base stations do not share a common time reference. Due to the fact that received signals are only processed offline, no information is available online when to start IQ sample recording. This can be overcome by continuous recording, which results in large noise-only received data, which is impractical. Moreover, considering two-way ranging, nodes have to switch roles and a receiver becomes transmitter and vice versa. This requires inevitably some online information, i.e. signal detection.

In wireless communication systems, this information is naturally provided as the receiver aligns to the incoming signal for correct data demodulation. In this thesis, no online data demodulation is performed as signal processing is done in an offline step. Coarse synchronization is therefore achieved via Global Navigation Satellite System (GNSS) modules added to each transceiver testbed. The precise GNSS synchronization is voluntarily degraded by adding a sufficiently high time jitter to simulate coarse-only synchronization, replacing coarse-only synchronization i.e. through the Medium Access Control (MAC) layer or alignment to the preamble. The implemented ranging protocol corresponds hence to the timeslot two-way ranging (see Chapter 3.2.2.2).

In the following, implementation details of the multi-channel ranging testbed are presented.

4.1.3 Implementation Details

4.1.3.1 Transceiver Architecture

The radio transceiver testbed depicted in Figure 4.2 can be split into the Xilinx Zynq-045 SoC and the Analog Devices AD9361 radio-front end.

Xilinx Zynq-045 SoC

- **ARM processor**: The dual-core 1 GHz ARM processor is running an open embedded Linux operating system and has an external 512 MB RAM.
- **SD card**: The host PC can access the SD card via the ARM processor. SD card read and write speed are limiting factors for the rate with which range estimates can be repeated. A 32 GB SD card offers a 90 MB/s write speed [Pan17].
- **TX application**: The transmit application written in C-code, reads once the transmit IQ file to the RAM, configures the AD9361 as well as the signal processing blocks implemented into the FPGA matrix via registers. Over the AXI bus it then transfers the IQ samples to the TX FIFO in the FPGA matrix.
- **RX application**: The C-code application performs configuration analog to the TX application. Upon valid receive IQ samples in the RX FIFO, the application stores them to the ARM connected RAM. After completed reception, IQ data in the RAM is saved into a new RX IQ data file on the SD card.
- **TX/RX FIFO**: The 32 kS TX and 64 kS RX FIFOs serve as buffer between the non-real-time Linux operating system and the real-time signal processing towards the AD9361.
- **Trigger engine**: Based on the trigger signal from the trigger control block, the trigger engine starts IQ sample transfer to the IF mixing block for transmission, or sample storage in the RX FIFO for reception. The trigger

engine also controls the IF frequency for up- and down-mixing.

- **IF mixer**: The IF mixing stage performs up- and down-mixing as well as up-sampling and decimation for transmission and reception respectively. Details are presented in Chapter 4.1.3.2.
- **Trigger control**: The GNSS Pulse Per Second (PPS) signal used for coarse time synchronization, offers a 30 ns Root Mean Square (RMS) precision [Ubl] which corresponds to a 9 m ranging precision. The trigger signal is voluntarily degraded by adding a 1 ms $\equiv$ 300 km jitter. Consequently, the coarse time synchronization only offers frame alignment to a timeslot but not precision timing. Passing this degraded trigger signal to both, the TX and RX trigger engine, allows intra-node alignment of transmission and reception on a sample basis required for two-way ranging.
- **ADC/DAC resampler**: Dual-port FIFOs are used for sampling frequency adaptation between the FPGA and the AD9361. While the FPGA runs at a clock frequency of 125 MHz, the AD9361 is configured to the sampling frequency of 20 MHz. IQ sample transfer is realized with a data flow control structure. On the receiver side, each block pushes its data to the output and sets a valid flag. The AD9361 Digital to Analog Converter (DAC) sets a read request, which is passed through all bocks to the TX FIFO that pushes its data to the output and sets a valid flag. Data and the valid signal propagate through all blocks to the AD9361 DAC. Careful dimensioning of buffer sizes and thresholds for the read request avoid under- and overflows in the different FIFOs.

Analog Devices AD9361 radio-front end

The transmitter and receiver sampling frequency is set to 20 MHz and the IF low pass filter is configured with a cut-off frequency of 3.1 MHz corresponding to the virtual bandwidth of 3 MHz.

- **Transmitter**: Transmit samples are converted from digital to analog domain and up-mixed to carrier frequency f_w. The AD9361 on the ARRADIO board offers a maximum output power of $P_t \approx 0$ dBm.
- **Receiver**: The receiver comprises a Low Noise Amplifier (LNA) with a 2.5 dB noise figure, down-mixing and analog to digital conversion. The receiver has various variable gain stages. Automatic gain control is deactivated to avoid phase variations during a two-way multi-channel exchange and hence a degraded PoA metric. Adaptation of the gain to actual reception conditions, is achieved by monitoring the average signal amplitude in the RX application. The level on a completed multi-channel reception i comprising C channels is calculated and used to modify the gain for the next multi-channel reception $i+1$, to fit the dynamic range without saturation.

GNSS module

In order to characterize the ranging error for the range estimators from Chapter 3.4.2, the corresponding real range in an outdoor field trial needs to be determined. The ground truth is obtained from GNSS position estimates. For this purpose each testbed integrates a uBlox C94-M8P application board GNSS module [Ubl] which also provides the PPS signal used for coarse time synchronization. The module provides position estimates with a 2.5 m median error in normal urban conditions. Based on the two-dimensional GNSS positions and a prior known antenna height, ranging ground truth can be established. The ground truth reference error is neglected as the GNSS position inaccuracy of 2.5 m is smaller than the expected Time of Flight (ToF) and PoF ranging precision (see Figure 3.25).

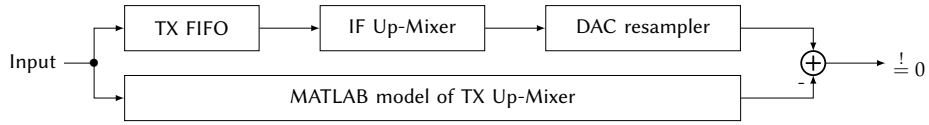
4.1.3.2 Numerical Intermediate Frequency Mixer

The numerical IF mixing stage realizes baseband to IF frequency conversion and channel switching according to (3.17) and (3.27), for transmitter and receiver respectively. Baseband IQ signals have a sampling frequency of 1 MHz largely sufficient for LPWA waveforms. In order to cover the entire SRD 868 MHz band of 7 MHz, a IF sampling frequency of 20 MHz has been chosen. The up-sampling by a factor 20 is achieved by inserting 19 zero samples. A 229 tap Finite Impulse Response (FIR) filter with a cut-off frequency of 500 kHz and a 30 dB stop band attenuation is used for interpolation. Up-conversion is realized with a mixer based on the Coordinate Rotation Digital Computer (CORDIC) algorithm, that adds a phase rotation $\phi[k]$ to the complex input sample $s[k]$ as

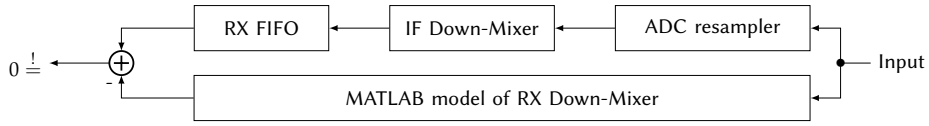
$$r[k] = s[k]\, e^{j\phi[k]}. \tag{4.5}$$

The instantaneous phase $\phi[k]$ is obtained through phase accumulation

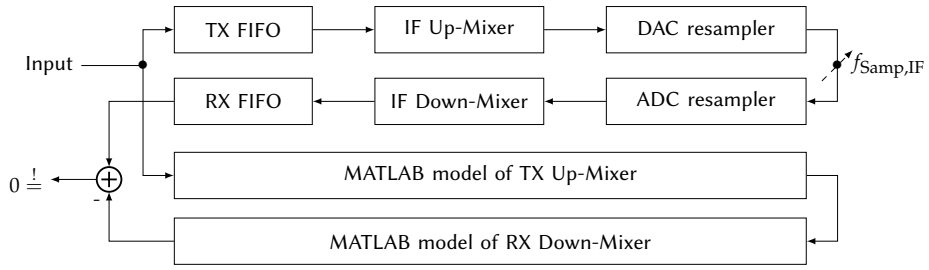
$$\phi[k] = \phi[k-1] + 2\pi\, f_c[k]\, T_{\text{Samp}} \mod 2\pi, \tag{4.6}$$



(a) *Transmitter validation.*



(b) *Receiver validation.*



(c) *Validation of the flow control structure, i.e. speed test.*

FIGURE 4.3 – *Signal flow diagrams for the validation of the VHDL design by comparison to MATLAB models of implemented processing blocks.*

with $\phi[0] = 0$ and instantaneous mixing frequency $f_c[k]$. The CORDIC algorithm offers an efficient way for the implementation of the IF mixer in VHDL.

The different channel frequencies f_c are stored in a Look-Up Table (LUT) and after utilizing channel frequency f_c for K_S samples, the LUT switches to frequency f_{c+1}. Phase accumulation is continuous over the set of C channels so that there are no phase discontinuities.

The receiver comprises the equivalent blocks in inverse order, performing down-conversion, anti-alias filtering and decimation.

Transmit and receive IF blocks share a common time reference and are aligned via the trigger control. This enables the required phase coherence between transmitter and receiver, i.e. $\Sigma\Delta\phi_{\mathrm{R}c} = \text{const.}$ required for multi-channel ranging.

4.1.3.3 Validation of the VHDL Design

The implementation of the presented transceiver testbed is based on an operational design comprising the TX/RX applications, TX/RX FIFOs and the ADC/DAC resampler, available in the laboratory. These blocks have been adapted in the framework of this thesis and the IF mixing block has been developed as well as the GNSS module added.

MATLAB models of the IF mixing block have been developed in order to verify the VHDL implementation. This verification is achieved through first simulating the VHDL blocks and comparing their outputs to the MATLAB generated output. And secondly, in final implementation, output signals are monitored on the DAC resampler for transmission (see Figure 4.3a) and input signals are injected at the Analog to Digital Converter (ADC) resampler for reception (see Figure 4.3b).

By these means, FPGA blocks have been validated to produce bit-identical outputs compared to their MATLAB models. The MATLAB models of the IF mixing block are integrated into the numerical simulations with MATLAB.

Verification of timing constraints and of the flow control structure is achieved by a loop-back of the DAC resampler output to the ADC resampler input. RX FIFO output is compared to the output of the concatenation of up- and down-mixier MATLAB models (see Figure 4.3c).

4.1.4 Radio Transceiver Testbed Variants and Parameterizations

During the different stages of this thesis, the multi-channel transceiver testbed has been adapted and parameterization modified. Extending the wireless transmission range has been the principal motivation for these modifications. Table 4.2 lists three main configurations used throughout this thesis.

		Config Short	***Config Long***	***Config FEM***
Number of channels	C	16		
Channel spacing	Δf	200 kHz		
Virtual bandwidth	B_{virt}	3 MHz		
Bandwidth	B	10 kHz		
Preamble code length	K_{code}	32 (Gold)	256 (Gold)	7 (Barker)
Preamble duration	T_{preamble}	3.2 ms	25.6 ms	0.7 ms
One-way ranging duration	T_{ranging}	51.2 ms	409.6 ms	11.2 ms
Hardware configuration		Passive circulator		FEM
Transmit power	P_{t}	0 dBm	−5 dBm	12.5 dBm
Noise figure	N_{F}	2.5 dB		2 dB
Ranging Signal to Noise Ratio (SNR)	$\left(\frac{E_{\text{S}}}{N_0}\right)_{\text{req}}$	[Wol+18a] Algo I 25 dB	[WdDC19a] Algo II 18 dB	Algo II (≈ 20 dB) The ranging SNR has not yet been verified experimentally, but is expected to be approximately similar to the other configurations.
Ranging receiver sensitivity	P_{req}	−121.5 dBm	−137.5 dBm	−119.5 dBm
Link budget	L	121.5 dB	127.5 dB	132 dB

TABLE 4.2 – *Radio transceiver testbed variants and parameterizations used in experimentations and field trials.*

The *Config Short* is considered the base configuration which allows illustrating the precision gain of multi-channel PoF ranging with narrowband signals. This configuration is sufficient for laboratory, i.e. cabled setups where receiver sensitivity is not of concern. Signal bandwidth and the resulting symbol duration are typical for LPWA modulation schemes.

Config Long provides improved receiver sensitivity through a processing gain by increasing the length of the preamble symbol code. The total multi-channel exchange attains durations in the order of several hundred milliseconds, which is typical for LPWA transceivers.

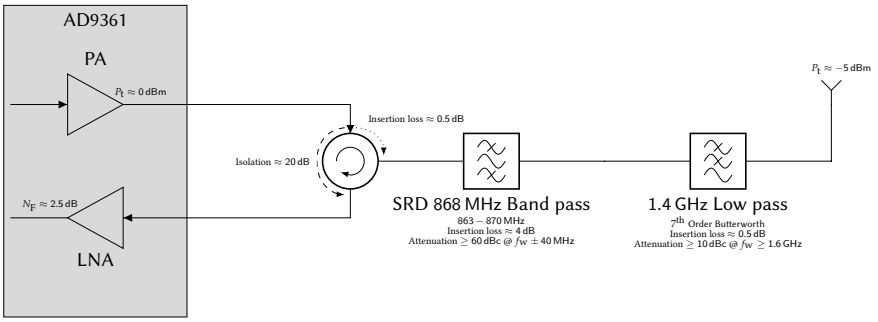
In order to connect the AD9361 Transmitter (TX) output and Receiver (RX) input to the same antenna, both *Config Short* and *Config Long* integrate a circulator as depicted in Figure 4.4a and Figure 4.5a. A 866.5 MHz band pass filter of 7 MHz bandwidth, 60 dB out-off band attenuation and a 4 dB insertion loss is used for the suppression of interferences outside the SRD 868 MHz band. This filter, although attenuating out-off band, has however pass bands at uneven multiples of its center frequency. Hence a 1.4 GHz low pass filter adds sufficient attenuation at frequencies around 2.6 GHz, corresponding to the third-order pass band of the band pass filter. Due to the insertion loss of the circulator and the filters, antenna port output power is limited to $P_{\text{t}} \approx -5$ dBm.

Config FEM overcomes the transmit power limitation of *Config Short* and *Config Long* by adding an active radio Front End Module (FEM) [Sky18, SKY66423-11EK3 Evaluation Board for 868 MHz Application.] comprising a Power Amplifier (PA), a LNA and a TX/RX switch. Switching the FEM from transmission to reception mode is aligned to transmit and reception timeslots (see Figure 3.8b) with a FPGA GPIO generated control signal. The complete setup is depicted in Figure 4.4b and Figure 4.5b. LPWA typical output powers of upto 20 dBm can be achieved with this configuration.

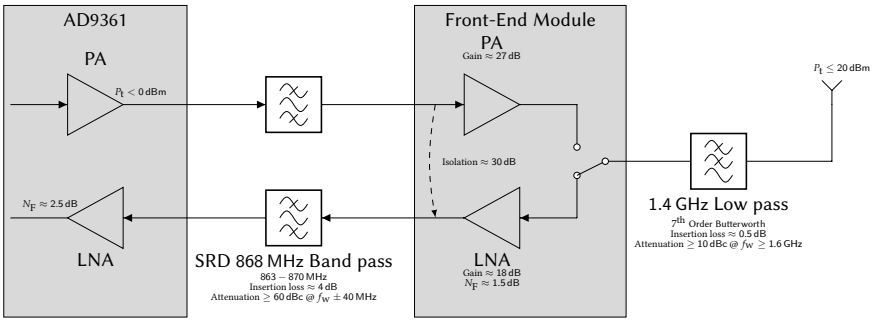
For the purpose of comparing the multi-channel ranging studied in this thesis to the ranging function in the commercially available LPWA LoRa 2.4 GHz SX1280 (SX1280) chipset [Sem17b], the preamble length has been set to a 7 bit Barker code. This parameterization offering a fair comparison with the SX1280, is justified and detailed in Chapter 4.3.1.3.

4.2 Simulations and Experimentations

The following sections study ToF and multi-channel PoF ranging through detailed simulation and experimentation. The gain in precision of the phase based ranging approach is illustrated and the influence of hardware imperfections, i.e. Carrier Frequency Offset (CFO) is investigated.

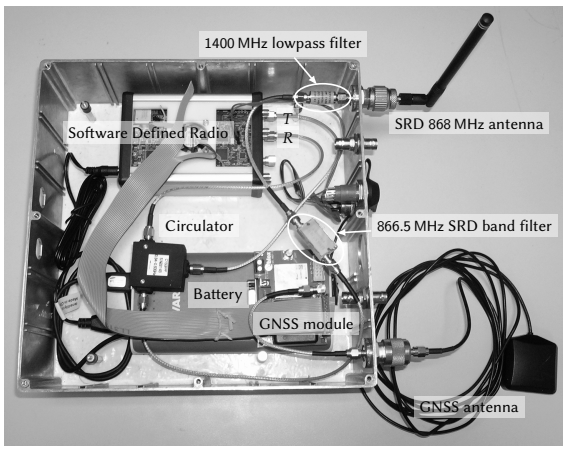


(a) *AD9361 RF setup with passive circulator.*

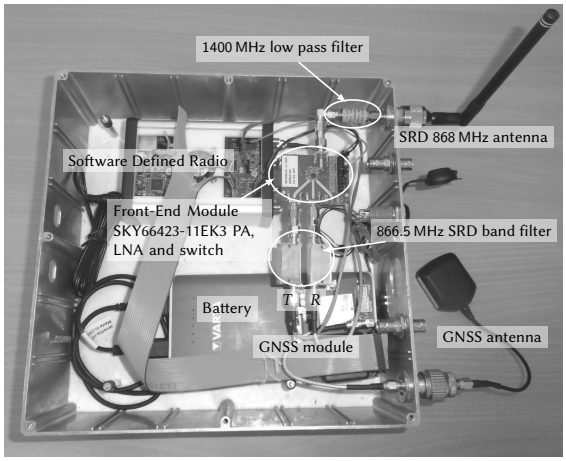


(b) *AD9361 RF setup with active FEM.*

FIGURE 4.4 – *RF hardware configurations for the transceiver testbed variants (schematic).*



(a) *AD9361 RF setup with passive circulator.*



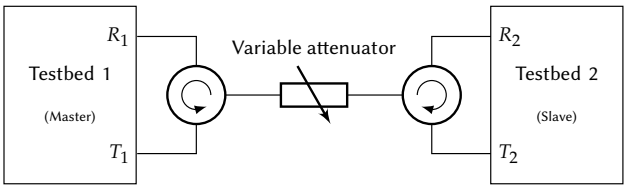
(b) *AD9361 RF setup with active FEM.*

FIGURE 4.5 – *RF hardware configurations for the transceiver testbed variants (photo).*

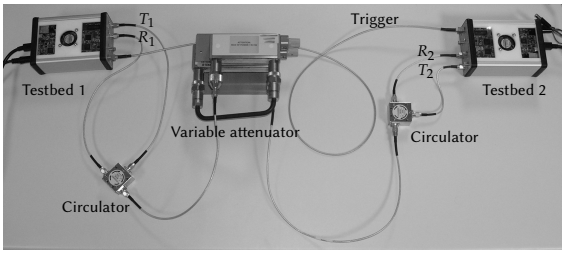
4.2.1 Hardware Calibration

4.2.1.1 Frequency

Each multi-channel transceiver testbed integrates a Voltage Controlled Temperature Compensated Crystal Oscillator (VCTCXO) clock reference [Tai17] characterized by a ± 0.5 ppm temporal frequency drift. The oscillators are trimmed so that the absolute residual remaining CFO is below ≈ 20 Hz, i.e. ≈ 23 ppb at 868 MHz. This allows performing experimentation without CFO.



(a) *Schematic of the cabled setup.*



(b) *Real setup with a trigger line for coarse time synchronization instead of GNSS based timeslot alignment.*

FIGURE 4.6 – *Experimental setup for multi-channel ranging in a cabled AWGN channel. The impact of AWGN on range estimation is evaluated for different E_S/N_0 obtained with a variable attenuator.*

4.2.1.2 Amplitude, Phase and Delays

Implementation dependent RF gains and phase shifts $g_{\mathrm{R}c}^{[X]}$ in (3.21) and (3.25) are generally frequency dependent and need hence calibration.

Furthermore, implementation specific time delays between the transmitter and the receiver path need to be calibrated. TX and RX FIFOs are synchronized in time (see Chapter 4.1.3.1), however the following blocks, *e.g.* the IF mixer with up-sampling and decimation as well as the analog hardware (filters, amplifiers) add time delays. These delays are deterministic and time invariant.

Calibration is therefore performed at a sufficiently high $E_S/N_0 = 20\,\mathrm{dB}$, where ToF and PoF estimation attain their respective Cramer Rao Lower Bound (CRLB) according to Figure 3.25. Implementation dependent time delays and phase shifts are measured in a cabled AWGN channel of a propagation delay $\tau_0 \approx 0\,\mathrm{s}$. A variable attenuator of attenuation A_V is used to select the E_S/N_0 according to

$$\left(\frac{E_S}{N_0}\right)^{\mathrm{dB}} = (P_t)^{\mathrm{dBm}} - (A_V)^{\mathrm{dB}} - (N_0)^{\mathrm{dBm/Hz}} - (B)^{\mathrm{dBHz}} + (K_{\mathrm{code}})^{\mathrm{dB}} - (N_F)^{\mathrm{dB}}, \tag{4.7}$$

whereby transmit power is verified with a spectrum analyzer. The setup for calibration and AWGN channel experimentation is depicted in Figure 4.6.

A total of $O = 10^2$ two-way exchanges is performed and localization metrics are extracted according to the algorithm from Chapter 3.4.

Delay calibration is achieved by subtracting the average ToF over all channels and all measurements from the un-calibrated ToF measurements. PoF measurements are calibrated by compensating the phase shift proportional to the propagation delay and channel frequency. For this purpose the average relative phase shift of adjacent channels over all channels and all measurements is calculated. Delay and phase calibrated ToF and PoF are given by

$$\widehat{T}_{\mathrm{ToF}_c}^{[1,2]} = \widehat{T}_{\mathrm{ToF}_c,\text{un-calibrated}}^{[1,2]} - \underset{O}{\mathrm{mean}}\left(\underset{c}{\mathrm{mean}}\left(\widehat{T}_{\mathrm{ToF}_c,\text{uncalibrated}}^{[1,2]}\right)\right), \tag{4.8a}$$

$$\widehat{\phi}_{\mathrm{PoF}_c}^{[1,2]} = \widehat{\phi}_{\mathrm{PoF}_c,\text{un-calibrated}}^{[1,2]} - c\ \underset{O}{\mathrm{mean}}\left(\underset{c\in[0,C-2]}{\mathrm{mean}}\left(\widehat{\phi}_{\mathrm{PoF}_{c+1},\text{un-calibrated}}^{[1,2]} - \widehat{\phi}_{\mathrm{PoF}_c,\text{un-calibrated}}^{[1,2]}\right)\right), \tag{4.8b}$$

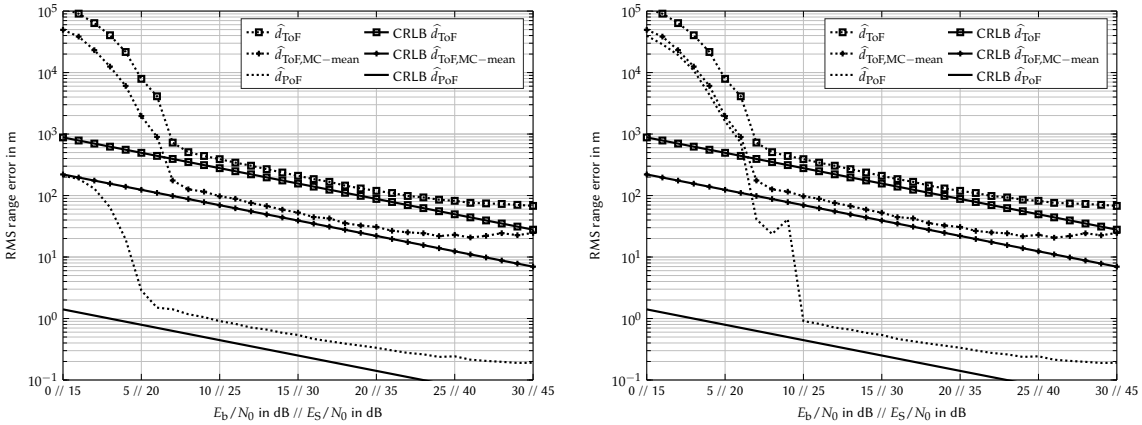
with un-calibrated ToF $\widehat{T}_{\mathrm{ToF}_c,\text{uncalibrated}}^{[1,2]}$ and PoF $\widehat{\phi}_{\mathrm{PoF}_c,\text{uncalibrated}}^{[1,2]}$ at propagation delay $\tau_0 \approx 0\,\mathrm{s}$.

The amplitudes of the complex hardware gains $g_{\mathrm{R}c}^{[X]}$ are considered to be constant over the maximum possible virtual bandwidth $B_{\mathrm{virt}} < 7\,\mathrm{MHz}$ in the SRD 868 MHz band. This assumption is valid regarding the magnitude of the frequency response of the various RF components over this rather narrow bandwidth. Amplitude, delay and phase variations during the multi-channel packet exchange are avoided by deactivation of the Automatic Gain Control (AGC). Different AD9361 receiver gain values do not show an impact on the localization metrics and calibration.

The calibration setup is performed for each hardware configuration from Table 4.2 and applied to the following experimentation and field trials.

4.2.2 Performances in an AWGN Channel

Initial simulations for an AWGN channel have been presented in Chapter 3.5. MATLAB simulations integrate the numerical IF up- and down-mixing blocks that produce identical output as the VHDL implementation.



(a) *PoF range ambiguity is not resolved but a prior known.* (b) *PoF range ambiguity is resolved with averaged ToF* $d_{ToF,mean}$ *estimates.*

FIGURE 4.7 – *Simulated RMS ranging error in an AWGN channel for a signal bandwidth* $B = 10\,\mathrm{kHz}$ *and a virtual multi-channel bandwidth* $B_{\mathrm{virt}} = 3\,\mathrm{MHz}$ *and Config Short parameterization from Table 4.2.*

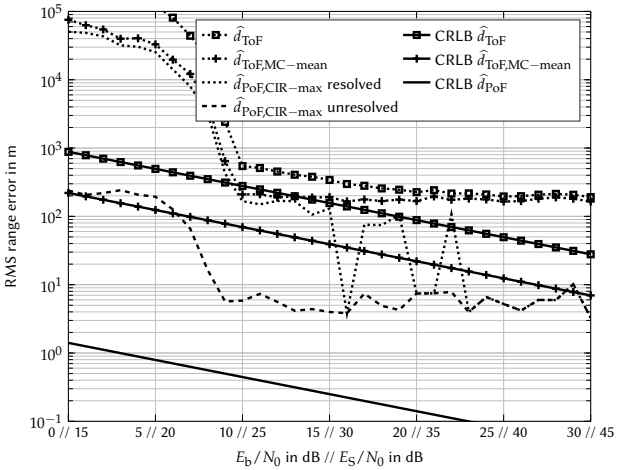


FIGURE 4.8 – *Measured RMS ranging error in an AWGN channel with the experimental setup from Figure 4.6 for a signal bandwidth* $B = 10\,\mathrm{kHz}$ *and a virtual multi-channel bandwidth* $B_{\mathrm{virt}} = 3\,\mathrm{MHz}$ *and Config Short parameterization from Table 4.2. PoF range estimation for resolved and unresolved ambiguity is depicted.*

Consequently, simulation and experimentation results may only vary due to the analog signal processing blocks and the radio channel.

Figure 4.7a shows simulation results for the *Config Short* with parameters given in Table 4.2. Simulations are performed without CFO and CFO in experimentation is considered negligible due to the oscillator calibration (see Chapter 4.2.1). Algorithms, however perform all steps, including CFO estimation and the associated corrections. The range ambiguity $R_{\max}$ is not resolved by ToF measurements but considered to be a prior known. As ranges $d \in [0, 4]\mathrm{km}$ are simulated, which are larger than $R_{\max} = 750\,\mathrm{m}$, range ambiguity is resolved with the actual, true range. Hence for low E_S/N_0, ranging errors are bound by the ambiguity, i.e. $R_{\max}/\sqrt{12} = 750\,\mathrm{m}/\sqrt{12} \approx 216\,\mathrm{m}$ RMS error. PoF ranging converges to the CRLB for $E_S/N_0 > 25\,\mathrm{dB}$.

Resolving the range ambiguity with averaged ToF $\hat{d}_{\mathrm{ToF,MC-mean}}$ measurements according to (1.74) is illustrated in Figure 4.7b. For low $E_S/N_0 < 25\,\mathrm{dB}$, ToF does not provide the required precision for correct range ambiguity resolution. Consequently, PoF ranging errors correspond to ToF errors. If ToF precision does not allow range ambiguity resolution, other techniques such as resolving the ambiguity on the system level with multiple base stations or by means of Angle of Arrival (AoA) estimation can be applied.

Figure 4.8 shows the experimental ranging error for the cabled AWGN channel setup from Figure 4.6 and *Config Short* parameterization from Table 4.2. Results for unresolved and $\hat{d}_{\mathrm{ToF,MC-mean}}$ resolved range ambiguity are illustrated. The causes for the level-out of ranging precision at high levels of SNR with *Config Short* have not been investigated further as PoF based ranging attains a RMS precision better than 10 m. This phenomen is not observed in the follwing experiments (see Figure 4.12) with *e.g. Config Long*.

Figure 4.9 depicts the Cumulative Distribution Function (CDF) of $\hat{d}_{\mathrm{ToF,MC-mean}}$ ambiguity resolved PoF

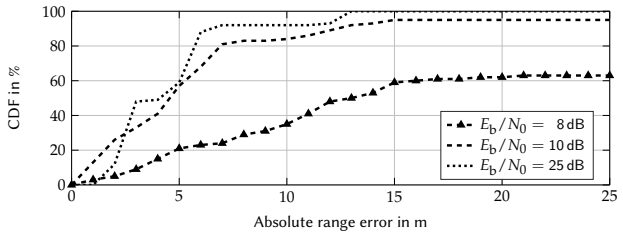
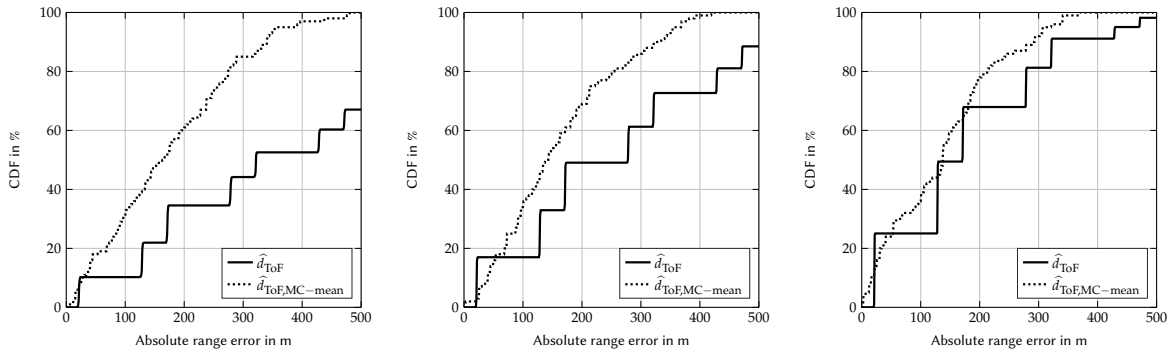


FIGURE 4.9 – *Measured PoF $\widehat{d}_{\text{PoF,CIR}-\max}$ ranging error CDF in an AWGN channel with the experimental setup from Figure 4.6 for a signal bandwidth $B = 10\,\text{kHz}$ and a virtual multi-channel bandwidth $B_{\text{virt}} = 3\,\text{MHz}$ and Config Short parameterization from Table 4.2.*



(a) $E_S/N_0 = 10\,\text{dB}$. (b) $E_S/N_0 = 15\,\text{dB}$. (c) $E_S/N_0 = 20\,\text{dB}$.

FIGURE 4.10 – *Measured ToF ranging error CDF in an AWGN channel with the experimental setup from Figure 4.6 for a signal bandwidth $B = 10\,\text{kHz}$ and a virtual multi-channel bandwidth $B_{\text{virt}} = 3\,\text{MHz}$ and Config Short parameterization from Table 4.2.*

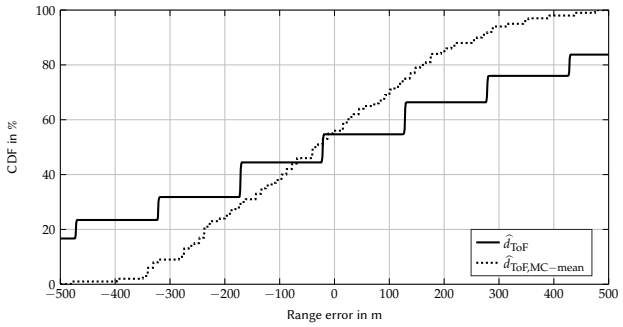


FIGURE 4.11 – *Measured signed ToF ranging error CDF at $E_S/N_0 = 10\,\text{dB}$ in an AWGN channel with the experimental setup from Figure 4.6 for a signal bandwidth $B = 10\,\text{kHz}$ and a virtual multi-channel bandwidth $B_{\text{virt}} = 3\,\text{MHz}$ and Config Short parameterization from Table 4.2.*

measurements and shows that in $\approx 10\%$ of the cases $\widehat{d}_{\text{ToF,MC}-\text{mean}}$ precision is insufficient for ambiguity resolution at $E_S/N_0 = 10\,\text{dB}$. As a result, the estimated and resolved PoF range is wrong by a multiple of $R_{\max}$, yielding large RMS errors in Figure 4.8.

Figure 4.10 shows the ToF CDF and shows that in about 10% of the cases the ranging error is above half the ranging ambiguity $R_{\max}/2$, explaining why PoF ambiguity resolution fails in these cases. Figure 4.10 also shows the improvement when averaging over successive and hence independent single channel ToF measurements.

The step-shaped CDF for single channel ToF ranging arises due to the baseband sampling frequency $f_{\text{Samp,BB}} = 1\,\text{MHz}$ leading to a $c_0/(2f_{\text{Samp,BB}}) = 150\,\text{m}$ ToF range resolution. Steps of different length are result of a non-zero range bias and the fact that the CDF for the absolute value of the error is depicted, leading to two error values for each range resolution bin. Figure 4.11 illustrates the signed ranging error CDF confirming the presence of a range bias.

PoF ranging error CDFs depicted in Figure 4.9 show that PoF ranging in an AWGN channel achieves sub-10 m ranging errors in 90% of the cases for sufficient high E_S/N_0.

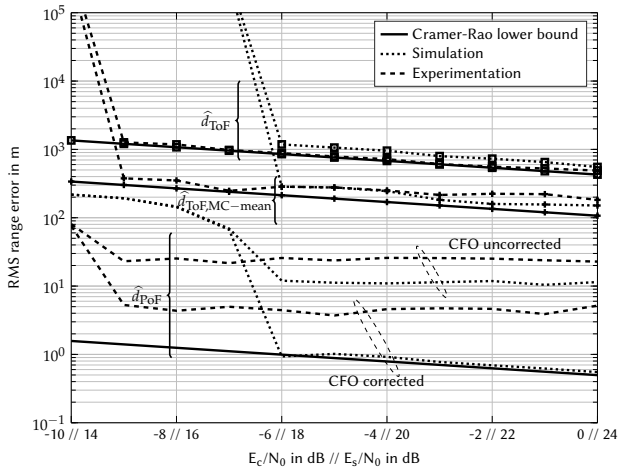


FIGURE 4.12 – *Simulated and measured RMS ranging error in an AWGN channel with the experimental setup from Figure 4.6 for a signal bandwidth $B = 10\,\mathrm{kHz}$ and a virtual multi-channel bandwidth $B_{\mathrm{virt}} = 3\,\mathrm{MHz}$ and Config Long parameterization from Table 4.2. The correction of CFO induced errors improves PoF ranging precision.*

4.2.3 Correction of Carrier Frequency Offset based Errors

Preliminary simulations (see Chapter 3.5) have shown that phase errors due to constant CFO can be corrected by applying (3.93).

Figure 4.12 illustrates ranging errors for ToF and PoF (unresolved ambiguity) ranging with CFO. Experimentations are performed with *Config Long* from Table 4.2 and the setup is depicted in Figure 4.5a. Simulations comprise a CFO $\delta_f \in [-5, 5]$ppm. In experimentation a constant 5 ppm CFO is achieved by modifying sampling and carrier frequency

$$f_{\mathrm{Samp,IF}} = 20\,\mathrm{MHz} \quad \rightarrow \quad f_{\mathrm{Samp,IF}} = (1 + 5\,\mathrm{ppm})\,20\,\mathrm{MHz} \quad = 20.000\,100\,\mathrm{MHz}, \tag{4.9a}$$

$$f_{\mathrm{w}} = 868\,\mathrm{MHz} \quad \rightarrow \quad f_{\mathrm{w}} = (1 + 5\,\mathrm{ppm})\,868\,\mathrm{MHz} \quad = 868.004\,340\,\mathrm{MHz}. \tag{4.9b}$$

The CFO error in form of Term IV in (3.82) has a negligible impact on ToF estimates as it is much smaller than the ToA estimation precision

$$\frac{c_0}{2}\frac{\delta_f}{1+\delta_f} K_{\mathrm{S}} T_{\mathrm{Samp}} = \frac{c_0}{2}\frac{5\,\mathrm{ppm}}{1+5\,\mathrm{ppm}} 25.6\,\mathrm{ms} = 19.2\,\mathrm{m} \ll 100\,\mathrm{m} \approx \frac{c_0}{2}\left(\epsilon^{[T_1,R_2]}_{\widehat{t_{\mathrm{A}c}}} + \epsilon^{[T_2,R_1]}_{\widehat{t_{\mathrm{A}c}}}\right). \tag{4.10}$$

Considering PoF measurements, CFO induced errors can be fully corrected in simulation, while experimentation only shows a precision improvement from 25 m to 5 m. Furthermore, experimentation results do not converge to the CRLB. This mismatch between simulation and experimentation can have different causes:

- CFO estimation in experimentation does not achieve the required precision.
- The hypothesis of a constant frequency offset is not valid for the given clock source and the considered two-way duration of $2T_{\mathrm{preamble}} = 51.2\,\mathrm{ms}$ or the multi-channel ranging duration $2T_{\mathrm{ranging}} = 819.2\,\mathrm{ms}$. Moreover, frequency drift and oscillator phase noise/jitter are hardware imperfections possibly affecting ranging precision.

4.2.4 Performances in a Multipath Propagation Channel

After having validated two-way multi-channel ranging by both simulation and experimentation in an AWGN channel, performances in multipath scenarios are investigated. Ranging errors are characterized by numerical simulation for different multi-channel parameterizations and different multipath channel types. Simulated ranging errors for the European Telecommunications Standards Institute (ETSI) Typical urban (Tux) multipath channel model [ETS10] (see Chapter 2.3.5) are given in Figure 4.13.

For first path detection, empirically determined threshold $\gamma_{\mathrm{first}} = -7\,\mathrm{dB}$ and range $R_{\mathrm{first}} = 300\,\mathrm{m}$ show best performances. These values are in coherence with the Tux channel model characteristics delay spread and path gain ratio. Globally, ranging precision degrades compared to the frequency flat AWGN channel.

A closer study of the set of C ToF measurements reveals that range is over-estimated due to multipath and hence resulting in a positive biased ranging error. For a frequency flat channel, no bias is observed. Therefore, the

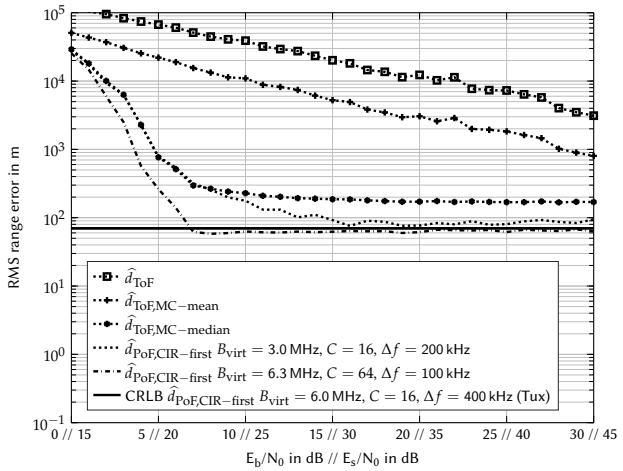


FIGURE 4.13 – *Simulated RMS ranging error in the ETSI Tux channel for a signal bandwidth $B = 10\,\mathrm{kHz}$ and a different virtual multi-channel bandwidths B_{virt} and Config Short parameterization from Table 4.2.*

median $\widehat{d}_{\mathrm{ToF,MC-median}}$ over the C ToF estimates drastically improves the ranging accuracy in multipath scenarios compared to averaging $\widehat{d}_{\mathrm{ToF,MC-mean}}$. Coherent multi-channel performances, with range ambiguity resolved by the median ToF range, show a small improvement compared to the time based approach. Increasing the number of utilized channels $C = 64$ with a frequency spacing $\Delta f = 100\,\mathrm{kHz}$, further improves coherent multi-channel performances. Whereas, the median on ToF estimates $\widehat{d}_{\mathrm{ToF,MC-median}}$ does not improve with more channels C. This is explained by the fact that single channel ToF measurements are statistically non independent but similarly biased due to multipath propagation and hence averaging or taking the median cannot improve the precision. Coherent multi-channel precision approximately reaches the multipath CRLB derived in Chapter 3.3.4.

4.3 Multi-Channel Ranging Field Trials

Simulation and experimentation have shown that PoF ranging outperforms ToF ranging in both AWGN and multipath channels. In order to confirm and complement numerical simulation results with multipath channel models, outdoor ranging field trials are performed. Field trials demonstrate the performances in a real world scenario and help adapting algorithms to the actual environment. Although field trials are a very valuable illustration, their generalization remains limited if sample size is small or the scenario too specific.

In the following, different field trial setups and the results are presented. A comparison to the ToF ranging function of the LoRa 2.4 GHz SX1280 radio chip [Sem17b] is made and an outlier detection, mitigation and elimination strategy is studied.

4.3.1 Urban Propagation Scenario

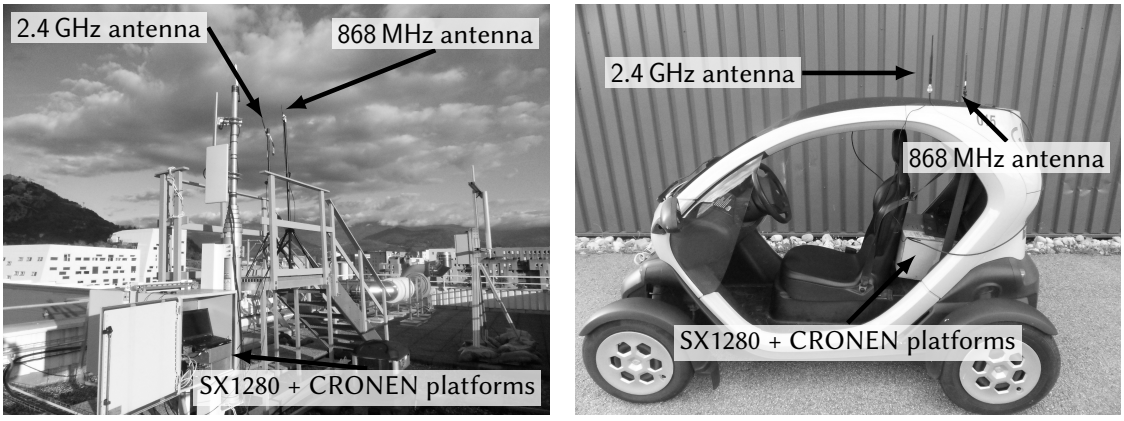
Field trials are performed in an urban propagation scenario on an industrial campus with mainly office buildings and open spaces, i.e. car parks and meadows.

In order to reflect a typical LPWA application scenario, one node is placed on a 26 m high roof top of an office building acting as base station. The other node is installed into a small electrical car with a plastic roof. The setup is depicted in Figure 4.14. The platform *Config FEM* variant from Table 4.2 is utilized for the following field trials.

Figure 4.15 shows the map of the campus and the measurement positions obtained through the GNSS acting as ground truth. The measurements are split into different propagation conditions according to their position:

- Line of Sight (LoS): The base station and the node are in LoS condition with only minor obstruction through trees and flat building.
- None Line of Sight (NLoS): The direct LoS path is blocked by a neighboring building b_3 which is higher than the roof top where the base station is installed.
- Urban canyon: The mobile node is in the street canyon between two five-story tall office buildings (b_1 and b_3) of which one of them is the building hosting the base station on its roof top.

Raw range estimates from ToF and PoF measurements are presented in Figure 4.16 and Figure 4.17. A total of 3500 measurements has been performed. The position index allows associating the ranging estimate to a position on the map given in Figure 4.15.



(a) *Base station testbed at a* 26 m *high roof top of an office building* b_1.

(b) *Mobile node installed into a small electrical car.*

FIGURE 4.14 – *Transceiver testbed setup for urban propagation scenario field trials.*

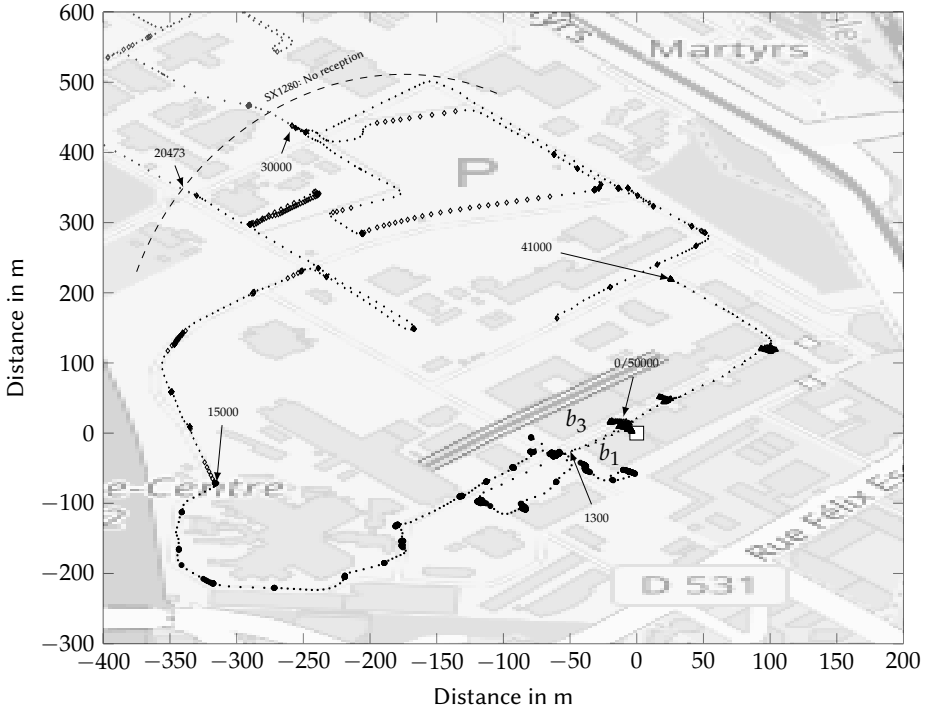
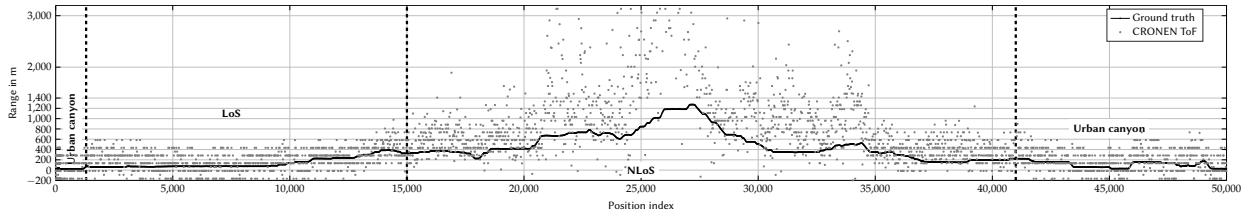
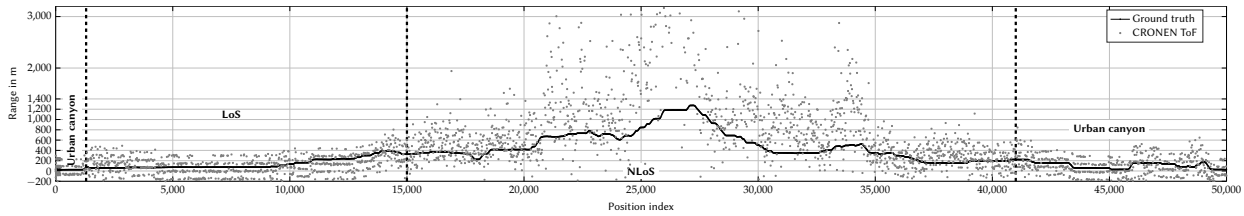


FIGURE 4.15 – *Ground truth positions for CRONEN. Base station (□) at height* $h_b = 26\,\text{m}$ *and mobile node at height* $h_m = 1.5\,\text{m}$. *Mobile node in LoS (•), NLoS (◇) and urban canyon (△) scenario. In bold are stationary position indexes.*

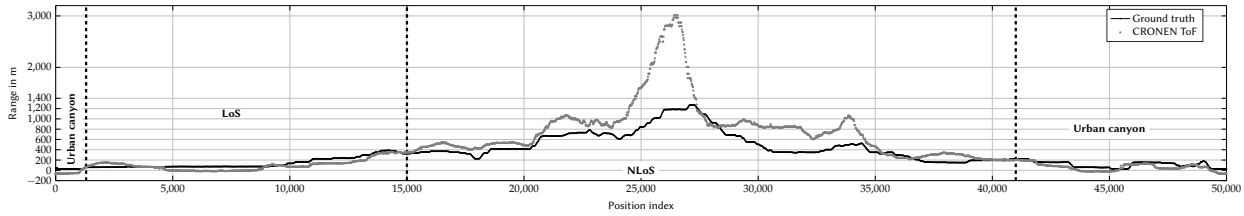
Calculating the median over C single channel ToF measurements clearly shows the sampling resolution step size of $c_0/(2 \cdot f_{\text{Samp,BB}}) = 150\,\text{m}$ as depicted in Figure 4.16a. The sampling resolution step size can equally be observed as 150 m step motive in the range estimation CDF in Figure 4.18a. Due to the continuous ground truth, the steps disappear in the ranging error CDFs in Figure 4.18c. Errors upto 500 m are observed for the urban LoS and urban canyon zones, while errors are much larger in NLoS condition. Interpolation of the received signals r_c before processing for localization metric extraction, *e.g.* ToA, with a factor 16 yields in a 9.4 m range resolution step size. Results in Figure 4.16b and Figure 4.18a confirm this. Interpolation however does only marginally improve ranging error statistics as illustrated in Figure 4.18c on single channel ToF, multi-channel averaged ToF and multi-channel ToF median measurements. Single channel ToF measurements attain less than 500 m in 70% of the cases. Averaging C single channel ToF measurements allows aggregating the same signal energy as used for multi-channel PoF measurements, however averaging results in less accurate estimates as large errors on single channel ToF measurements are taken into account. This can be overcome by calculating the median over C single channel ToF measurements, practically eliminating large outliers. Multi-channel ToF median range estimation achieves 500 m error in 80% of the cases. Figure 4.16c illustrates range estimation results, when combining successive



(a) *CRONEN raw ToF median range estimates* $\widehat{d}_{\text{ToF,MC}-\text{median}}$.

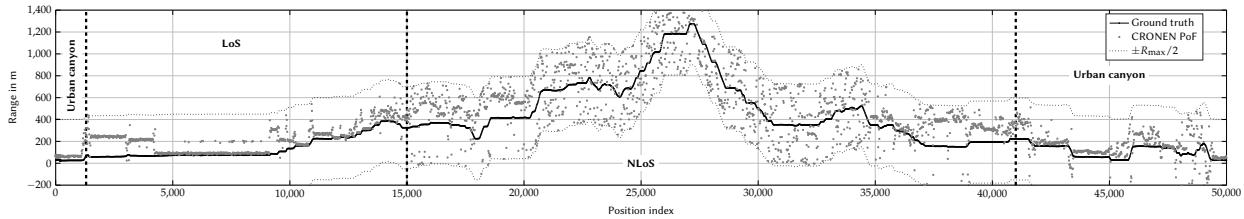


(b) *CRONEN raw ToF median range estimates with a factor* 16 *interpolation* $\widehat{d}_{\text{ToF,MC}-\text{median}_{IP16}}$.

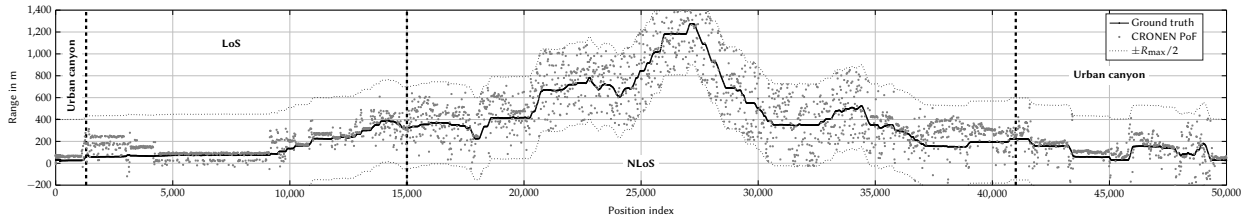


(c) *CRONEN raw ToF median range estimates with a factor* 16 *interpolation and smoothing over* 100 *successive measurements* $\widehat{d}_{\text{ToF,MC}-\text{median}_{IP16,S100}}$.

FIGURE 4.16 – *CRONEN raw ToF range estimates for the real outdoor scenario in Figure 4.15.*



(a) *CRONEN raw PoF range estimates* $\widehat{d}_{\text{PoF,CIR}-\text{max}}$.

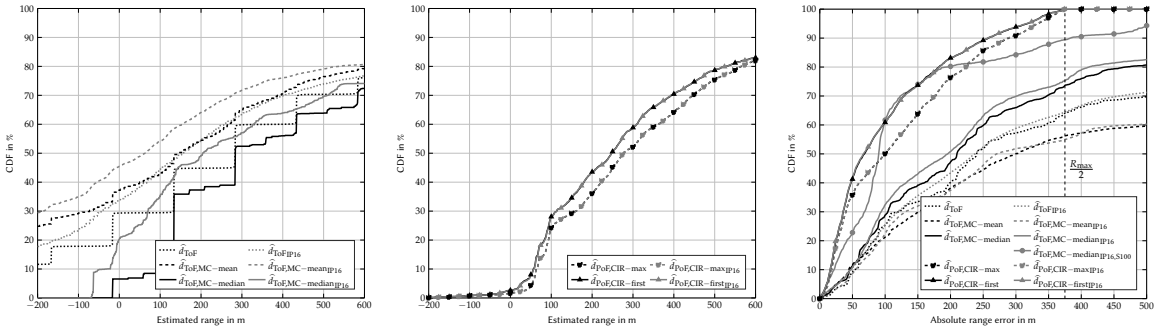


(b) *CRONEN raw PoF range estimates* $\widehat{d}_{\text{PoF,CIR}-\text{first}}$.

FIGURE 4.17 – *CRONEN raw PoF range estimates for the real outdoor scenario in Figure 4.15.*

multi-channel ToF median measurements by calculating a moving median over 100 successive estimates. Globally ToF measurements reflect the real range, however with large biases especially in the NLoS zone. Filtering over multiple successive measurements improves the ranging precision as confirmed by the CDF in Figure 4.18c, however performing a moving median over 100 measurements is equivalent to a time duration of 16 min considering a packet transmission every 10 s. This is impractical and causes large biases for nodes with even very slow mobility.

Figure 4.17 shows range estimates obtained on PoF measurements with $\widehat{d}_{\text{PoF,CIR}-\text{max}}$ and $\widehat{d}_{\text{PoF,CIR}-\text{first}}$ estimators . The PoF range ambiguity is resolved with the ground truth as ambiguity resolution is assumed a problem apart and not resolvable with ToF due to large ToF errors. Therefore Figure 4.17 indicates the PoF ranging ambiguity with respect to the ground truth ($\pm R_{\max}/2$). PoF errors distributed over the entire interval $\pm R_{\max}/2$ signify that range estimation fails as no information is obtained through phase estimates.



(a) *ToF range estimate CDFs illustrating the impact of the sampling resolution step size.*

(b) *PoF range estimate CDFs illustrating the impact of the sampling resolution step size.*

(c) *Ranging errors.*

FIGURE 4.18 – *Overall ToF and PoF ranging as well as ranging error CDFs for the measurements from Figure 4.17.*

This is the case in the NLoS zone and hence the absolute PoF ranging error is bound by $R_{\max}/2$ as illustrated in the CDFs in Figure 4.18c. Considering the LoS and urban canyon measurements, PoF ranging estimates are less noisy compared to ToF measurements. The first path detection algorithm provides more accurate range estimates compared to taking the path of strongest amplitude. Interpolation of the received signals before localization metric extraction has no impact on the resolution of PoA estimates. The range resolution step size for PoF based range estimation depends on the sampling points of the estimated Channel Impulse Response (CIR). This can be scaled by sufficient zero padding of the channel transfer function giving the necessary interpolation in the CIR so that sampling resolution step size is much smaller than the ranging resolution ΔR dependent on the virtual bandwidth.

The quantitative comparison of single- and multi-channel ToF ranging as well as PoF ranging is given by the CDFs in Figure 4.18c. PoF measurements outperform ToF ranging due to increased virtual bandwidth. Obtaining a multi-channel ToF ranging accuracy of 500 m in 80% of the cases is coherent with the simulation results from Figure 4.7 and Figure 4.13. The overall field trial performances lie in between the simulated ranging error for free-space propagation (60 m RMS) and the ETSI Tux channel (5 km RMS), considering a $E_S/N_0 = 30\,\text{dB}$. Compared to LoRa Time Difference of Arrival (TDoA) localization attaining a 200 m accuracy with 125 kHz bandwidth signals [Pod+19], the CRONEN ToF ranging is less accurate explained by the reduced bandwidth of only $B = 10\,\text{kHz}$.

In order to get detailed insight into performances, the different propagation scenarios as well as node mobility are investigated separately in the following.

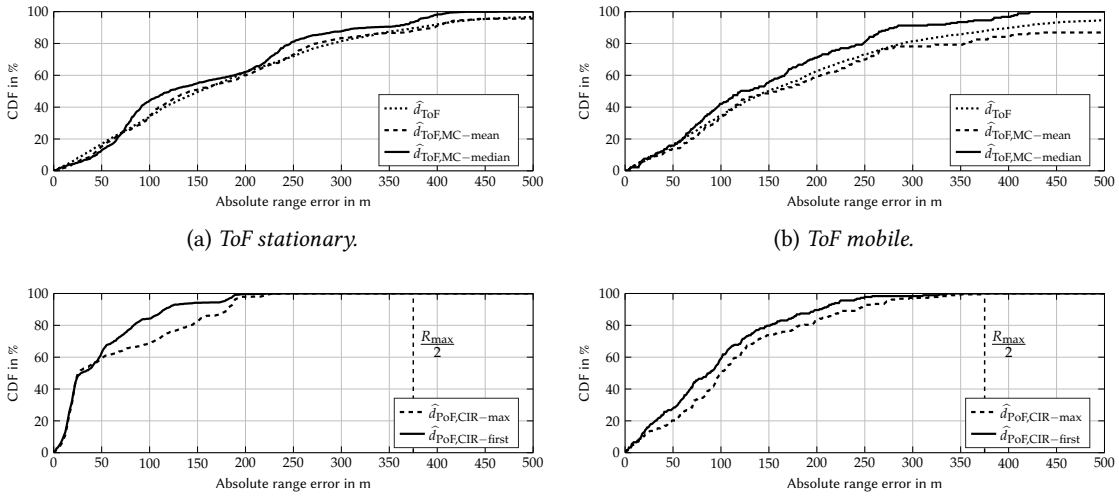
4.3.1.1 Line of Sight Scenario

The ranging measurements in the LoS propagation scenario are split into stationary measurements and measurements when the node was moving with a speed $< 36\,\text{km/h}$.

Figure 4.19 illustrates the ranging errors for ToF and PoF separated into measurements for which the node is stationary and range estimates performed during movement of the node. The CDFs are calculated on the interpolated received signals.

ToF ranging achieves approximately less than 300 m error in 90% of the cases. ToF median performances in stationary and mobile conditions are comparable. Considering the stationary ToF estimates in Figure 4.19a shows that averaging or taking the median over C single channel ToF estimates does not improve precision by a factor $\sqrt{C} = 4$ as expected theoretically. This can be explained by the fact that performances are not limited by the precision of ToF measurements but by the accuracy which is impeded by multipath induced biases. Consequently, single channel ToF measurements are statistically dependent and hence averaging does not improve the ranging error. This interpretation is supported by the slightly degraded performances of single channel and mean ToF measurements in Figure 4.19b for mobile conditions. Single measurements become more independent and hence taking the median allows improving the ranging error.

PoF measurements reveal smaller ranging errors compared to ToF estimates. In stationary conditions PoF measurements attain 100 m error in 90% of the cases. In a mobile scenario, ranging errors are almost uniformly distributed in the ranging ambiguity interval, meaning that PoF based range estimation fails due to the loss of phase coherence between sequentially obtained PoA estimates. The CDFs furthermore show improved performances of the first path detection algorithm in comparison to range estimation based on the path of strongest amplitude.



(a) *ToF stationary.* (b) *ToF mobile.*

(c) *PoF stationary.* (d) *PoF mobile.*

FIGURE 4.19 – *Field trial ranging error CDFs in the LoS scenario.*

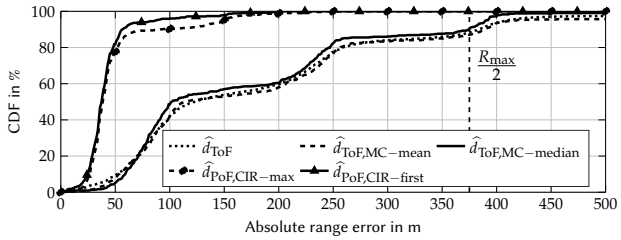


FIGURE 4.20 – *Field trial ranging error CDFs in the stationary urban canyon scenario.*

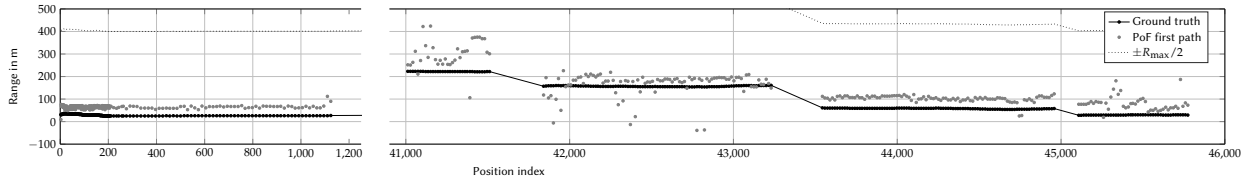


FIGURE 4.21 – *PoF range estimates in the stationary urban canyon, illustrating biases due to multipath propagation.*

4.3.1.2 Urban Canyon Scenario

Ranging error CDFs for the stationary urban canyon scenario are presented in Figure 4.20. The scenario includes ranges upto 200 m as depicted in Figure 4.21. ToF ranging achieves 400 m error in 90% of the cases. The observed step motive of 150 m corresponds to the initial sampling resolution of 1 MHz. Although interpolation reduces the step size to 9.4 m, the 150 m step size with slightly inclined steps remains due to taking the statistical median over C single channel ToF measurements (compare Figure 4.18a).

PoF ranging clearly outperforms ToF measurements by a factor 8, attaining 50 m in 90% of the estimates. The gain in accuracy is due to the significantly increased virtual bandwidth compared to the narrowband instantaneous signal bandwidth. Moreover, the 50 m accuracy corresponds to the range resolution $\Delta R = 50\,\text{m}$, which gives the limitation for the resolution of adjacent multipath components.

A zoom on PoF measurements in the urban canyon in Figure 4.21 illustrates that range estimates are biased due to multipath reflections. Measurements are very precise, i.e. 80% of the estimates lie within an interval of only 25 m. Despite this fact, ranging biases degrade accuracy and hence overall performances. The detection of a propagation situation with a ranging bias and how to process in such cases is studied in Chapter 4.3.2.

4.3.1.3 Comparison to State of the Art LPWA Ranging

Ranging performances presented in the previous sections have shown a precision improvement between ToF and PoF techniques. This is theoretically expected due to the increased bandwidth available for range estimation. It is however also interesting to compare these ranging field trials to results on LPWA localization reported in the state of the art. Although system configurations and parameterization are different, the comparison allows gathering

	SX1280	**CRONEN**
Instantaneous bandwidth B	1625 kHz	10 kHz
RMS bandwidth B_{RMS}	$\frac{B}{\sqrt{12}} = 469\,\text{kHz}$	$\sqrt{\frac{B^2+\Delta f^2(C^2-1)}{12}} = 922\,\text{kHz}$
Receiver sensitivity P_{req}	−117 dBm [Sem17b]	−123 dBm [Wol+18a]
Symbol time T_{S}	$\frac{2^m}{B} = \frac{2^{10}}{1625.00\,\text{kHz}} = 0.63\,\text{ms}$	$\frac{K_{\text{code}}}{B} = \frac{7}{10\,\text{kHz}} = 0.7\,\text{ms}$
One-way ranging duration T_{ranging}	$T_{\text{S}} K_{\text{ranging}} = 0.63\,\text{ms} \cdot 18 = 11.34\,\text{ms}$	$T_{\text{S}} C = 0.7\,\text{ms} \cdot 16 = 11.2\,\text{ms}$

TABLE 4.3 – *LPWA ranging platform configurations for SX1280 and CRONEN.*

a sense for the potential of the different positioning methods. For the following comparison, the assumption is made that ranging accuracy and precision are comparable to localization performances. This hypothesis holds, assuming that for the localization process only the best ranging estimates are selected and hence ranging and positioning precision are equivalent (see Chapter 1.5.3). Received Signal Strength Indicator (RSSI) fingerprinting based localization with both Sigfox and LoRa signals achieves about 400 m accuracy in urban scenarios [ABBW18; AK19]. Positioning with ToA based techniques and 125 kHz bandwidth LoRa signals attains averaged over different use cases and propagation environments a 200 m accuracy [Pod+19; LoR18]. Time based positioning with signals of even less bandwidth, *e.g.* Sigfox is impractical and hence no results for comparison exist.

Multi-channel PoA based positioning methods fill this gap, as they allow combining narrowband to Ultra-Narrow Band (UNB) signals for long-range low-power communication with large virtual bandwidths through signal processing for improved positioning accuracy.

The field trials presented in the previous sections attain in a real outdoor urban propagation scenario a ranging precision of about 100 m with signals of only 10 kHz instantaneous bandwidth.

While the field trials demonstrate the potential of phase based ranging, a direct simultaneous comparison to existing LPWA ranging solutions allows a fair and quantitative comparison under equal conditions. In order to achieve such a benchmarking, PoF ranging with CRONEN is compared to the ToF ranging function of the LoRa 2.4 GHz SX1280 radio chip [Sem17b].

Existing work on this chipset focuses on the hardware design and RF performances [Dog17], while ranging field trials have limited statistical sample size [Rob19] or are performed over short ranges in LoS [Sem17a] or indoor environments [Wi6]. A recent localization system based on the SX1280 chip achieves a 3 m positioning precision [Huy+19], however neither raw ranging characterization, nor detailed description of the propagation scenario are given.

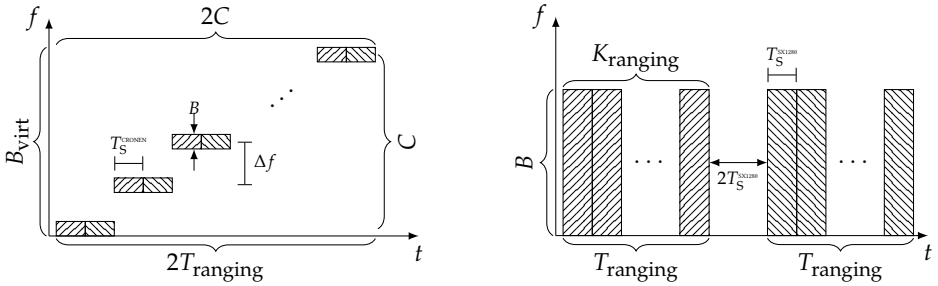
The aim of the following work is hence two-fold:

- Benchmark the SX1280 ToF ranging function in urban outdoor propagation scenarios with LPWA typical distances.
- Comparing multi-channel PoF ranging with the platform developed in this thesis, i.e. CRONEN to the state-of-the-art SX1280 ToF ranging, considering urban propagation environments and a fair comparison.

This fair comparison can be established despite the fact that the two platforms have different modulation schemes, operate in different frequency bands and have different parameters by considering the following. LPWA networks underlie energy consumption and regulation constraints. Comparing both platforms for equal transmit power and equal time on air is consequently just.

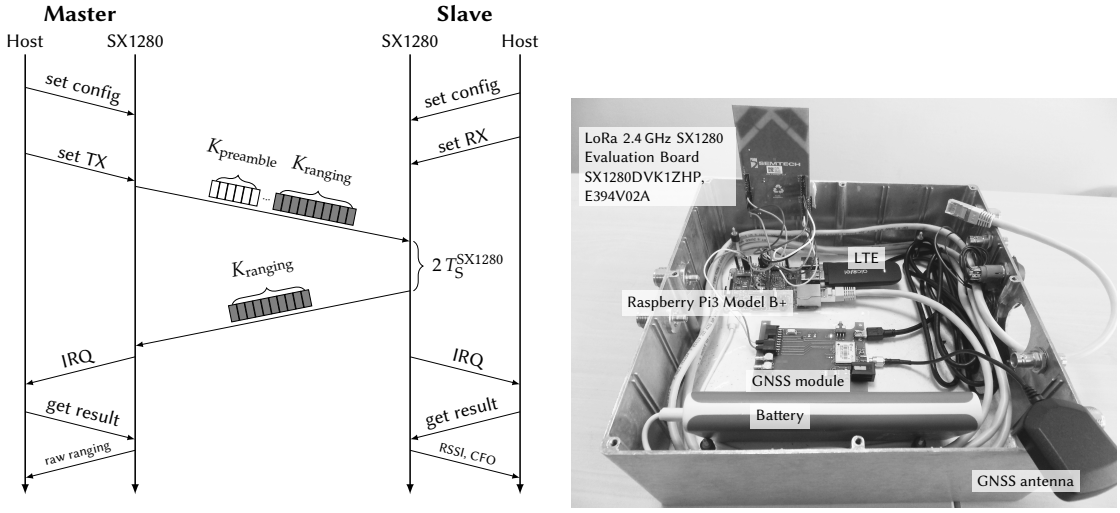
For this purpose the SX1280 chip is used with a maximum chirp bandwidth $B = 1625\,\text{kHz}$ and maximum LoRa spreading factor $m = 10$ for optimal ToA precision. The PoF multi-channel ranging platform CRONEN is used with *Config FEM*. Table 4.3 shows the respective configurations and Figure 4.22 compares their spectrum occupation. The number of LoRa ranging symbols K_{ranging} is adjusted so that the ranging signal duration corresponding to the time-on-air is equal for both platforms.

These configurations meet hence the criteria for a fair comparison. The difference in receiver sensitivity, in theory equal when considering equal symbol time, arises due to different noise figures and how sensitivity is defined. As field trials primarily aim at the characterization of ranging accuracy in scenarios sufficiently above receiver sensitivity and hence below the maximum range, this mismatch is not of concern.



(a) *CRONEN.* (b) *SX1280.*

FIGURE 4.22 – *Spectrum occupation for CRONEN and SX1280 two-way ranging protocols.*



(a) *SX1280 ToF ranging protocol.* (b) *SX1280 ranging platform based on the evaluation board [Semb].*

FIGURE 4.23 – *SX1280 ToF ranging.*

Comparing performances in the SRD 868 MHz band to those in the ISM 2.4 GHz band is critical regarding the 8.8 dB supplementary free-space path loss according to (1.1). For the following benchmarking this choice has been made in lack for commercially available LPWA two-way ranging solution in the SRD 868 MHz band. Furthermore, depending on the propagation model [Hat80] for urban scenarios, the 8.8 dB difference is no longer valid. Moreover, for antennas of physically equal antenna dimensions, the frequency dependency of the path loss vanishes and so the 8.8 dB gap.

The SX1280 chip integrated ToF ranging function operates according to the classical ping-pong two-way ToF protocol with a master initiating the exchange and a slave answering the ranging request as illustrated in Figure 4.23a. The slave performs a CFO estimation to compensate the CFO induced range bias. Figure 4.23b depicts the platform with the SX1280 comprising equally a GNSS module serving as ground truth. The platform assembly, the development of the corresponding software drivers, testing and preliminary field trials have been realized in a Master internship in support of this thesis [Le 19].

The correct implementation and configuration of the SX1280 is validated by ToF measurements in a cabled setup analog to the setup used for the AWGN channel measurements with CRONEN in Figure 4.6. Both nodes are configured to a maximum output power $P_t = 12.5$ dBm. An 80 dB attenuation is used to avoid receiver saturation in the cabled setup. Figure 4.24 shows the range error histograms for SX1280 ToF ranging. The precision configuration with high bandwidth achieves sub-meter precision conform to the application note [Sem17a]. For reduced signal bandwidth, ranging precision degrades. Bandwidth and ranging precision, i.e. the standard deviation $\sigma_{\widehat{d}}$ are inverse proportional as expected from the CRLB in (1.43).

In order to perform benchmarking under the same propagation conditions, the SX1280 slave and master platforms are installed close to the CRONEN platforms on the roof top and on the car, respectively (see Figure 4.14). Figure 4.25 depicts the raw range estimates obtained with the SX1280 ToF ranging function simultaneously to the measurement campaign from Figure 4.15 and Figure 4.17. A total of 50000 measurements corresponding to the position index are performed for the SX1280. The difference in data set size arises due to the higher measurement

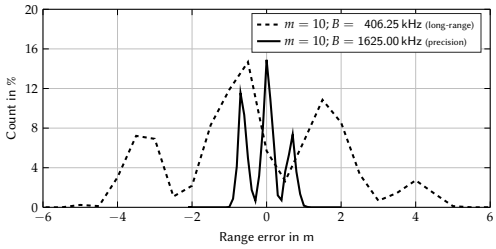
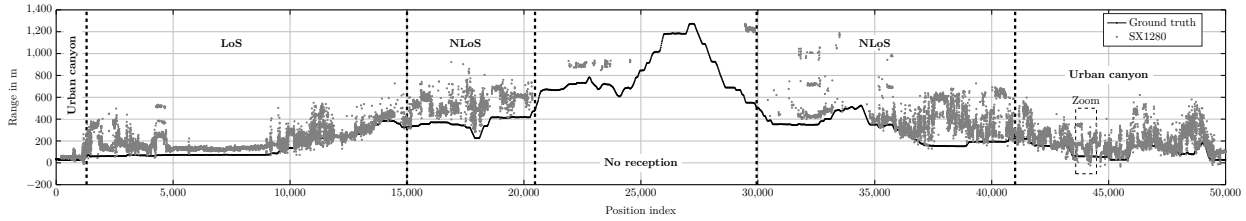


FIGURE 4.24 – *SX1280 range precision in a cabled AWGN channel for the long-range ($\sigma_{\widehat{d}} = 2.1\,\mathrm{m}$) and precision ($\sigma_{\widehat{d}} = 0.5\,\mathrm{m}$) configuration.*



(a) *ToF estimates.*

(b) *ToF estimates smoothed with a moving median over* 100 *measurements.*

FIGURE 4.25 – *SX1280 ToF range estimates for the real outdoor scenario in Figure 4.15.*

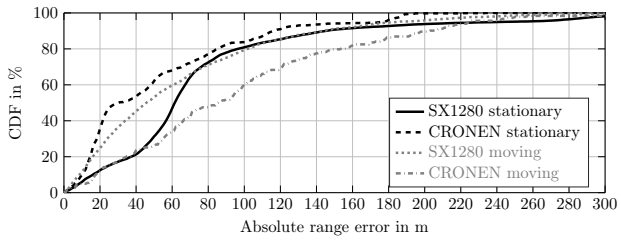


FIGURE 4.26 – *CRONEN and SX1280 range error CDFs for the LoS scenario.*

rate on the SX1280 compared to CRONEN. Figure 4.25 reveals that for position index $20500 - 30000$, corresponding to ranges larger 500 m, no range information is obtained on the SX1280. This is due to the building b_3 in Figure 4.15 blocking the LoS and adding a supplementary attenuation, so that no communication is possible.

The comparison of CRONEN PoF ranging to the SX1280 ToF ranging feature in the LoS section of the measurement series is given in Figure 4.26. The SX1280 provides valid range estimates in both moving and stationary scenarios of comparable accuracy. Considering stationary measurements only, CRONEN outperforms the SX1280 with a factor 2 in 50% of the cases. This result is in coherence with theoretical ranging precision, due to the RMS bandwidth ratio $B_{\mathrm{RMS}}^{\mathrm{CRONEN}} / B_{\mathrm{RMS}}^{\mathrm{SX1280}} \approx 2$.

Raw range estimates in the NLoS scenario are not exploitable. However, methods to detect such a NLoS scenario can be applied. An obstruction and NLoS propagation detection method [Sel14] based on the RSSI can be applied to SX1280 measurements. CRONEN offers the advantage that the available estimation of the CIR allows applying more sophisticated NLoS detection methods, i.e. based on macroscopic propagation channel characteristics. This will be studied in Chapter 4.3.2.

A zoom on raw range estimation results in the urban canyon is depicted in Figure 4.27. For the position index $43680 - 43830$, the mobile node was strictly stationary. The SX1280 range estimates alternate between two distinct values, which can be explained by small-scale fading due to dynamics in the environment causing multipath components to vary in amplitude. The SX1280 ToF based range estimation acquires either one of these two paths present in this scenario. For the position index $43965 - 44280$, the mobile node has been displaced very slowly ($\approx 1\,\mathrm{cm/s}$) and the SX1280 range measurements vary in a sweep-like manner over more than 200 m.

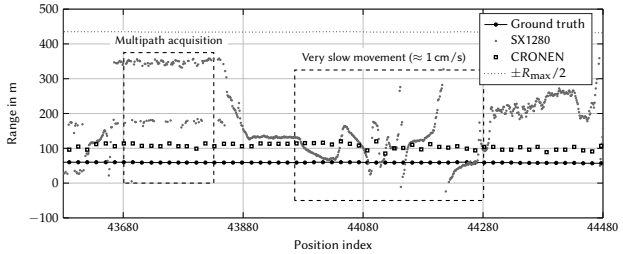


FIGURE 4.27 – *SX1280 and CRONEN raw range estimates in the urban canyon (zoom).*

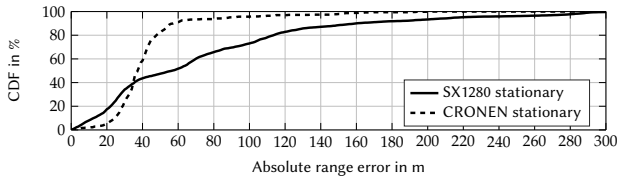


FIGURE 4.28 – *SX1280 and CRONEN range error CDFs for the stationary urban canyon scenario.*

Meanwhile CRONEN range estimates show less variability as well as a smaller bias. This sweep-like range variation can be interpreted as being the result of multipath reflections bouncing several times between the two facades of the urban canyon. Centimeter position changes provide constructive and destructive interference, so that multiple back and forth bouncing paths appear or vanish, explaining the large range variations for centimeter displacement. Figure 4.28 illustrates the CDFs in the urban canyon scenarios, showing that CRONEN outperforms the SX1280.

In this comparative study between the SX1280 radio chip and the coherent multi-channel ranging implementation for LPWA networks CRONEN, both solutions reveal to be competitive. Performances are improved compared to existing TDoA based solutions, i.e. [Pod+19]. The SX1280 provides valid range estimations in mobile scenarios with tested speeds $< 36\,\mathrm{km/h}$ while CRONEN fails. For stationary LoS and urban canyon scenarios CRONEN outperforms the SX1280 due to its increased virtual bandwidth $B_{\mathrm{virt}} = 3\,\mathrm{MHz}$. Being able to scale ranging precision independently from receiver sensitivity, i.e. coverage is a strong argument for coherent multi-channel ranging. Transposing the CRONEN concept to the ISM 2.4 GHz band offers a 80 MHz bandwidth and excellent ranging precision, while conserving low levels of receiver sensitivity through narrowband instantaneous signal bandwidths.

NLoS propagation scenarios, which do not allow obtaining valid range estimates with CRONEN will be studied in the following section.

4.3.2 Outlier Detection, Mitigation and Elimination

Strong multipath and NLoS propagation scenarios are a fundamental problem for delay based radio signal based positioning. Due to attenuation or blockage, the direct path is so weak that it is not observable and hence no unbiased range information is available in such a case. Three strategies are possible in this situation:

- Fingerprinting methods can be applied to associate the observed multipath biased information to a position. This however requires the creation of a database of geo-referenced estimates.
- Take advantage of multipath propagation. In Ultra-Wide Band (UWB) systems multipath components are sufficiently resolved to identify and separate them, which allows their tracking [URGW16; MDDU17]. With the help of geometric information about the environment, multipath information contributes to the positioning process [Mei14]. In millimeter wave systems where the propagation channel is rather sparse [Zha+19], techniques of Simultaneous Localization and Mapping (SLAM) allow determining position and environment geometry in a joint process [GGD14; Koi+20].
- Exclude multipath and NLoS biased estimates. Considering a scenario of a node to be localized in a network, multiple base stations are required *e.g.* for trilateration. Sufficient redundancy of base stations allows excluding those links that are biased [BKLL17], *e.g.* based on the standard deviation of successive observations [KNT00] or the Kurtosis calculated on the CIR [ZSL13]. For this purpose, the different single link estimates are weighted according to the quality of the estimate. In GNSS, the set of satellites used for calculating the positioning solution can be selected as function of *e.g.* SNR, elevation, to guarantee clear sky visibility in an urban canyon, or the resulting Geometric Dilution of Precision (GDOP) [Inn+16; SDR16].

Coherent multi-channel ranging, applied to LPWA networks, provides increased bandwidth and hence the possibility to extract metrics related to the quality of range estimates. However, considering the maximum available

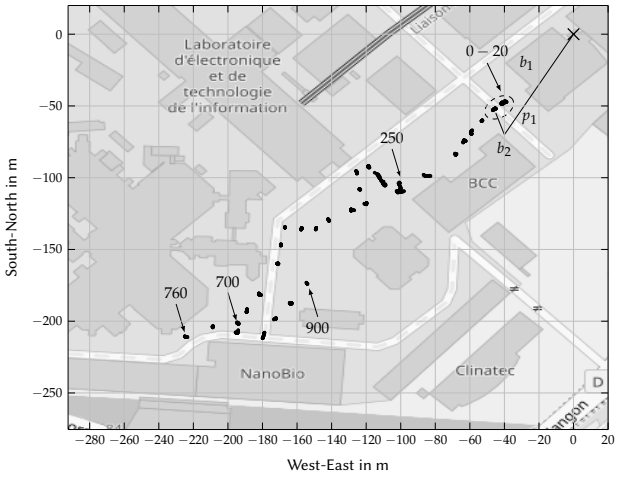


FIGURE 4.29 – *GNSS ground truth positions (•) with respect to the roof testbed (×) at* $(0, 0)$.

bandwidth of 7 MHz in the SRD 868 MHz band or 80 MHz in the ISM 2.4 GHz band, multipath components are not sufficiently resolved to apply geometric approaches as possible in UWB positioning. Therefore, the following study focuses on the third option, i.e. outlier detection and mitigation as fingerprinting techniques go beyond the framework of parametric estimation due to the required databases.

Based on the available estimation of the CIR, macroscopic propagation channel characteristics from Chapter 2.3.3 can be calculated and used to detect strong multipath or NLoS propagation. These macroscopic metrics applied to UWB CIR estimates allow classification into LoS and NLoS scenarios [MGWW10]. Extensive measurement campaigns [JYL01] reveal that delay spread σ_τ and ranging biases are related. Maximum Likelihood (ML) based ToA estimation with insufficient bandwidth to resolve each multipath component acquires a ToA estimate corresponding to the first path plus the mean excess delay $\widehat{t_\mathrm{A}} = \tau_0 + \overline{\tau}_e$. Measurement campaigns in [JYL01] empirically determined a proportionality between the mean excess delay $\overline{\tau}_e$ and the delay spread σ_τ that can be used for range bias mitigation

$$\begin{aligned}\widehat{d}_{\mathrm{PoF,CIR-calib}} &= c_0 \left(\widehat{t_\mathrm{A}} - \psi_\tau \widehat{\sigma_\tau}\right) \\ &= c_0 \left(\tau_0 + \overline{\tau}_e - \psi_\tau \widehat{\sigma_\tau}\right) \approx c_0 \tau_0,\end{aligned} \tag{4.11}$$

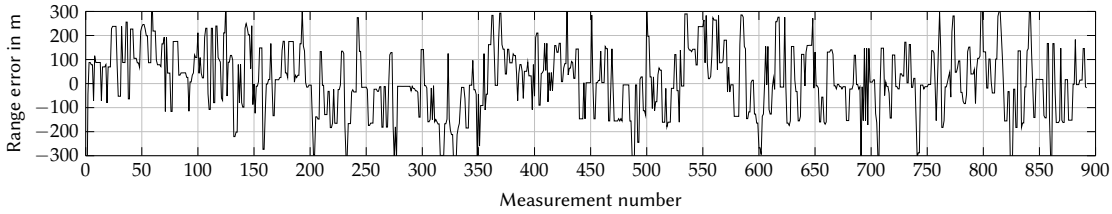
with proportionality factor ψ_τ.

In the scenario depicted in Figure 4.29, ranges up to $d_\mathrm{max} = 300\,\mathrm{m}$ are covered and empirically 90% of the mobile ground testbed positions have LoS conditions to the roof testbed. The radius of the first Fresnel zone $R_{\mathrm{Fresnel},1} = \sqrt{c_0 R/(4 f_\mathrm{w})} \approx 5\,\mathrm{m}$ is only obstructed by trees on some positions. A total of 900 measurements has been performed with *Config Long* from Table 4.2.

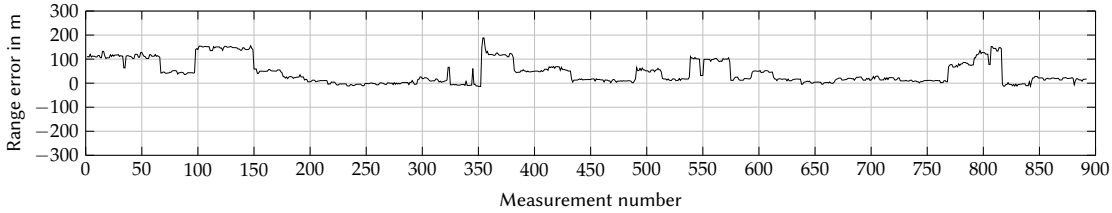
The comparison of performances in the following section to those previously obtained is difficult, due to a different configuration of the transceiver testbeds and due to a different propagation scenario. In order to illustrate the performances of the outlier detection and mitigation techniques presented in the following, they are compared to range estimates obtained by the previously studied ToF and PoF methods. Although repetitive, this approach allows confirming previous conclusions and clearly sets the framework for outlier detection and mitigation techniques. Figure 4.30 shows the ToF and PoF range estimation errors for this setup. A three sample moving median is applied to both estimates in order to exclude outliers due to interference that is not inherently detected by the testbed and processing. Phase based estimates reveal a higher precision compared to time based ranging, due to the improved temporal resolution through increased bandwidth. The CDFs in Figure 4.31 show ranging errors for raw, i.e. estimates without the application of a moving median and smoothed estimates for both ToF and PoF. Statistical processing of the C single channel ToF estimates allows improving precision to the previously reported $\approx 250\,\mathrm{m}$ in 90% of the cases. However, the main precision gain is achieved with PoF measurements attaining $\approx 150\,\mathrm{m}$ in 90% of the measurements.

Figure 4.30b also shows that although PoF measurements are very precise, different biases are observed and estimates are not accurate. Comparing these to the ground truth range in Figure 4.32, reveals that the biases are mostly position related.

For the measurements $1 - 150$, a bias is observed corresponding most likely to a multipath reflection p_1 via the building b_2, stronger than the direct path obstructed by the edge of building b_1 in Figure 4.29. More insight into this situation is provided by Figure 4.33 illustrating the estimated CIRs for a biased and an unbiased range estimate.



(a) *Moving median smoothed* $\widehat{d}_{\mathrm{ToF,MC-median}_{S3}}$ *ranging error.*



(b) *Moving median smoothed* $\widehat{d}_{\mathrm{PoF,CIR-max}_{S3}}$ *ranging error.*

FIGURE 4.30 – *Field trial ToF and PoF ranging errors for the* 900 *measurements.*

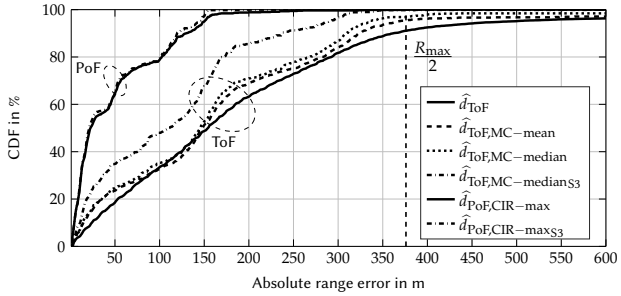


FIGURE 4.31 – *Ranging errors for field trial ToF and PoF estimation comprising NLoS biases.*

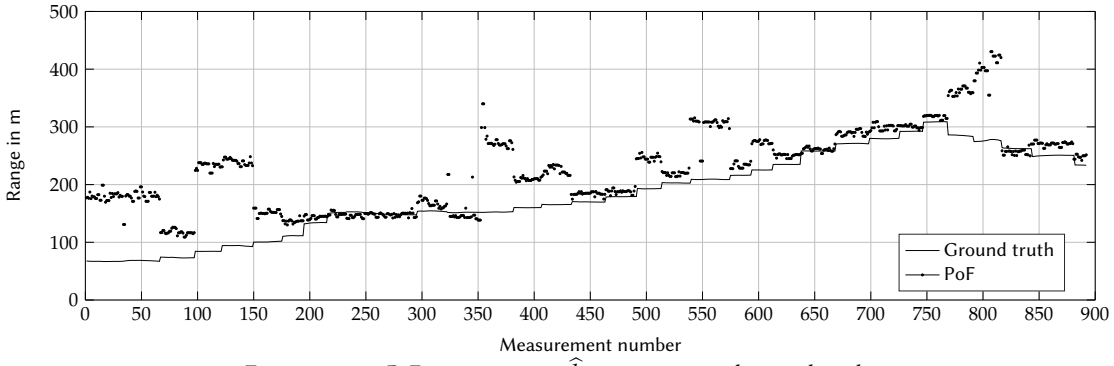


FIGURE 4.32 – *PoF measurements* $\widehat{d}_{\mathrm{PoF,CIR-max}}$ *and ground truth.*

While the unbiased CIR has a main lobe of width corresponding to the range resolution ΔR, the biased CIR has a large delay spread σ_τ. Figure 4.34 illustrates the CIRs for all 900 measurements. The ranging error i.e. the biases in Figure 4.30b can be compared to the delay spread σ_τ calculated for each estimated CIR according to (2.29) given in Figure 4.35. It can be stated, that biases correlate with larger delay spreads.

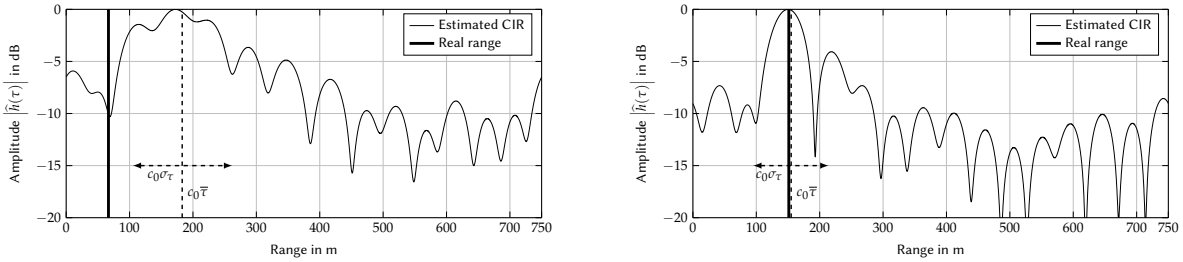
Range estimates with NLoS mitigation according to (4.11) are given in Figure 4.36. A minimum error is achieved for $\psi_\tau = 0.7$. The factor ψ_τ is chosen to minimize the error in 90% of the cases. These results are confirmed by the findings in extensive channel characterization campaigns where $\psi_\tau = [1 \ldots 0.5]$ in the suburban configuration [JYL01].

Biased estimates can be detected by calculating the delay spread and comparing it to a threshold ζ_{opt}

$$\text{Unbiased,} \quad \text{if} \quad \sigma_\tau < \zeta_{\mathrm{opt}}, \tag{4.12a}$$

$$\text{Biased,} \quad \text{if} \quad \sigma_\tau \geq \zeta_{\mathrm{opt}}. \tag{4.12b}$$

Determining this threshold ζ_{opt} is propagation scenario dependent and needs also adjustment to the range resolution ΔR defining the minimum delay spread due to the main lobe in the CIR.



(a) *CIR* $\widehat{h}(\tau)$ *of measurement* 20 *(range bias).* (b) *CIR* $\widehat{h}(\tau)$ *of measurement* 250 *(range bias free).*

FIGURE 4.33 – *Comparison of estimated CIRs* $\widehat{h}(\tau)$.

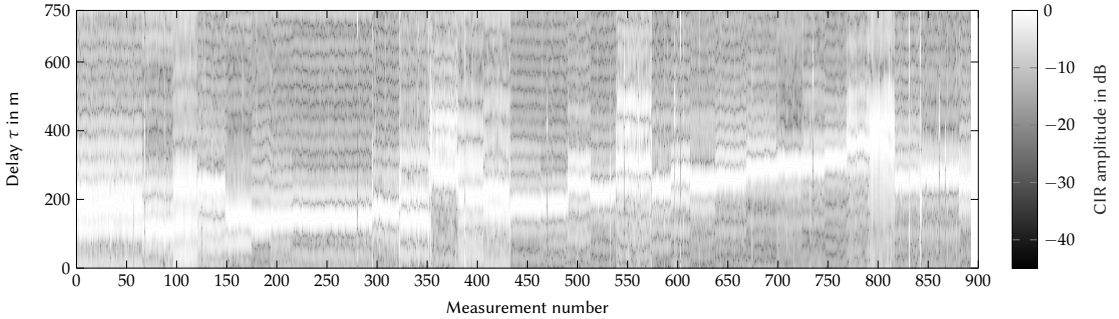


FIGURE 4.34 – *All CIRs as image.*

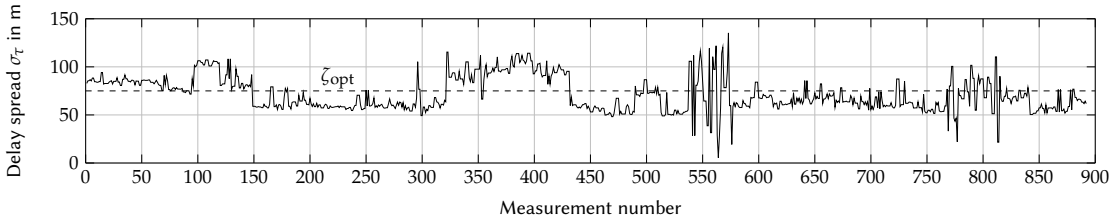


FIGURE 4.35 – *Estimated delay spread* σ_τ *of smoothed PoF measurements from Figure 4.30b.*

Figure 4.37 shows the delay spread histograms for the sets of bias free and biased classified measurements. The sets are generated depending on whether PoF errors exceed or not 30 m. Biased estimates can be detected and removed by considering only estimates for which $\sigma_\tau < \zeta_{\text{opt}} \approx 75\,\text{m}$. This corresponds to retaining 62% of all measurements, a missed bias detection of 22% and a 21% false alarm rate. The minimum delay spread of $\approx 50\,\text{m}$ is explained by the range resolution $\Delta R = 50\,\text{m}$.

Figure 4.38 depicts the first path detection with $R_{\text{first}} = 300\,\text{m}$ and $\gamma_{\text{first}} = -7\,\text{dB}$. The parameters R_{first} and γ_{first} are obtained through minimization of the error in 90% of the cases. Measurements classified as range bias free according to (4.12) are marked bold. Comparing Figure 4.30b and Figure 4.38, first path detection reduces biases *e.g.* for the measurements $100 - 150$ and $540 - 570$, while NLoS classification allows eliminating measurements that cannot be corrected, *e.g.* $1 - 150$ or $350 - 400$.

The CDFs in Figure 4.39 give a quantitative comparison of the different NLoS mitigation and classification methods. Maximum amplitude based PoF ranging achieves 120 m in 90% of the cases. Correcting range biases by subtracting a distance statistically proportional to the delay spread, improves to 70 m in 90% of the measurements. This correction is based on the empirically determined and over large measurement campaigns averaged proportionality factor ψ_τ. Consequently, the factor ψ_τ is not optimal for a specific, single measurement. For this reasons, searching the first path in the CIR achieves best performances with a ranging error less than 50 m in 90% of the cases. All methods combined with an outlier exclusion further improve precision, due to the elimination of non-corrected and hence still biased range estimates.

Combining first path detection to mitigate ranging biases in moderate multipath combined with classification to eliminate NLoS biased estimates, outperforms the other investigated methods. This optimal method achieves an error of 30 m or less in 90% of the cases, while conserving 62% of the ranging measurements.

The technique of multi-channel ranging applied to LPWA networks and its combination with CIR based outlier detection and mitigation techniques allows improving ranging accuracy. Furthermore, it provides a ranging estimate quality indicator that can be used to properly weight range estimates in the positioning process. A patent application for the association of these methods has been filed [WdDC19b].

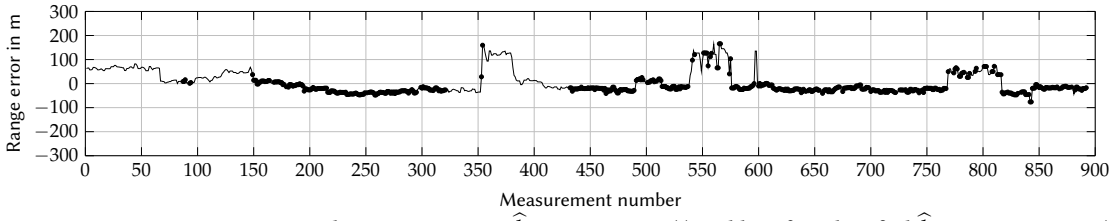


FIGURE 4.36 – *Range estimation with NLoS mitigation $\widehat{d}_{\text{PoF,CIR}-\text{calib}\,S3}$ (-) and bias free classified $\widehat{d}_{\text{PoF,CIR}-\text{calib}\,S3,BR}$ (·).*

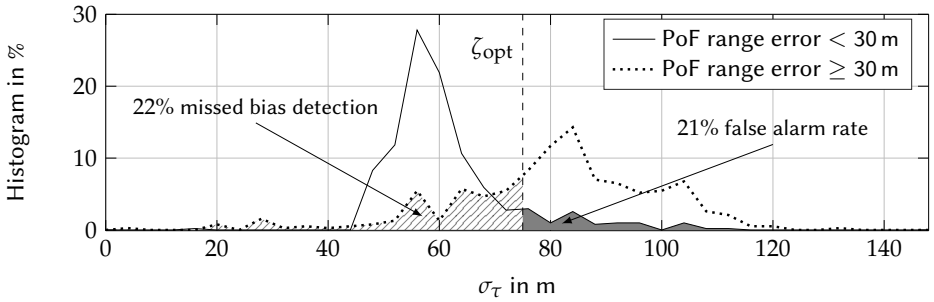


FIGURE 4.37 – *Delay spread histograms for biased PoF ranging estimates $\widehat{d}_{\text{PoF,CIR}-\text{first}\,S3}$ detection.*

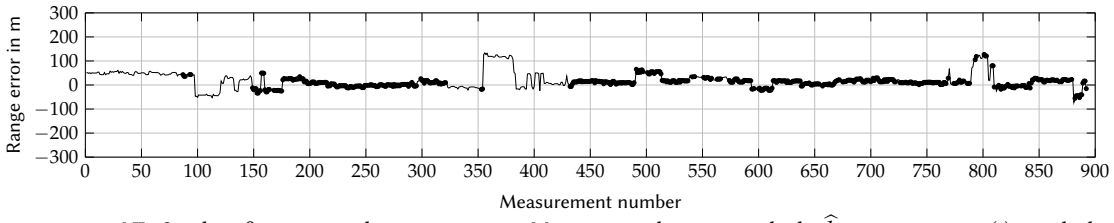


FIGURE 4.38 – *NLoS classification and mitigation: Moving median smoothed $\widehat{d}_{\text{PoF,CIR}-\text{first}\,S3}$ (-) and bias free classified $\widehat{d}_{\text{PoF,CIR}-\text{first}\,S3,BR}$ (·).*

4.4 Conclusion and Perspectives

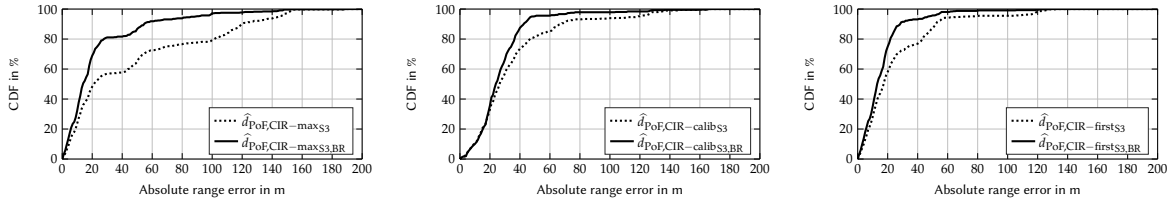
A SDR based multi-channel ranging platform, called CRONEN has been implemented and tested. The testbed performs IQ sample data transmission and reception in the SRD 868 MHz band according to the timeslot two-way multi-channel ranging protocol. The transceiver chipset has an independent local oscillator for each, transmit and receive branch. For this reason and in order to reduce the bandwidth of IQ data for post processing, a numerical IF mixing stage has been implemented. This allows maintaining phase coherence between transmit and receive branch over multiple channels as required for multi-channel ranging.

The working hypotheses assumed for deriving the signal model have been validated by comparison of simulation results with measurements obtained in a cabled AWGN channel. Multi-channel ranging achieves errors below 10 m in 90% of the cases in an AWGN channel with 10 kHz narrowband Binary Phase Shift Keying (BPSK) signals, a total ranging protocol duration of 819.2 ms and typical low-cost oscillators with a ± 0.5 ppm frequency stability.

Simulation results reveal that multi-channel ranging significantly degrades in multipath propagation channels. In the ETSI Tux channel, a 100 m RMS ranging error is obtained by simulation.

Outdoor field trials in a semi-urban industrial office building site, reveal that in LoS condition, PoF clearly outperforms ToF with an error less than 125 m and 350 m in 90% of the cases, respectively. PoF estimates are much more precise than ToF measurements, while accuracy in both depends on the availability of a detectable first path. ToF measurements need to be averaged over more than 100 measurements to achieve a level of precision comparable to a single PoF measurement. Despite the outstanding performances of the PoF approach, it does neither work in moving scenarios nor in NLoS scenarios where phase on different channels becomes totally random and does not allow range estimation.

Having demonstrated the improved ranging precision of multi-channel ranging with LPWA typical narrowband signals, a comparison with existing LPWA ranging solutions is established. The comparison is conducted between CRONEN developed in this thesis and the SX1280 ToF ranging function. Both solutions are compared based on equal transmit power and equal time on air for a fair comparison of ranging performances with respect to energy consumption and duty cycle restrictions. Multi-channel ranging offers a virtual bandwidth for high ranging precision which is scalable independent from the narrowband instantaneous bandwidth required for long-range



(a) *Maximum amplitude detection* $\widehat{d}_{\mathrm{PoF,CIR-max}}$. (b) *Delay spread based bias mitigation* $\widehat{d}_{\mathrm{PoF,CIR-calib}}$ *[JYL01].* (c) *First path detection* $\widehat{d}_{\mathrm{PoF,CIR-first}}$.

FIGURE 4.39 – *PoF ranging error CDFs for different outlier detection, exclusion or mitigation methods.*

transmissions. The comparison in outdoor field trials shows that CRONEN provides improved ranging performances compared to SX1280. This is explained by the increased RMS bandwidth of CRONEN compared to the fixed bandwidth of the SX1280.

Moreover, all field trials have shown that multipath heavily impedes ranging accuracy although precision can be improved by PoF ranging. Strong multipath or NLoS propagation do physically not allow estimating the direct path. In response to this problematic, a delay spread based outlier detection and elimination scheme has been investigated. The measured CIR obtained through multi-channel ranging, allows estimating the delay spread. Range measurements obtain an error less than 30 m in 90% of the case in outdoor field trials when detecting and eliminating biased measurements, which correlate with large delay spreads. This scheme helps a location solver to reject those range measurements that are biased in order to perform precise positioning.

Supplementary simulations with different channel models will complete the study in this chapter. Based on these simulations, more suited ranging algorithms for multipath propagation can be designed. The study can equally be conducted with the transceiver testbed and a channel emulator. This allows working with real hardware and multipath propagation, but allows controlling the radio channel. More field trial measurement campaigns will complete, confirm and refine the findings provided in this chapter.

Combining multi-channel ranging for improved temporal resolution and applying beamforming techniques to reduce multipath biases is a promissing perspective to be pursued [Lu07].

Bibliography of Chapter 4

[ABBW18] M. Aernouts, B. Bellekens, R. Berkvens, and M. Weyn. "A Comparison of Signal Strength Localization Methods with Sigfox". In: *2018 15th Workshop on Positioning, Navigation and Communications (WPNC)*. 2018, pp. 1–6.

[AK19] G. G. Anagnostopoulos and A. Kalousis. "A Reproducible Comparison of RSSI Fingerprinting Localization Methods Using LoRaWAN". In: *16th Workshop on Positioning, Navigation and Communications (WPNC)*. 2019.

[Ana13] Analog Devices. *RF Agile Transceiver AD9361*. http://www.analog.com/media/en/technical-documentation/data-sheets/AD9361.pdf. 2013.

[BKLL17] W. Bakkali, M. Kieffer, M. Lalam, and T. Lestable. "Kalman Filter-Based Localization for Internet of Things LoRaWAN™ End Points". In: *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*. 2017, pp. 1–6.

[CEP18] CEPT. *ERC Recommendation 70-03*. Aug. 2018.

[Cro17] CrowdSupply. *LimeSDR: Flexible, Next-generation, Open Source Software Defined Radio*. https://www.crowdsupply.com/lime-micro/limesdr. 2017.

[Dio+19] C. Diouf et al. "A 400 Msps SDR platform for prototyping accurate wideband ranging techniques". In: *16th Workshop on Positioning, Navigation and Communications (WPNC)*. 2019.

[Dog17] M. Dogotari. "Hardware Design and RF Performance Evaluation of a Long Range 2.4 GHz Radio Module". MA thesis. 2017.

[ETS10] ETSI. *Universal Mobile Telecommunications System (UMTS); Deployment aspects (3GPP TR 25.943 version 9.0.0 Release 9)*. European Telecommunications Standards Institute (ETSI), 2010.

[Ett] Ettus Research - A National Instruments Brand. *USRP Bus Series*. https://www.ettus.com/product-categories/usrp-bus-series/. Accessed: 2020/07/31.

[Gre] Great Scott Gadgets. *HackRF One*. https://greatscottgadgets.com/hackrf/one/. Accessed: 2020/07/31.

[GGD14] F. Guidi, A. Guerra, and D. Dardari. "Millimeter-Wave Massive Arrays for Indoor SLAM". In: *2014 IEEE International Conference on Communications Workshops (ICC)*. 2014, pp. 114–120.

[Hat80] M. Hata. "Empirical Formula for Propagation Loss in Land Mobile Radio Services". In: *IEEE Transactions on Vehicular Technology* 29.3 (1980), pp. 317–325.

[Huy+19] K. Huy et al. "iLoc: A Low-Cost Low-Power Outdoor Localization System for Internet of Things". In: *GlobeCom 2019*. 2019.

[Inn+16] A. Innac et al. "Reliability testing for multiple GNSS measurement outlier detection". In: *2016 European Navigation Conference (ENC)*. 2016, pp. 1–8.

[JYL01] Y. Jeong, H. You, and C. Lee. "Calibration of NLOS Error for Positioning Systems". In: *IEEE VTS 53rd Vehicular Technology Conference, Spring 2001. Proceedings (Cat. No.01CH37202)*. Vol. 4. 2001, 2605–2608 vol.4.

[KNT00] E. M. Knorr, R. T. Ng, and V. Tucakov. "Distance-based outliers: algorithms and applications". In: *The VLDB Journal* 8.3 (2000), pp. 237–253. URL: https://doi.org/10.1007/s007780050006.

[Koi+20] R. Koirala et al. "Simultaneous Localization and Mapping in Millimeter Wave Networks with Angle Measurements". In: *submitted to IEEE ICC, Dublin*. 2020.

[Le 19] K. Le Déroff. "Conception d'une Architecture de Test et Analyse Comparative de Systèmes de Mesures de Distance par Ondes Radio Bande Étroite". MA thesis. Université de Savoie Mont-Blanc and CEA-Leti Grenoble, 2019.

[LoR18] LoRaAlliance. *Geolocation Whitepaper*. https://lora-alliance.org/resource-hub/lora-alliance-geolocation-whitepaper. Accessed: 2020/07/31. 2018.

[Lu07] D. Lu. "Multipath Mitigation in TOA Estimation Based on AOA". PhD thesis. Department of Electrical and Computer Engineering, Calgary, Alberta, 2007.

[MDDU17] J. Maceraudi, F. Dehmas, B. Denis, and B. Uguen. "Multipath-Aided Direct Path ToA Reconstruction for Integrated UWB Receivers in Generalized NLoS". In: *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)*. 2017, pp. 1–5.

[MGWW10] S. Marano, W. M. Gifford, H. Wymeersch, and M. Z. Win. "NLOS Identification and Mitigation for Localization based on UWB Experimental Data". In: *IEEE Journal on Selected Areas in Communications* 28.7 (2010), pp. 1026–1035.

[Mei14] P. Meissner. "Multipath-Assisted Indoor Positioning". PhD thesis. Graz University of Technology, 2014.

[Myr] Myriad RF. *LimeSDR USB*. https://myriadrf.org/projects/component/limesdr/. Accessed: 2020/07/31.

[Pan17] Panasonic. *microSD/SDHC Memory Card, Consumer Plus pSLC Model - RP-SMPE32DA1*. 2017.

[Pod+19] N. Podevijn et al. "Experimental TDoA Localisation in Real Public LoRa Networks". In: *2019 International Conference on Indoor Positioning and Indoor Navigation (IPIN)*. 2019.

[Rak17] Rakon. *Single chip oscillator RPT7050A*. 2017.

[Rob19] S. Robinson. *Semtech SX1280 2.4GHz LoRa Ranging Tranceivers*. https://github.com/LoRaTracker/SX1280_Testing. Accessed: 2020/07/31. 2019.

[SDR16] C. R. Sekhar, V. S. I. Dutt, and G. S. Rao. "GDoP estimation using Simulated Annealing for GPS and IRNSS combined constellation". In: *Engineering Science and Technology, an International Journal* 19.4 (2016), pp. 1881 –1886. URL: http://www.sciencedirect.com/science/article/pii/S221509861630739X.

[Sel14] O. Seller. "Ranging and Positioning System". Pat. 2 767 847. 2014.

[Semb] Semtech. *SX1280DVK1ZHP Development Kit for the SX1280 and SX1281 Transceivers*. https://www.semtech.com/products/wireless-rf/24-ghz-transceivers/sx1280. Accessed: 2020/07/31.

[Sem17a] Semtech. *Application Note: An Introduction to Ranging with the SX1280 Transceiver*. 2017.

[Sem17b] Semtech. *SX1280/SX1281 Long Range, Low Power, 2.4 GHz Transceiver with Ranging Capability*. 2017.

[Sky18] Skyworks. *SKY66423-11: 860 to 930 MHz RF Front-End Module*. 2018.

[Tai17] Taitien. *3.2 x 2.5 mm SMD Voltage Controlled Temperature Compensated Crystal Oscillator (VCTCXO) - TX Type*. 2017.

[Ubl] Ublox. *High precision GNSS performance for the mass market: NEO-M8P series*. https://www.u-blox.com/en/product/neo-m8p-series. Accessed: 2020/07/31.

[URGW16] M. Ulmschneider, R. Raulefs, C. Gentner, and M. Walter. "Multipath Assisted Positioning in Vehicular Applications". In: *2016 13th Workshop on Positioning, Navigation and Communications (WPNC)*. 2016, pp. 1–6.

[Wi6] Wi6Labs. *Iot And Geo-Tracking : The Feedback Of A French Start-Up From Bretagne*. http://www.wi6labs.com/2018/08/02/iot-et-geolocalisation-le-retour-dexperience-dune-startup-bretonne/. Accessed: 2020/07/31.

[WdDC19a] F. Wolf, S. de Rivaz, F. Dehmas, and J. P. Cances. "Field Trials on Accurate Multi-Channel Ranging for Narrowband LPWAN". In: 2019, pp. 1–6.

[Wol+18a] F. Wolf et al. "Coherent Multi-Channel Ranging for Narrowband LPWAN: Simulation and Experimentation Results". In: *15th Workshop on Positioning, Navigation and Communications (WPNC)*. 2018, pp. 1–6.

[WdDC19b] F. Wolf, S. de Rivaz, F. Dehmas, and J.-P. Cances. "Méthode d'Estimation de Distance dans un Réseau LPWA et Méthode d'Estimation de Position Associée". FR. Pat. Application N° 1910165. 2019.

[Xil15] Xilinx. *Zynq-7000 All Programmable SoC (Z-7030, Z-7035, Z-7045, and Z-7100): DC and AC Switching Characteristics*. https://www.xilinx.com/support/documentation/data_sheets/ds191-XC7Z030-XC7Z045-data-sheet.pdf. 2015.

[Zha+19] G. Zhang et al. "Millimeter-Wave Channel Characterization in Large Hall Scenario at the 10 and 28 GHz Bands". In: *2019 13th European Conference on Antennas and Propagation (EuCAP)*. 2019, pp. 1–4.

[ZSL13] J. Zhang, J. Salmi, and E. Lohan. "Analysis of Kurtosis-Based LOS/NLOS Identification Using Indoor MIMO Channel Measurement". In: *IEEE Transactions on Vehicular Technology* 62.6 (2013), pp. 2871–2874.

5

Advanced Range Estimation Algorithms

„Wenn Sie diese Frage ... erledigten, könnten Sie sich des höchsten Interesses aller Physiker sicher sein."

– Heinrich Rudolf Hertz (1857 – 1894)

Chapter contents

Precise Low Power Wide Area (LPWA) network positioning can be achieved with multi-channel ranging. However, multipath propagation encountered in real outdoor scenarios significantly degrades localization performances. Instead of rejecting biased measurements as studied in the previous chapter, advanced ranging algorithms will be investigated.

5.1 Comparison of Multi-Channel Ranging Algorithms

Multi-channel ranging provides a sampled estimate of the channel transfer function as given by (3.86). For delay estimation it is hence natural to convert the channel transfer function measurement to the Channel Impulse Response (CIR) in time domain to estimate the delay of the first path (see Chapter 3.4.2.3). This straightforward phase based approach achieves a significant improvement in ranging precision with narrowband LPWA signals compared to classical time based techniques. Simulations with multipath propagation models and outdoor field trials have shown that the radio channel mainly limits performances. Ranging precision degrades due to close multipath components which cannot be resolved due to overlapping main lobes in the Inverse Discrete Fourier Transform (IDFT). It is hence interesting to study advanced ranging algorithms such as high-resolution algorithms or learning based methods, and their application to multi-channel ranging.

The following comparative study is the result of a joint work [Wol+19b] in cooperation with a PhD student specialized in the field of machine learning.

Precise and accurate delay estimation in multipath propagation channels requires sufficient range resolution in order to separate adjacent multipath components. The field trials presented in Chapter 4.3 are performed with a virtual bandwidth $B_{\text{virt}} = 3\,\text{MHz}$, equivalent to a range resolution $\Delta R = 50\,\text{m}$. The obtained ranging errors correspond to this range resolution. Increasing the virtual bandwidth to the maximum of 7 MHz allowed in the SRD 868 MHz band will improve range resolution to $\Delta R \approx 22\,\text{m}$. In applications, where meter-level precision is required, this range resolution is insufficient. High resolution algorithms, when applied to the range estimation problem, aim at separating different multipath components closer than the initial range resolution [AMB18; CFT07]. In the ideal case, free-space propagation performances can be achieved. The Multiple Signal Classification (MUSIC) algorithm [Sch86] widely used for Angle of Arrival (AoA) estimation problems [GM99; dM06; TVVH16; PMCM15] can be adapted to multi-channel delay i.e. range estimation [KOL15; LPCY06; ZYLS06; Sun+17; LF14]. Its application to multi-channel ranging for LPWA networks will be studied in the following.

While MUSIC belongs to the family of parametric estimators, learning based signal processing methods potentially offer an alternative approach, in case parametric estimators cannot be found or signal models are absent, but data is available.

Machine learning has various applications in the domain of wireless communications [MHH18; Luo+19]. Learning based algorithms can be classified according to [BLJ13] into:

- **Supervised Learning**: In the learning phase, labeled data is used to train the algorithm in order to produce the wanted output on a given input. For this purpose, an expert database is required. Typical approaches are based on regression methods, *e.g.* for prediction applications. In the context of positioning, localization metrics such as Received Signal Strength Indicator (RSSI), AoA, Time of Arrival (ToA), Phase of Arrival (PoA) can be used to construct an expert database which is labeled with the ground truth position or range. The training of a learning algorithm allows finding the best matching estimator taking *e.g.* multipath propagation into account [IRM15; AB17].
- **Unsupervised Learning**: Labels are not available and hence no expert database can be constructed. Unsupervised learning methods mainly aim at solving clustering problems. Localization metrics can *e.g.* be classified into sets belonging to different positions or to different propagation conditions, *e.g.* Line of Sight (LoS) or None Line of Sight (NLoS) [MGWW10].
- **Reinforcement Learning**: Reinforcement based learning algorithms perform actions and are rewarded or punished according to the output of their action in order to learn the correct actions to take [SB+98]. In wireless positioning, reinforcement learning is used *e.g.* in tracking algorithms [Yan+19] or to ensure robust localization [CZBL19].

Learning algorithms have been applied to positioning problems in various contexts [Mal+19; AK19]. Range estimation based on CIR measurements is realized with a Deep Neural Network (DNN) [Nii+19] or with a Convolutional Neural Network (CNN) based on "Wireless Fidelity" (WiFi) ToA measurements [BGL18].

Applying supervised learning based algorithms to range estimation based on multi-channel estimates potentially allows finding the best suitable model, i.e. taking advantage of hidden features in the channel transfer function, which are difficult to determine with parametric models due to the complexity of real propagation channel.

The following study compares the IDFT baseline solution (see Chapter 3.4.2.3) to MUSIC adapted to multi-channel ranging and DNN based range estimation.

5.1.1 Working Assumptions and Signal Model

Noise free one-way channel estimations from the multi-channel ranging protocol are given based on (3.40) and (3.44) by

$$\widehat{H}_{\mathrm{PoA}_c}^{[T_1,R_2]} = \widehat{\alpha_c}^{[T_1,R_2]}\, e^{j\,\widehat{\phi_{\mathrm{A}c}}^{[T_1,R_2]}} = \underbrace{A_c^{[T_1,R_2]}\, e^{-j\,2\pi(f_\mathrm{w}+f_c)\tau_0}}_{H_c^{[T_1,R_2]}}\, e^{j\left(-2\pi f_c t_0+\phi_\mathrm{R}^{T_1}-\phi_\mathrm{R}^{R_2}\right)}, \tag{5.1a}$$

$$\widehat{H}_{\mathrm{PoA}_c}^{[T_2,R_1]} = \widehat{\alpha_c}^{[T_2,R_1]}\, e^{j\,\widehat{\phi_{\mathrm{A}c}}^{[T_2,R_1]}} = \underbrace{A_c^{[T_2,R_1]}\, e^{-j\,2\pi(f_\mathrm{w}+f_c)\tau_0}}_{H_c^{[T_2,R_1]}}\, e^{j\left(+2\pi f_c t_0+\phi_\mathrm{R}^{T_2}-\phi_\mathrm{R}^{R_1}\right)}, \tag{5.1b}$$

assuming no frequency offset, i.e. $\delta_f = 0$. This hypothesis simplifies the signal model, simulations and holds true for calibrated oscillators on the transceiver testbeds. If frequency offset is to be considered, PoA estimates need to be corrected according to (3.93).

The IDFT, MUSIC and DNN based ranging algorithms take as input the channel transfer function estimates according to (3.87)

$$\begin{aligned}\widehat{H}_{\mathrm{PoF}_c}^{[1,2]} &= \widehat{H}_{\mathrm{PoA}_c}^{[T_1,R_2]}\; \widehat{H}_{\mathrm{PoA}_c}^{[T_2,R_1]} \\ &= H_c^{[T_1,R_2]}\; H_c^{[T_2,R_1]}\; e^{\,j\left(\underbrace{\phi_\mathrm{R}^{T_1}-\phi_\mathrm{R}^{R_2}+\phi_\mathrm{R}^{T_2}-\phi_\mathrm{R}^{R_1}}_{\Sigma\Delta\phi_\mathrm{R}}\right)} + \tilde{N}_c,\end{aligned} \tag{5.2}$$

with noise $\tilde{N}_c$, modeling all encountered noise effects. The sum difference of initial oscillator phases $\Sigma\Delta\phi_\mathrm{R}$ is constant over all channels and hence not of concern, i.e. it will be omitted in the following. Due to the two-way ranging protocol required for eliminating the unknown time offset t_0, the square of the channel transfer function is estimated. Considering the tapped delay line channel model from (2.19), (5.2) can be rewritten as

$$\tilde{H}_c = \widehat{H}_{\mathrm{PoF}_c}^{[1,2]} = \left(\sum_{p=0}^{P-1} a_p e^{-j2\pi(f_\mathrm{w}+f_c)\tau_p}\right)^2 + \tilde{N}_c = \sum_{p=0}^{\tilde{P}-1} \tilde{a}_p e^{-j2\pi(f_\mathrm{w}+f_c)\tilde{\tau}_p} + \tilde{N}_c, \tag{5.3}$$

with $\tilde{(\cdot)}$ denoting amplitude, delay and number of the propagation paths after expansion of the square.

5.1.2 Advanced Range Estimation Methods

5.1.2.1 Path Delay Estimation Through Multiple Signal Classification

Estimating the delays $\tilde{\tau}_p$ from (5.3) can be formulated as MUSIC problem analog to [LF14]. For this purpose the C channel transfer function estimates $\tilde{H}_c$ are grouped into the vector

$$\tilde{\boldsymbol{H}} = \begin{pmatrix} \tilde{H}_0 \\ \vdots \\ \tilde{H}_{C-1} \end{pmatrix} = \begin{pmatrix} \sum_{p=0}^{\tilde{P}-1} \tilde{a}_p e^{-j2\pi(f_\mathrm{w}+f_0)\tilde{\tau}_p} \\ \vdots \\ \sum_{p=0}^{\tilde{P}-1} \tilde{a}_p e^{-j2\pi(f_\mathrm{w}+f_{C-1})\tilde{\tau}_p} \end{pmatrix} + \begin{pmatrix} \tilde{N}_0 \\ \vdots \\ \tilde{N}_{C-1} \end{pmatrix} \in \mathbb{C}^{C\times 1}. \tag{5.4}$$

Considering $f_c = c\Delta f$ and integrating the phase rotation at the channel $c = 0$ into the complex amplitude $\tilde{\alpha}'_p = \tilde{\alpha}_p\, e^{-j2\pi f_\mathrm{w}\tilde{\tau}_p}$, allows modifying (5.4) as

$$\tilde{\boldsymbol{H}} = \begin{pmatrix} \tilde{a}'_0 & + & \tilde{a}'_1 & + & \dots & + & \tilde{a}'_{\tilde{P}-1} \\ \tilde{a}'_0 e^{-j2\pi\Delta f\tilde{\tau}_0} & + & \tilde{a}'_1 e^{-j2\pi\Delta f\tilde{\tau}_1} & + & \dots & + & \tilde{a}'_{\tilde{P}-1} e^{-j2\pi\Delta f\tilde{\tau}_{\tilde{P}-1}} \\ \vdots & & \vdots & & \vdots & & \vdots \\ \tilde{a}'_0 e^{-j2\pi\Delta f(C-1)\tilde{\tau}_0} & + & \tilde{a}'_1 e^{-j2\pi\Delta f(C-1)\tilde{\tau}_1} & + & \dots & + & \tilde{a}'_{\tilde{P}-1} e^{-j2\pi\Delta f(C-1)\tilde{\tau}_{\tilde{P}-1}} \end{pmatrix} + \begin{pmatrix} \tilde{N}_0 \\ \tilde{N}_1 \\ \vdots \\ \tilde{N}_{C-1} \end{pmatrix}. \tag{5.5}$$

The so-called imaging vector can be defined as

$$\boldsymbol{\chi}^{C}\left(\tilde{\tau}_p\right) = \left[1\; e^{-j2\pi\Delta f\tilde{\tau}_p}\; \ldots\; e^{-j2\pi(C-1)\Delta f\tilde{\tau}_p}\right]^{\mathrm{T}} \in \mathbb{C}^{C\times 1}. \tag{5.6}$$

Further defining

$$\boldsymbol{\mathcal{X}}^{C} = \left[\boldsymbol{\chi}^{C}\left(\tilde{\tau}_0\right)\; \boldsymbol{\chi}^{C}\left(\tilde{\tau}_1\right)\; \ldots\; \boldsymbol{\chi}^{C}\left(\tilde{\tau}_{\tilde{P}-1}\right)\right] \in \mathbb{C}^{C\times\tilde{P}}, \tag{5.7}$$

allows reformulating (5.5) in matrix form as

$$\tilde{\boldsymbol{H}} = \begin{pmatrix} \tilde{H}_0 \\ \vdots \\ \tilde{H}_{C-1} \end{pmatrix} = \boldsymbol{\mathcal{X}}^{C}\tilde{\boldsymbol{\alpha}}' + \tilde{\boldsymbol{N}}, \tag{5.8}$$

with amplitude $\tilde{\boldsymbol{\alpha}}' = \left[\tilde{\alpha}'_0\; \tilde{\alpha}'_1\; \ldots\; \tilde{\alpha}'_{\tilde{P}-1}\right]^{\mathrm{T}} \in \mathbb{C}^{\tilde{P}\times 1}$ and noise $\tilde{\boldsymbol{N}} = \left[\tilde{N}_0\; \tilde{N}_1\; \ldots\; \tilde{N}_{C-1}\right]^{\mathrm{T}} \in \mathbb{C}^{C\times 1}$.

The classical MUSIC algorithm requires multiple successive channel measurements $\tilde{\boldsymbol{H}}(t)$ over time t, in order to calculate the autocorrelation function

$$\boldsymbol{R}_{\tilde{H}\tilde{H}} = \mathbb{E}\left[\tilde{\boldsymbol{H}}(t)\tilde{\boldsymbol{H}}^{*}(t)\right]. \tag{5.9}$$

Based on this autocorrelation function, the Singular Value Decomposition (SVD) can be given, which allows determining propagation delays $\tilde{\tau}_p$ according to a spectral decomposition as given in (5.12). If multiple snapshots over time are not available, the autocorrelation function cannot be constructed. Therefore, the so-called Hankel matrix is defined by

$$\boldsymbol{\Gamma} = \begin{pmatrix} \tilde{H}_0 & \tilde{H}_1 & \cdots & \tilde{H}_{C-L_\Gamma-1} \\ \tilde{H}_1 & \tilde{H}_2 & \cdots & \tilde{H}_{C-L_\Gamma} \\ \vdots & \vdots & \vdots & \vdots \\ \tilde{H}_{L_\Gamma} & \tilde{H}_{L_\Gamma+1} & \cdots & \tilde{H}_{C-1} \end{pmatrix} \in \mathbb{C}^{(L_\Gamma+1)\times(C-L_\Gamma)}, \tag{5.10}$$

with $1 \leq L_\Gamma < C-1$. It allows applying MUSIC to a single snapshot [LF14], i.e. a single channel transfer function estimation on C channels. The SVD of the Hankel matrix in (5.10) is given by

$$\boldsymbol{\Gamma} = \Big[\underbrace{\boldsymbol{U}_{\mathrm{S}}}_{(L_\Gamma+1)\times\tilde{P}} \quad \underbrace{\boldsymbol{U}_{\mathrm{N}}}_{(L_\Gamma+1)\times(L_\Gamma+1-\tilde{P})}\Big] \underbrace{\operatorname{diag}\left(\lambda_0\;\lambda_1\;\ldots\;\lambda_{\tilde{P}-1}\;0\;\ldots\;0\right)}_{(L_\Gamma+1)\times(C-L_\Gamma)} \Big[\underbrace{\boldsymbol{V}_{\mathrm{S}}}_{(C-L_\Gamma)\times\tilde{P}} \quad \underbrace{\boldsymbol{V}_{\mathrm{N}}}_{(C-L_\Gamma)\times(C-L_\Gamma-\tilde{P})}\Big]^{*}, \tag{5.11}$$

with singular values $\lambda_0 \geq \lambda_1 \geq \ldots \geq \lambda_{\tilde{P}-1} \geq 0$, signal and noise subspace $\boldsymbol{U}_{\mathrm{S}}$, $\boldsymbol{U}_{\mathrm{N}}$, respectively. Signal and noise subspace are orthogonal, while the signal space is spanned by the imaging vectors $\boldsymbol{\chi}\left(\tilde{\tau}_p\right)$ belonging to the actual propagation delays $\tilde{\tau}_p$. Consequently the set of delays $\tilde{\tau}_p$ can be obtained as the peaks in the imaging function $\mathcal{Y}$, defined by the orthogonal projection of the imaging vector $\boldsymbol{\chi}^{L_\Gamma+1}$ to the noise subspace $\boldsymbol{U}_{\mathrm{N}}$

$$\mathcal{Y}(\tau) = \frac{\left\|\boldsymbol{\chi}^{L_\Gamma+1}(\tau)\right\|_2}{\left\|\boldsymbol{U}_{\mathrm{N}}^{*}\boldsymbol{\chi}^{L_\Gamma+1}(\tau)\right\|_2}. \tag{5.12}$$

The imaging function $\mathcal{Y}$ can be interpreted as a delay spectrum function with peaks corresponding to the delays $\tilde{\tau}_p$. The range estimate $\widehat{d}_{\mathrm{PoF,MUSIC}}$ is obtained by applying the first path detection to (5.12).

In contrast to the IDFT approach, delay estimation by the MUSIC algorithm can achieve arbitrary high resolution for sufficiently low noise [LF14].

Two parameters can be modified and optimized in the MUSIC formulation for delay estimation. The parameter L_Γ allows defining the degree of correlation of the Hankel matrix. According to [LF14] $L_\Gamma \approx C/2$ is a good choice, which allows resolving $\tilde{P} \leq L_\Gamma$ propagation paths. The MUSIC algorithm furthermore requires the partitioning of the SVD into the signal and the noise subspace. The signal subspace is spanned by $\tilde{P}$ orthogonal, i.e. independent imaging vectors $\boldsymbol{\chi}^{L_\Gamma+1}\left(\tilde{\tau}_p\right)$. It is hence necessary to have a prior knowledge about the number of paths $\tilde{P}$. Partitioning of the subspaces can be achieved with a threshold on the singular values in order to separate zero singular values from non-zero singular values. Alternatively this parameter $\tilde{P}$ can be obtained with techniques from *e.g.* [Di85; KC94]. For the following study however, the number of propagation paths in the CIR is considered to be known.

5.1.2.2 Range Estimation with a Deep Neural Network

The range estimation problem can be addressed by a DNN based regression approach. It can be viewed as determining a function

$$g^{\boldsymbol{w}} : \mathbb{C}^C \rightarrow \mathbb{R}, \tag{5.13}$$

which allows computing the range based on the complex channel transfer function estimates. The parameter $\boldsymbol{w}$ contains the weights of the DNN network and this parameter needs to be determined such that the function $g^{\boldsymbol{w}}$ correctly maps channel estimates $\{\tilde{H}_c\}_{c=0}^{C-1}$ to the corresponding range d. The process of determining the weights $\boldsymbol{w}$ is called training step. It is achieved in a supervised learning phase with a so-called expert database

$$\mathcal{D} = \left\{ \left(\{\tilde{H}_{c,k}\}_{c=0}^{C-1}; d_k \right) \right\}_{k=1}^{K}, \tag{5.14}$$

which contains a set of K input channel transfer function estimates $\{\tilde{H}_{c,k}\}_{c=0}^{C-1}$ and the associated range d_k, called label. Based on this expert database, the training or optimization step consists in finding the network parameter $\boldsymbol{w}$, which minimizes the loss function

$$\mathcal{L}(\boldsymbol{w}) = \mathbb{E}\left[\left(g^{\boldsymbol{w}} \left(\{\tilde{H}_{c,k}\}_{c=0}^{C-1} \right) - d_k \right)^2 \right]. \tag{5.15}$$

Optimization with *e.g.* a gradient descend algorithm iteratively updates the network parameter $\boldsymbol{w}$ to converge to an optimum solution. Calculating the gradient for a non-trivial function $g^{\boldsymbol{w}}$ and a large database $\mathcal{D}$ is computationally too complex. Hence, to solve the optimization problem, an iterative Stochastic Gradient Descent (SGD) algorithm, widely used in literature [BCN18] is applied. At each iteration, the SGD algorithm randomly samples a mini-batch $\mathcal{B}_{\mathrm{DNN}i}$ of data from the expert database, i.e. $\mathcal{B}_{\mathrm{DNN}i} \in \mathcal{D}$. Calculating the stochastic gradient on the mini-batch $\mathcal{B}_{\mathrm{DNN}i}$ is computationally feasible. Subsequently, the network parameter $\boldsymbol{w}$ is updated with

$$\boldsymbol{w}_{i+1} = \boldsymbol{w}_i - \rho \frac{1}{|\mathcal{B}_{\mathrm{DNN}i}|} \nabla \mathcal{L}(\boldsymbol{w}_i, \mathcal{B}_{\mathrm{DNN}i}), \tag{5.16}$$

where ρ denotes the learning rate and $\nabla(\cdot)$ the gradient operator. The training phase aims at finding the parameter $\widehat{\boldsymbol{w}}$ that achieves range estimation with the smallest ranging error over the expert database. It is hence intuitively clear, that size, diversity and quality of the expert database play a crucial role regarding the performances of the DNN.

During the prediction phase, the range estimate $\widehat{d}_{\mathrm{PoF,DNN}}$ for a new input channel transfer function measurement $\{\tilde{H}_c\}_{c=0}^{C-1}$ is given by

$$\widehat{d}_{\mathrm{PoF,DNN}} = g^{\widehat{\boldsymbol{w}}} \left(\{\tilde{H}_c\}_{c=0}^{C-1} \right). \tag{5.17}$$

5.1.3 Numerical Simulations

Numerical simulations are conducted to evaluate the performances of the MUSIC and DNN based range estimators and comparison to the IDFT approach is given. Simulations consider a two-path propagation scenario with a direct and one multipath component

$$h(t) = \alpha_0 \delta(t - \tau_0) + \alpha_1 \delta(t - \tau_1). \tag{5.18}$$

The amplitude ratio is given by $\beta = |\alpha_1| / |\alpha_0|$ and the path delay difference is denoted $\Delta\tau = \tau_1 - \tau_0$.

Channel transfer function estimates are directly obtained from the model given in (5.2) instead of simulating the complete signal model from Chapter 3.2 and executing the localization metric extraction algorithms. This simplification is equivalent to simulating the whole signal model, but speeds up simulation considerably. The channel measurements are generated for $C = 16$ channels with a frequency spacing $\Delta f = 200\,\mathrm{kHz}$, resulting in a virtual bandwidth $B_{\mathrm{virt}} = 3\,\mathrm{MHz}$, a range resolution $\Delta R = 50\,\mathrm{m}$ and a maximum unambiguous range $R_{\max} = 750\,\mathrm{m}$. Noise on the channel estimates is simulated by adding Additive White Gaussian Noise (AWGN) of variance σ^2 to each generated channel estimate $\widehat{H}_{\mathrm{PoF}_c}^{[1,2]}$.

The first path detection algorithm from (3.91) is used on both, the IDFT and the MUSIC estimator, with the parameters $R_{\mathrm{first}} = 300\,\mathrm{m}$ and $\gamma_{\mathrm{first}} = -7\,\mathrm{dB}$. As simulations only consider a two-path propagation scenario, the number of paths to be estimated by the MUSIC method is set to $\tilde{P} = 3$, accounting for the two paths and the resulting phantom path (see Chapter 3.4.2.3).

Parameter	Symbol	Value
Path amplitude ratio	$\beta = \lvert\alpha_1\rvert / \lvert\alpha_0\rvert$	$-30,\ -25,\ -20,\ \ldots,\ -5,\ -3,\ -1,\ 0,\ 1,\ 3,\ 5,\ 10\,\mathrm{dB}$
Path delay difference	$\Delta\tau = \tau_1 - \tau_0$	$0,\ 10,\ 20,\ \ldots,\ 200\,\mathrm{m}$
Signal to Noise Ratio (SNR)	E_S / N_0	$-30,\ -25,\ -20,\ \ldots,\ 50\,\mathrm{dB}$
Monte Carlo runs		1500

TABLE 5.1 – *DNN training data generation parameters.*

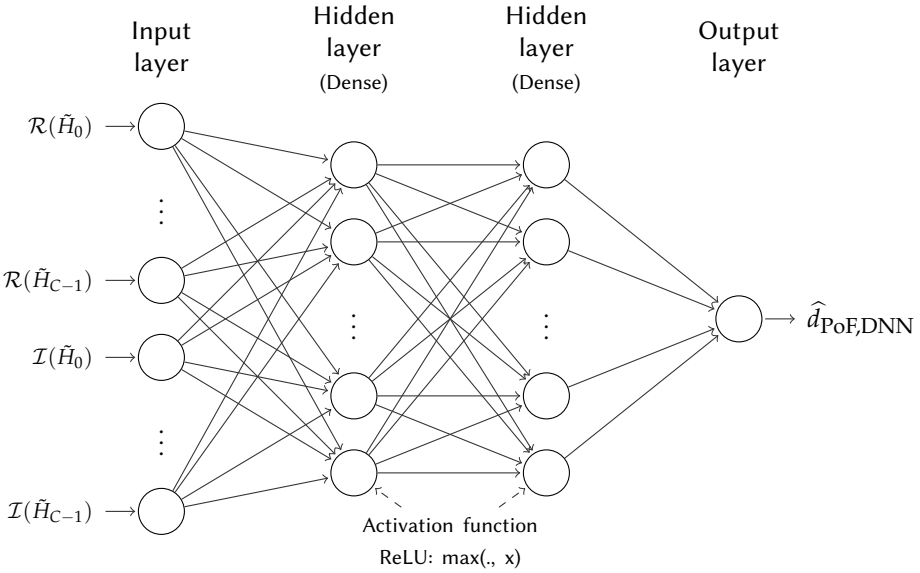


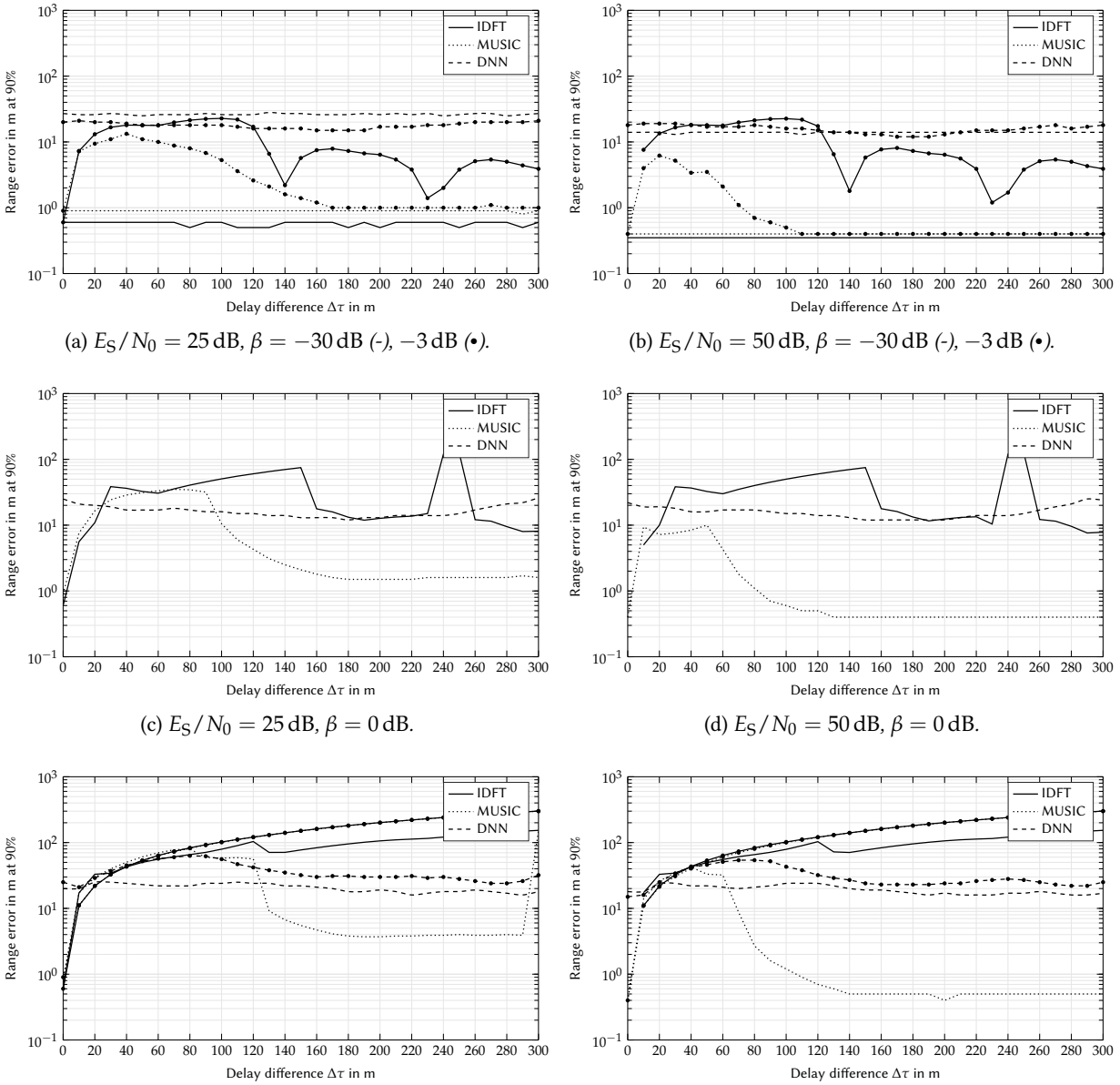
FIGURE 5.1 – *Illustration of the DNN architecture for multi-channel range estimation.*

For the DNN based range estimator, the expert database $\mathcal{D}$ needs to be created, which is achieved with numerical Monte Carlo simulation. For each parameter triplet $(\beta, \Delta\tau, E_S/N_0)$ in Table 5.1 a set of 1500 channel transfer function estimate $\{\tilde{H}_c\}_{c=0}^{C-1}$ realizations is generated. The totality of these simulated channel measurements constitutes the expert database $\mathcal{D}$.

This database is used to train the DNN based range estimator whose architecture is given in Figure 5.1. The DNN comprises three hidden layers of 128 units. Each neuron has a Rectifier Linear Unit (ReLU) activation except the final layer. For practical reasons the complex channel measurements are split into real $\mathcal{R}$ and imaginary part $\mathcal{I}$, resulting in $2C$ inputs for the DNN. Other representations such as providing the channel estimates as amplitude and phase information are equally possible and equivalent, and may provide easier normalization [Raj+18]. During the learning phase, a mini-batch of $\lvert\mathcal{B}_{\mathrm{DNN}i}\rvert = 32$ samples is randomly taken in each iteration from the expert database. The gradient descend optimization is performed with a learning rate $\rho = 0.001$.

The benchmarking of the IDFT, MUSIC and DNN estimators is done on a common and identical set of 5000 Monte Carlo simulations for each channel parameter configuration triplet $(\beta, \Delta\tau, E_S/N_0)$.

Figure 5.2a, Figure 5.2c and Figure 5.2e compare the maximum ranging error in 90% of the cases for the IDFT $\widehat{d}_{\mathrm{PoF,CIR-first}}$ and MUSIC $\widehat{d}_{\mathrm{PoF,MUSIC}}$ estimator as function of the path delay difference $\Delta\tau$. For a path delay difference approximately equal to the multi-channel range resolution ($c_0\Delta\tau \approx \Delta R$), a maximum error is observed, as overlapping main lobes form a larger lobe. The IDFT based range estimator shows performances with a side lobe-like shape with respect to the path delay difference $\Delta\tau$. This is explained by the fact that different main- and side lobes of the two path add up in a constructive or destructive manner, resulting in an altered CIR where first peak detection will be erroneous. The precision gain of MUSIC over the IDFT technique is most pronounced for path delay differences $\Delta\tau > 100\,\mathrm{m}$ as MUSIC resolves multiple propagation paths and precision asymptotically attains single path precision. Range estimation degrades as the path amplitude ratio β increases, which makes the detection of a weak first path difficult. For $\beta = 10\,\mathrm{dB}$, first path detection does no longer find the first path below the threshold $\gamma_{\mathrm{first}} = -7\,\mathrm{dB}$. Ranging errors then grow linearly with delay difference $\Delta\tau$. These findings are confirmed at high E_S/N_0, where MUSIC clearly outperforms the IDFT approach as depicted in Figure 5.2b,



(a) $E_S/N_0 = 25\,\text{dB}$, $\beta = -30\,\text{dB}$ *(-)*, $-3\,\text{dB}$ *(•)*.

(b) $E_S/N_0 = 50\,\text{dB}$, $\beta = -30\,\text{dB}$ *(-)*, $-3\,\text{dB}$ *(•)*.

(c) $E_S/N_0 = 25\,\text{dB}$, $\beta = 0\,\text{dB}$.

(d) $E_S/N_0 = 50\,\text{dB}$, $\beta = 0\,\text{dB}$.

(e) $E_S/N_0 = 25\,\text{dB}$, $\beta = 3\,\text{dB}$ *(-)*, $10\,\text{dB}$ *(•)*.

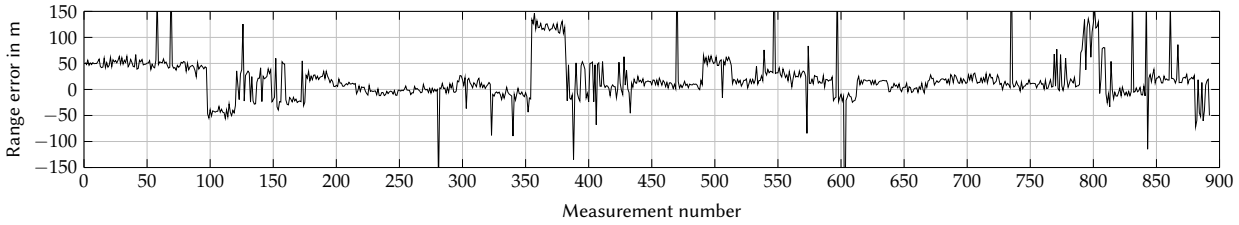
(f) $E_S/N_0 = 50\,\text{dB}$, $\beta = 3\,\text{dB}$ *(-)*, $10\,\text{dB}$ *(•)*.

FIGURE 5.2 – *Simulated ranging error for IDFT, MUSIC and DNN estimators in a two-path propagation scenario.*

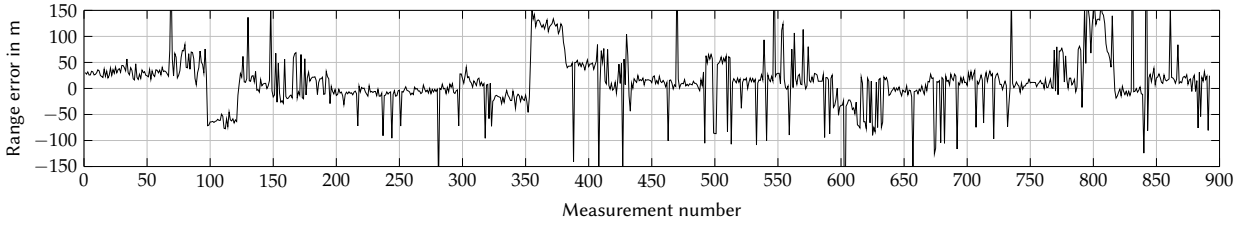
Figure 5.2d and Figure 5.2f. The first path detection algorithm parameters γ_{first} and R_{first} have been optimized for the European Telecommunications Standards Institute (ETSI) multipath channels. In order to improve performances, these parameters need to be adapted to the actual propagation channel. Furthermore, applying the first path detection algorithm to the imaging function in (5.12), which does not give the actual path amplitudes needs to be modified to determine the actual corresponding path amplitudes before applying the first path detection algorithm.

The try and error approach for determining the parameterization and the training database showed that ranging performances are very sensitive to the expert database. Empirically best and plausible performances have been obtained when training the DNN with multiple amplitude ratios close to the $\beta = 0\,\text{dB}$ as given in Table 5.1.

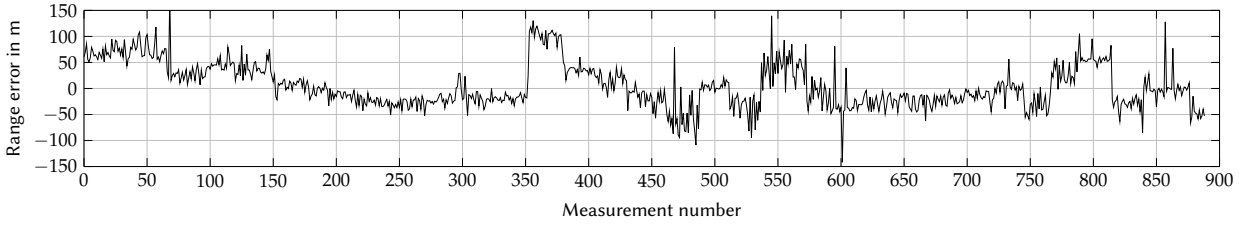
Figure 5.2 shows that the resulting DNN algorithm has comparable performance with respect to both IDFT and MUSIC algorithms. While for $\beta < 0\,\text{dB}$ it slightly performs less than the parametric methods, for $\beta \geq 0\,\text{dB}$, the precision of the DNN algorithm takes over when $\Delta\tau < 100\,\text{m}$ and at low E_S/N_0, but still remains lower than MUSIC technique when $\Delta\tau$ increases. In addition, it is worth to highlight that the proposed DNN algorithm is less sensitive to the variation of the parameters β, $\Delta\tau$, and E_S/N_0. In fact, the range estimation error almost remains constant at $\approx 25\,\text{m}$ when these parameters vary, demonstrating therefore the robustness of the DNN algorithm.



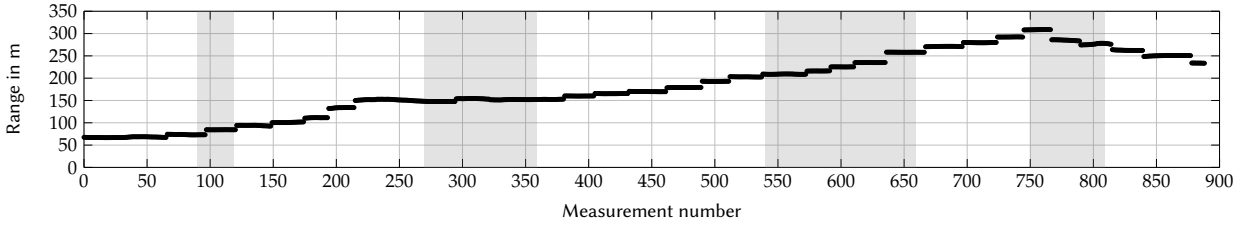
(a) *Ranging error on IDFT* $\widehat{d}_{\mathrm{PoF,CIR-first}}$.



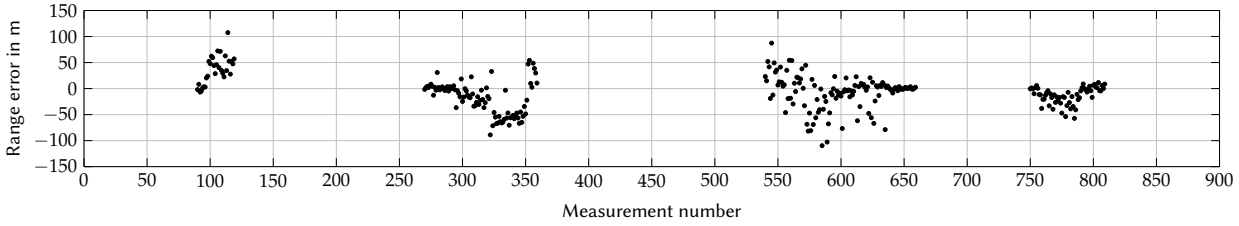
(b) *Ranging error on MUSIC* $\widehat{d}_{\mathrm{PoF,MUSIC}}$.



(c) *Ranging error for the Synthetic Data Trained DNN (S-DNN)* $\widehat{d}_{\mathrm{PoF,S-DNN}}$.



(d) *Global Navigation Satellite System (GNSS) ground truth with white = training data for DNN, gray = range estimation with DNN.*



(e) *Ranging error for synthetic and field trial data, i.e. the Mixed Data Trained DNN (M-DNN)* $\widehat{d}_{\mathrm{PoF,M-DNN}}$.

FIGURE 5.3 – *Multi-channel narrowband ranging errors for the* 900 *field trial measurements with* 10 kHz *bandwidth signals.*

5.1.4 Application to Field Trials

Numerical simulations have revealed that MUSIC outperforms the IDFT approach in terms of multipath resolution and they have shown furthermore, that the DNN method is robust against strong multipath. In this section, the three estimators are applied to real outdoor field trial channel measurement data.

Their performances are compared on the field trial measurements depicted in Figure 4.29 obtained with *Config Long* from Table 4.2.

Figure 5.3 shows the ranging errors for the different range estimation strategies. IDFT ranging precision in Figure 5.3a is below 30 m, however for certain positions large biases (> 100 m) are observed. Processing the field trial

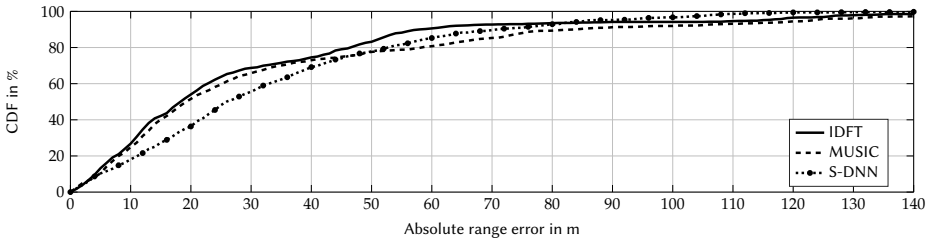


FIGURE 5.4 – *CDFs for field trial multi-channel narrowband range estimation with* 10 kHz *bandwidth signals on all* 900 *measurements.*

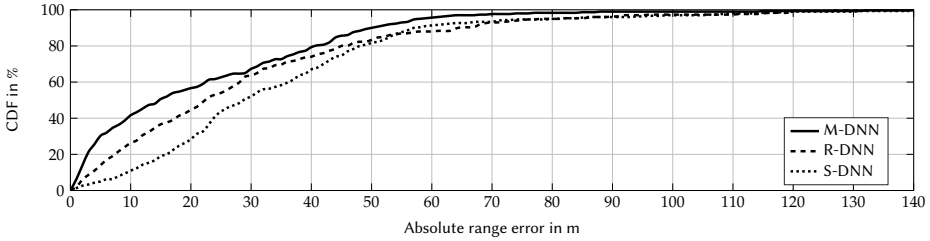


FIGURE 5.5 – *CDFs for field trial multi-channel narrowband range estimation with* 10 kHz *bandwidth signals on* 1/3 *of the measurements (Figure 5.3d, gray).*

measurements with the MUSIC algorithm in Figure 5.3b does not decrease these biases, despite the high-resolution capacity. Possible causes are insufficient SNR E_S/N_0 (compare Figure 5.2) or the mismatch between the hypothesis of a two-path channel, i.e. $\tilde{P} = 3$ and the real propagation channel.

Regarding the DNN approach, when trained on synthetic data and then applied on field trial data, the S-DNN slightly performs less than the two parametric estimators (Figure 5.3c). Once more, the hypothesis of a two-path channel is no longer valid in a real environment, leading to channel measurements that were not seen in the synthetic database. The Cumulative Distribution Functions (CDFs) in Figure 5.4 summarize the ranging accuracy of the performed field trial.

In order to overcome the weakness of an incomplete database, training can be performed on a portion of the real field trial data (Figure 5.3d), which is considered to constitute the expert database. Figure 5.5 shows the CDF for the Real Data Trained DNN (R-DNN) when trained on 2/3 and applied to the remaining 1/3 of the real field trial data in comparison to performances when the S-DNN is applied to the same 1/3 of the data.

Furthermore, better results can be obtained by taking advantage of synthetic data, by using these data to pre-train the DNN and then refining it with some field trial data (M-DNN) [Zap+18], thus reducing the need of an extensive geo-referenced channel measurement database. Figure 5.3e and Figure 5.5 show the results for this approach. The resulting M-DNN has better performances than both the S-DNN and the R-DNN, therefore demonstrating the benefit of taking into consideration both, real and synthetic data, for a robust algorithm.

In conclusion, parametric estimators and synthetic data trained deep learning achieve a ranging error below 60 m to 80 m in 90% of the cases and mixed data trained deep learning attains 45 m 90% of the cases.

Multi-channel narrowband LPWA ranging accuracy has been evaluated by numerical simulation in a two-path propagation scenario. Parametric range estimation through MUSIC outperforms the state of the art IDFT approach, due to its high-resolution property. In numerical simulation and for sufficient large E_S/N_0, MUSIC achieves more accurate range estimates for close multipath components than the IDFT technique. Applied to real outdoor field trials, MUSIC and IDFT estimators show comparable performances (60 to 80 m in 90% of the cases).

The deep learning based range estimation algorithm shows high robustness to multipath, with 25 m error in simulation and 45 m in 90% of the cases on the field trial data, when trained on mixed data. Multi-channel measurements provide improved temporal resolution through sequentially increased bandwidth. Combined with deep learning techniques, they are potential enablers for precise LPWA localization due to appropriate signal processing, especially for unknown and dense multipath propagation scenarios. Yet, generalization of these findings to other scenarios remains open.

Further work may consider training deep neural networks assuming more complex channel models. Extensive field trials will provide a comprehensive database for training with mixed, i.e. synthetic and real data.

The range and position estimation method through DNN based techniques is a promissing approach for accurate LPWA localization in challenging propagation enviroments. A patent application on this technique has been filed [WSdD19].

5.2 Conclusion and Perspectives

The IDFT based multi-channel ranging approach has a limited capability to resolve multipath due to the inherent side lobes of the IDFT. In order to overcome this shortcoming, high resolution algorithms can be used. The multi-channel range estimation can be formulated as MUSIC problem. Simulations have shown that MUSIC outperforms the IDFT based range estimator, however the algorithm requires high SNR levels.

Instead of relying on parametric estimators, learning based approaches recently find wide adoption in signal processing. Based on the sampled channel transfer function estimates, a DNN based range estimator has been trained on a simplistic two-path propagation model. The application of the DNN to real outdoor field trial data proves to be competitive with parametric estimators.

Several improvements for the investigated methods are possible. The parametric MUSIC estimator relies on the construction of the Hankel matrix with dimensions depending on a parameter L_Γ. This parameter as well as those of the first path algorithm can be optimized. The DNN based estimator can be trained with synthetic data of more realistic channel models, as well are refining with more field trial data.

Extracting localization metrics with a correlation based algorithm, i.e. Maximum Likelihood (ML) estimation is suboptimal and other approaches can be studied to improve the quality of the metrics in multipath scenarios. Instead of processing IQ data in this two step method, i.e. by first extracting localization metrics and then performing range estimation, it is also possible to design a framework that directly estimates range from IQ data.

Bibliography of Chapter 5

[AMB18] S. Aditya, A. F. Molisch, and H. M. Behairy. "A Survey on the Impact of Multipath on Wideband Time-of-Arrival Based Localization". In: *Proceedings of the IEEE* 106.7 (2018), pp. 1183–1203.

[AB17] H. Ahmadi and R. Bouallegue. "Exploiting machine learning strategies and RSSI for localization in wireless sensor networks: A survey". In: *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*. 2017, pp. 1150–1154.

[AK19] G. G. Anagnostopoulos and A. Kalousis. "A Reproducible Comparison of RSSI Fingerprinting Localization Methods Using LoRaWAN". In: *16th Workshop on Positioning, Navigation and Communications (WPNC)*. 2019.

[BGL18] O. Bialer, N. Garnett, and D. Levi. "A Deep Neural Network Approach for Time-Of- Arrival Estimation in Multipath Channels". In: *2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. 2018, pp. 2936–2940.

[BLJ13] M. Bkassiny, Y. Li, and S. K. Jayaweera. "A Survey on Machine-Learning Techniques in Cognitive Radios". In: *IEEE Communications Surveys Tutorials* 15.3 (2013), pp. 1136–1159.

[BCN18] L. Bottou, F. E. Curtis, and J. Nocedal. "Optimization Methods for Large-Scale Machine Learning". In: *SIAM Review* 60.2 (2018), 223–311. URL: http://dx.doi.org/10.1137/16M1080173.

[CZBL19] J. L. Carrera Villacrés, Z. Zhao, T. Braun, and Z. Li. "A Particle Filter-Based Reinforcement Learning Approach for Reliable Wireless Indoor Positioning". In: *IEEE Journal on Selected Areas in Communications* 37.11 (2019), pp. 2457–2473.

[CFT07] A. Chehri, P. Fortier, and P. Tardif. "On the TOA Estimation for UWB Ranging in Complex Confined Area". In: *2007 International Symposium on Signals, Systems and Electronics*. 2007, pp. 533–536.

[dM06] F. A. de Leon and J. J. S. Marciano. "Application of MUSIC, ESPRIT and SAGE Algorithms for Narrowband Signal Detection and Localization". In: *TENCON 2006 - 2006 IEEE Region 10 Conference*. 2006, pp. 1–4.

[Di85] A. Di. "Multiple Source Location - A Matrix Decomposition Approach". In: *IEEE Transactions on Acoustics, Speech, and Signal Processing* 33.5 (1985), pp. 1086–1091.

[GM99] E. Gonen and J. M. Mendel. "Subspace-Based Direction Finding Methods". In: *Madisetti, VK and Williams DB, editeur, The Digital Signal Processing Handbook, chapitre* 62 (1999).

[IRM15] A. Ibrahim, S. K. A. Rahim, and H. Mohamad. "Performance Evaluation of RSS-based WSN Indoor Localization Scheme using Artificial Neural Network SchemesJahn," in: *2015 IEEE 12th Malaysia International Conference on Communications (MICC)*. 2015, pp. 300–305.

[KOL15] S. Kim, D. Oh, and J. Lee. "Joint DFT-ESPRIT Estimation for TOA and DOA in Vehicle FMCW Radars". In: *IEEE Antennas and Wireless Propagation Letters* 14 (2015), pp. 1710–1713.

[KC94] H. Krim and J. H. Cozzens. "A Data-Based Enumeration Technique for Fully Correlated Signals". In: *IEEE Transactions on Signal Processing* 42.7 (1994), pp. 1662–1668.

[LPCY06] J. Li, L. Pei, M. Cao, and D. Yu. "Super-Resolution Time Delay Estimation Algorithm Based on the Frequency Domain Channel Model in OFDM Systems". In: *2006 6th World Congress on Intelligent Control and Automation*. Vol. 1. 2006, pp. 5144–5148.

[LF14] W. Liao and A. Fannjiang. "MUSIC for Single-Snapshot Spectral Estimation: Stability and Super-resolution". In: *CoRR* abs/1404.1484 (2014). arXiv: 1404.1484.

[Luo+19] N. C. Luong et al. "Applications of Deep Reinforcement Learning in Communications and Networking: A Survey". In: *IEEE Communications Surveys Tutorials* 21.4 (2019), pp. 3133–3174.

[Mal+19] M. E. Malmström et al. "5G Positioning -A Machine Learning Approach". In: *16th Workshop on Positioning, Navigation and Communications (WPNC)*. 2019.

[MHH18] Q. Mao, F. Hu, and Q. Hao. "Deep Learning for Intelligent Wireless Networks: A Comprehensive Survey". In: *IEEE Communications Surveys Tutorials* 20.4 (2018), pp. 2595–2621.

[MGWW10] S. Marano, W. M. Gifford, H. Wymeersch, and M. Z. Win. "NLOS Identification and Mitigation for Localization based on UWB Experimental Data". In: *IEEE Journal on Selected Areas in Communications* 28.7 (2010), pp. 1026–1035.

[Nii+19] A. Niitsoo et al. “A Deep Learning Approach to Position Estimation from Channel Impulse Responses”. In: *Sensors* 19.5 (2019), p. 1064.

[PMCM15] M. Passafiume, S. Maddio, A. Cidronali, and G. Manes. “MUSIC algorithm for RSSI-based DoA estimation on standard IEEE 802.11/802.15. x systems”. In: *World Sci. Eng. Acad. Soc. Trans. Signal Process* 11 (2015), pp. 58–68.

[Raj+18] S. Rajendran et al. “Deep Learning Models for Wireless Signal Classification With Distributed Low-Cost Spectrum Sensors”. In: *IEEE Transactions on Cognitive Communications and Networking* 4.3 (2018), pp. 433–445.

[Sch86] R. Schmidt. “Multiple Emitter Location and Signal Parameter Estimation”. In: *IEEE Transactions on Antennas and Propagation* 34.3 (1986), pp. 276–280.

[Sun+17] M. Sun et al. “Signal Subspace Smoothing Technique for Time Delay Estimation Using MUSIC Algorithm”. In: *Sensors* 17.12 (2017), p. 2868.

[SB+98] R. S. Sutton, A. G. Barto, et al. *Introduction to reinforcement learning. Vol. 135*. 1998.

[TVVH16] X. L. Tran, J. Vesely, S. Van Doan, and P. Hubacek. “UHF/C-band Testing of AOA Estimation Using MUSIC Algorithm”. In: *2016 New Trends in Signal Processing (NTSP)*. 2016, pp. 1–6.

[WSdD19] F. Wolf, M. Sana, S. de Rivaz, and F. Dehmas. “Méthode d’Estimation de Distance dans un Réseau LPWA et Méthode d’Estimation de Position Associée”. FR. Pat. Application N° 1910164. 2019.

[Wol+19b] F. Wolf et al. “Comparison of Multi-Channel Ranging Algorithms for Narrowband LPWAN Localization”. In: *2019 The International Symposium on Ubiquitous Networking (UNet)*. 2019, pp. 1–6.

[Yan+19] J. Yan et al. “Joint localisation and tracking for autonomous underwater vehicle: a reinforcement learning-based approach”. In: *IET Control Theory Applications* 13.17 (2019), pp. 2856–2865.

[Zap+18] A. Zappone et al. “Model-Aided Wireless Artificial Intelligence: Embedding Expert Knowledge in Deep Neural Networks Towards Wireless Systems Optimization”. In: *arXiv preprint arXiv:1808.01672* (2018).

[ZYLS06] F. Zhao, W. Yao, C. C. Logothetis, and Y. Song. “Comparison of Super-Resolution Algorithms for TOA Estimation in Indoor IEEE 802.11 Wireless LANs”. In: *2006 International Conference on Wireless Communications, Networking and Mobile Computing*. 2006, pp. 1–5.

Conclusion

Precise and accurate positioning in Low Power Wide Area (LPWA) networks is a challenging research field. The research community currently studies various approaches based on transmitted LPWA radio signals. Received Signal Strength Indicator (RSSI) and Time of Arrival (ToA) based techniques do not offer the precision required for many application contexts. Time based approaches being more precise than amplitude based techniques still suffer from limited bandwidth. Moreover, narrowband signals do not provide the required temporal resolution for accurate range measurements in multipath propagation environments typically encountered in LPWA networks.

Multi-channel ranging overcomes bandwidth limitations while being compatible to LPWA physical layers. Multiple narrowband channel estimations obtained sequentially on different frequencies are combined with a coherent processing method to obtain virtual large bandwidths. The principle is adapted to LPWA system constraints. Performances are evaluated with theoretical considerations of lower bounds and numerical simulations that illustrate how hardware impairments such as oscillator frequency offset can be corrected. Experimentation with a Software Defined Radio (SDR) based transceiver testbed validates working assumptions. Field trials in real outdoor urban scenarios, typical for LPWA networks, illustrate the significantly improved ranging precision of multi-channel ranging compared to classical single channel Time of Flight (ToF) measurements. The comparison to an industrial LPWA ranging solution emphasizes the scalability of ranging precision with multi-channel ranging while maintaining low levels of receiver sensitivity through instantaneous narrowband transmissions for long-range communication. Combining multi-channel ranging with advanced algorithms such as learning based methods proves to be a promising approach towards accurate positioning in LPWA networks with challenging multipath propagation.

The **first chapter** introduced the principles of LPWA networks and reviewed various physical layer standards and industrial solutions. Low-power and long-range communication is typically achieved with narrowband and low spectral efficiency modulation schemes. Signal bandwidths of LPWA systems range from 100Hz for Ultra-Narrow Band (UNB) up to 1 MHz when low spectral efficiency techniques are employed. Many Internet of Things (IoT) applications requiring wireless connectivity rely on LPWA networks. Those applications further require or benefit from the awareness of the geographical position within the network. Global Navigation Satellite System (GNSS) based localization offers highly accurate and precise position estimates in outdoor environments at the expense of power consumption. Achieving GNSS less, precise and accurate localization by taking advantage of the radio signals transmitted within the LPWA network opens up promising perspectives in terms of device complexity, power consumption and cost. An overview on radio signal based localization techniques has been given. Multi-channel ranging has been identified as suitable method for improved ranging precision within narrowband LPWA networks.

Challenges for precise and accurate radio signal based ranging have been illustrated in **chapter two**. These problematics include system level challenges such as narrowband transmissions to achieve low levels of receiver sensitivity and legal regulation limitations concerning i.e. transmit power and transmission duty cycle. Hardware challenges arise from low-cost components such as oscillators that exhibit frequency offsets, temporal drift and phase noise. These characteristics need to be considered for radio signal based localization as they affect the performance of positioning. A standard oscillator model has been presented and frequency offset influence on ToF ranging studied. Sufficient signal bandwidth and sophisticated signaling schemes allow overcoming the aforementioned challenges. However, the physical propagation channel remains as ultimate barrier to precise and accurate localization. Dense multipath propagation makes it difficult to resolve each multipath component with band limited signals. Strong multipath propagation and None Line of Sight (NLoS) scenarios do not allow recovering Line of Sight (LoS) range due to the practically absent LoS path. It is hence of importance to detect such a situation based on measurable channel characteristics in order to exclude biased range estimates from the location solving process. The chapter concluded by dressing the arising research questions and the scope of this thesis.

The principle of multi-channel ranging and differences with other methods is discussed in **chapter three**. Subsequently, the detailed signal model for multi-channel ranging has been developed. The model considers a general transceiver architecture with both, an analog Radio Frequency (RF) as well as a numerical Intermediate Frequency (IF) mixing stage. Transmitter and receiver carrier frequency synthesis is obtained from separate sources. The model includes clock impairments and multipath propagation. This general model is then adapted to multi-channel two-way ranging with unsynchronized nodes assuming a time invariant propagation channel and a constant frequency offset. Requirements on the transceiver hardware architecture are investigated. The required phase coherence between the two nodes is established in a round-trip packet exchange. This requires only intra-node phase coherence between the transmitter and the receiver branch, provided by a common Local Oscillator (LO). Theoretical performance bounds are derived based on Cramer Rao Lower Bounds (CRLBs). It has been shown that frequency offset induced errors can be corrected. Subsequently ranging algorithms have been constructed. CRLBs and numerical simulation have shown that meter-level ranging precision is achievable in an Additive White Gaussian Noise (AWGN) channel with 10kHz narrowband signals and multi-channel ranging.

Chapter four has investigated the practical feasibility of multi-channel ranging in LPWA networks. For this purpose a SDR based multi-channel transceiver testbed has been designed. Multi-channel ranging achieves errors below 10 m in 90% of the cases in both, simulation and experimentation in an AWGN channel. Outdoor field trials in real urban propagation scenarios have been performed and a comparison with an industrial ToF based ranging solution has been studied. Multi-channel Phase of Flight (PoF) range measurements are more precise compared to ToF measurements. However, large biases impede the accuracy of PoF ranging. Bias detection, mitigation and elimination techniques have been studied, which allow retaining only unbiased range estimates, achieving a 30 m ranging error in 90% of the outdoor field trials.

Chapter five investigated how advanced ranging algorithms can improve performances. The high-resolution algorithm Multiple Signal Classification (MUSIC) has been applied to the multi-channel ranging problem. It clearly outperforms the Inverse Discrete Fourier Transform (IDFT) based range estimator in a two-path channel model. However, these simulation results have not been confirmed when applying the MUSIC estimator to outdoor field trial measurements. Despite these findings, a learning based Deep Neural Network (DNN) range estimator showed to be competitive to the IDFT approach. These preliminary investigations are promissing as this method has the potential to outperform the IDFT technique in multipath scenarios especially when more comprehensive databases are available for the learning phase.

Main Contributions

Precise and accurate positioning within LPWA networks will be a key enabler for many IoT applications. This thesis addresses some challenges to achieve this goal, with the main contributions being:

- **A LPWA compatible ranging function for meter-level precision with narrowband to UNB signals in AWGN**
  Multi-channel ranging offers virtually increased bandwidth for precise range estimation. A comprehensive signal model [Wol+18b] comprising a general transceiver architecture, clock impairments and multipath propagation has been developed.
- **Validation by theory, simulations, experimentations and field trials**
  Theoretical performance bounds for multi-channel ranging have been derived and evaluated [Wol+18b] for the signal model. Multi-channel ranging applied to LPWA physical layers is studied in AWGN channels by numerical simulation and by experimentation with a SDR based transceiver testbed demonstrator developed in the framework of this thesis [Wol+18a]. A 10 m ranging precision is achieved. Outdoor field trials prove that PoF ranging is be more precise than ToF measurements, achieving 125 m and 250 m with 10 kHz signals respectively [WdDC19a].
- **Comparison to existing LPWA ranging solution**
  The proposed adaptation of multi-channel ranging to LPWA physical layers is compared to an existing industrial LPWA ranging solution. For this purpose, a methodology of comparison is defined. Performances of both platforms are evaluated and compared by outdoor field trials in LPWA typical propagation scenarios [Wol+19a].
- **Study of strategies to improve accuracy in multipath propagation channels**
  Multi-channel ranging provides estimates with a precision within a few 10m. However, large biases due to multipath propagation impede overall performances. Advanced range estimation techniques such as high-resolution algorithms and learning based methods are studied [Wol+19b]. A DNN based range

estimation technique has been patented [WSdD19]. Moreover an outlier detection scheme for multipath outdoor field trials has been developed [WdDC19a], achieving after outlier removal less than 30 m error in 90% of the cases. This procedure has been patented [WdDC19b].

Perspectives

Multi-channel ranging has proved to be applicable to LPWA networks and improves positioning precision and accuracy. Several perspectives can be pursued. These can be roughly grouped into low-level, hardware i.e. physical layer near topics, multipath and associated algorithm related investigations as well as high-level system considerations.

The thesis assumed multi-channel packet exchanges over rather short periods and constant clock frequency offsets. Further investigation is required to gain clear specifications how much time can lie between the channel measurements at different frequencies, regarding temporal radio channel variations, oscillator stability and phase noise. Appropriate algorithms such as tracking loops might be developed. Experimental demonstrations throughout this thesis have been made based on a SDR. In order to achieve final validation of the considered working hypotheses the integration of multi-channel ranging into existing and future LPWA solution and standards needs to be considered.

Several topics with respect to multipath propagation can be investigated. For this purpose, CRLBs need to be evaluated for a broader set of channel models. Such a study gives rise to an optimization strategy framework for the system parameters such as number of channels and frequency spacing. The thesis has considered uniform channel spacing, it is however also possible to use a non-uniform configuration which in turn might allow improving both ranging precision and maximum unambiguous range by joint optimization. In this context, it is also of interest to study windowing functions for the IDFT approach in order to reduce the side lobe level for optimal multipath resolution. From a more general perspective, it has to be questioned if the correlation based Maximum Likelihood (ML) localization metric extraction algorithms are optimal in multipath radio channels. The investigated advanced ranging algorithms have been applied to localization metrics obtained through ML estimation. New processing schemes departing directly from received IQ data shall be investigated. Promising machine learning based approaches require training with more realistic channel models and large field trial measurement datasets. Intermediate measurement campaigns on a channel emulator allow controlling the propagation channel and get detailed insight into potential improvements of algorithms. More field trials in a large-scale urban measurement campaign will allow validating the concept of multi-channel ranging and its limitations.

Field trials in urban propagation scenarios have shown that ranging accuracy is limited by multipath propagation. Future LPWA networks could include base stations equipped with beamforming enabled antenna arrays. Beamforming can be used in order to reduce multipath and hence decrease ranging biases. Preliminary measurements have shown an improved accuracy when employing directive antennas. In order to generalize these findings and to confirm the benefit of joint ranging and beamforming, simulations with angular dependent channel models can be conducted.

Furthermore, it has to be studied how the measured Channel Impulse Response (CIR) can be used not only for range extraction but also for getting reliable estimation quality indicators for the location solver.

Finally, a joint framework considering RSSI, ToA and Phase of Arrival (PoA) metrics for precise localization should be studied. Combining the set of all available metrics, information about the environment, *e.g.* street maps, star and mesh network topologies and sophisticated algorithms could be the answer to precise and accurate positioning in LPWA networks?

APPENDICES

A

Fresnel Zone for Radio Wave Propagation

The radius $R_{\text{Fresnel},k}$ of the k^{th} Fresnel zone with distance d_1, d_2 is derived from the distance difference between the direct and the once reflected path [Cam16] and can be given according to Figure 1.13 by

$$\Delta_1 = \sqrt{d_1^2 + R_{\text{Fresnel},k}^2} - d_1, \tag{A.1a}$$

$$\Delta_2 = \sqrt{d_2^2 + R_{\text{Fresnel},k}^2} - d_2. \tag{A.1b}$$

For the k^{th} Fresnel zone the following inequality holds

$$\Delta_1 + \Delta_2 \leq k\frac{\lambda_{\text{w}}}{2}. \tag{A.2}$$

After rearranging, squaring and solving, the Fresnel zone radius evaluates to

$$R_{\text{Fresnel},k} = \sqrt{\frac{\frac{k^4\lambda_{\text{w}}^4}{16} + \frac{k^3\lambda_{\text{w}}^3(d_1+d_2)}{2} + k^2\lambda_{\text{w}}^2\left[d_1d_2 + (d_1+d_2)^2\right] + 4k\lambda_{\text{w}}d_1d_2\,(d_1+d_2)}{4\,(d_1+d_2)\,[k\lambda_{\text{w}} + d_1 + d_2] + k^2\lambda_{\text{w}}^2}}. \tag{A.3}$$

All higher order terms in (A.3) are neglected as wavelength is small compared to the node distances ($k\lambda_{\text{w}} \ll d_1, d_2$). In approximation, Fresnel zone radius simplifies to

$$R_{\text{Fresnel},k} \approx \sqrt{\frac{k\lambda_{\text{w}}d_1d_2}{d_1+d_2}}. \tag{A.4}$$

Bibliography of Appendix A

[Cam16] Campbell Scientific. “Application Note: Line of Sight Obstruction”. In: (2016).

B

Derivations of Cramer-Rao Lower Bounds

In this appendix the derivations of various Cramer Rao Lower Bounds (CRLBs) are detailed. The CRLBs on the exotic radio localization techniques illustrate the attaignable precision and help judging if a method is applicable to LPWA positioning.

B.1 CRLB for RSSI-based Range Estimation

The estimated received power $\widehat{P}_\mathrm{r}$ can be expressed as a constant term $C_{\mathrm{st}0}$ integrating constant transmit power, antenna gains and carrier frequency. This term reflects the received power at the reference distance d_0. The second term models the logarithmic pathloss with pathloss exponent γ_L. However, the received power varies due to large- and small-scale fading which is modelled by a normal distributed noise term $(n_\mathrm{Channel})^\mathrm{dB}$ of variance $\left(\sigma^2_\mathrm{Channel}\right)^{\mathrm{dB}^2}$. Moreover, the receiver performs an estimation of the actual received power level. This estimation is not ideal and can be modelled with the $(n_\mathrm{RSSI})^\mathrm{dB}$ noise term following a normal distribution of variance $\left(\sigma^2_\mathrm{RSSI}\right)^{\mathrm{dB}^2}$ accounting *e.g.* for the step size of RSSI readings. The estimated receive power is given by

$$\begin{aligned}\left(\widehat{P}_\mathrm{r}\right)^\mathrm{dBm} &= (C_{\mathrm{st}0})^\mathrm{dBm} - 10\gamma_L \log_{10}\left(\frac{d}{d_0}\right) + (n_\mathrm{Channel})^\mathrm{dB} + (n_\mathrm{RSSI})^\mathrm{dB} \\ &= (C_{\mathrm{st}0})^\mathrm{dBm} - 10\gamma_L \frac{\ln\left(\frac{d}{d_0}\right)}{\ln 10} + (n_\mathrm{Channel})^\mathrm{dB} + (n_\mathrm{RSSI})^\mathrm{dB}. \end{aligned} \tag{B.1}$$

The Jacobian is given by

$$J_d = \frac{-10\gamma_L}{\ln 10}\frac{1}{d/d_0}\frac{1}{d_0} = \frac{-10\gamma_L}{d\ln 10}. \tag{B.2}$$

The Fisher Information Matrix (FIM) for range estimation is given by

$$I_d = J_d^T \Sigma^{-1} J_d = \left(\frac{-10\gamma_L}{d\ln 10}\right)^2 \frac{1}{\left(\sigma^2_\mathrm{Channel}\right)^{\mathrm{dB}^2} + \left(\sigma^2_\mathrm{RSSI}\right)^{\mathrm{dB}^2}}. \tag{B.3}$$

The standard deviation on RSSI based range estimation is given by

$$\sqrt{\mathrm{Var}\left(\widehat{d}\right)} \geq \sqrt{\frac{1}{I_d}} = \left(\frac{d\ln 10}{-10\gamma_L}\right)\sqrt{\left(\sigma^2_\mathrm{Channel}\right)^{\mathrm{dB}^2} + \left(\sigma^2_\mathrm{RSSI}\right)^{\mathrm{dB}^2}}. \tag{B.4}$$

Range estimation precision is proportional to the actual range, making it hence unsuitable for LPWA localization.

B.2 CRLB for Time of Arrival Estimation

In order to determine the CRLB for ToA, a delayed complex signal s_0 in AWGN n of total variance $\sigma^2 = N_0$ is considered

$$r(t) = \tilde{r}(t) + n(t) = s_0(t-\tau) + n(t). \tag{B.5}$$

The Jacobian of $\tilde{r}$ is given by

$$J_\tau(t) = \frac{\partial \tilde{r}(t)}{\partial \tau} = \frac{\partial s_0(t-\tau)}{\partial \tau} = -\frac{\partial s_0(t)}{\partial t}, \tag{B.6}$$

and according to [Kay93], the FIM I_τ for (B.5) results in

$$I_\tau(t) = J_\tau^T(t)\frac{1}{\sigma^2}J_\tau(t) = \frac{1}{\sigma^2}\left|\frac{\partial s_0(t)}{\partial t}\right|^2. \tag{B.7}$$

The total information is obtained by integrating over time

$$I_\tau = \int_{-\infty}^{\infty} I_\tau(t)\partial t = \int_{-\infty}^{\infty} \frac{1}{\sigma^2}\left|\frac{\partial s_0(t)}{\partial t}\right|^2 \partial t. \tag{B.8}$$

Applying the Fourier Transform theorem for derivatives and the theorem of Parsval yields

$$I_\tau = \frac{1}{\sigma^2}\int_{-\infty}^{\infty}\left|\frac{\partial s_0(t)}{\partial t}\right|^2 \partial t = \frac{1}{\sigma^2}\int_{-\infty}^{\infty}(2\pi f)^2\left|S_0(f)\right|^2 \partial f, \tag{B.9}$$

with signal spectrum S_0. The total energy available for ToA estimation is defined as

$$E_S = \int_{-\infty}^{\infty}|s_0(t)|^2\,\partial t = \int_{-\infty}^{\infty}|S_0(f)|^2\,\partial f. \tag{B.10}$$

According to [Kay93] the variance of an unbiased estimator is given by the CRLB as

$$\mathrm{Var}\left(\widehat{\tau}\right) \geq \mathrm{trace}\left(I_\tau^{-1}\right) = \frac{1}{\frac{1}{\sigma^2}\int_{-\infty}^{\infty}(2\pi f)^2\left|S_0(f)\right|^2\partial f} = \frac{1}{\frac{E_S}{\sigma^2}\frac{\int_{-\infty}^{\infty}(2\pi f)^2|S_0(f)|^2\partial f}{\int_{-\infty}^{\infty}|S_0(f)|^2\partial f}}. \tag{B.11}$$

Defining the root-mean-squared bandwidth by

$$B_{\mathrm{RMS}} = \sqrt{\frac{\int_{-\infty}^{\infty} f^2\left|S_0(f)\right|^2 df}{\int_{-\infty}^{\infty}\left|S_0(f)\right|^2 df}}, \tag{B.12}$$

allows simplifying (B.11) and ToA estimation standard deviation is bound by

$$\sqrt{\mathrm{Var}\left(\widehat{\tau}\right)} \geq \sqrt{\frac{1}{4\pi^2\frac{E_S}{N_0}B_{\mathrm{RMS}}^2}}. \tag{B.13}$$

It is worth noting, that this CRLB depends inverse proportional on the root-mean-squared bandwidth B_{RMS}. For non-coherent reception of r, the baseband spectrum S_0 centered at $f = 0$ is required for calculation. However, when signal reception is coherent to the emission of s_0, i.e. the absolute phase relation between transmitter and receiver are known, the passband spectrum S_0 integrating carrier frequency $f \gg 0$ results in a much larger root-mean-squared bandwidth B_{RMS}.

As a consequence, ToA estimation is more precise. This is the underlying principle in interferometric approaches and techniques that resolve carrier phase *e.g.* Real-Time Kinematic GPS (RTK-GPS).

B.3 CRLB for Delta-Sigma Monopulse AoA Estimation

The ratio of the difference to the sum signal is given according to (1.82) by

$$\frac{r_\Delta}{r_\Sigma} = -j\tan\left(\frac{\Delta\phi_A}{2}\right) = -j\tan\left(\frac{\pi D\sin(az)}{\lambda_w}\right), \tag{B.14}$$

with antenna spacing D. Considering the estimation of $\frac{r_\Delta}{r_\Sigma}$ in AWGN $n \sim \mathcal{N}(0, \sigma^2)$ yields

$$\widehat{\frac{r_\Delta}{r_\Sigma}} = \frac{r_\Delta}{r_\Sigma} + n(t). \tag{B.15}$$

The Jacobian of $\frac{r_\Delta}{r_\Sigma}$ is given by

$$J_{az} = \frac{\partial \frac{r_\Delta}{r_\Sigma}}{\partial az} = -j\frac{\frac{\pi D \cos(az)}{\lambda_\mathrm{w}}}{\cos^2\left(\frac{\pi D \sin(az)}{\lambda_\mathrm{w}}\right)} \tag{B.16}$$

and FIM I_{az} for (B.14) results in

$$I_{az} = J_{az}^T \frac{1}{\sigma^2} J_{az} = \frac{1}{\sigma^2}\left(\frac{\frac{\pi D \cos(az)}{\lambda_\mathrm{w}}}{\cos^2\left(\frac{\pi D \sin(az)}{\lambda_\mathrm{w}}\right)}\right)^2. \tag{B.17}$$

Consequently, the Delta-Sigma Monopulse Angle of Arrival (AoA) estimation standard deviation is bound by

$$\sqrt{\mathrm{Var}\left(\widehat{az}\right)} \geq \sqrt{I_{az}^{-1}} = \sigma\frac{\cos^2\left(\frac{\pi D \sin(az)}{\lambda_\mathrm{w}}\right)}{\frac{\pi D \cos(az)}{\lambda_\mathrm{w}}} \overset{|az| \ll 2\pi}{\approx} \frac{\sigma\lambda_\mathrm{w}}{\pi D}\cos^2\left(\frac{\pi D}{\lambda_\mathrm{w}} az\right). \tag{B.18}$$

B.4 CRLB for Doppler Direction Finder Based AoA Estimation

The instantaneous Doppler frequency as function of the angle $az(t) = \omega_\mathrm{D} t$ is given by

$$f_\mathrm{d}(t) = f_\mathrm{d}\left(az(t)\right) = -f_\mathrm{w}\frac{\omega_\mathrm{D} R_\mathrm{D} \sin\left(az(t) - az_i\right)}{c_0} = -f_\mathrm{w}\frac{\omega_\mathrm{D} R_\mathrm{D} \sin\left(\omega_\mathrm{D} t - az_i\right)}{c_0}, \tag{B.19}$$

with signal frequency f_w, signal angle az_i, antenna rotation speed ω_D and disc radius R_D.

Considering the estimation of the Doppler signal $f_\mathrm{d}(t)$ in AWGN $n \sim \mathcal{N}(0, \sigma^2)$ yields

$$\widehat{f_\mathrm{d}}(t) = f_\mathrm{d}(t) + n(t), \tag{B.20}$$

The Jacobian of $f_\mathrm{d}(t)$ is given by

$$J_{az_i}(t) = \frac{\partial f_\mathrm{d}(t)}{\partial az_i} = f_\mathrm{w}\frac{\omega_\mathrm{D} R_\mathrm{D} \cos\left(\omega_\mathrm{D} t - az_i\right)}{c_0} \tag{B.21}$$

and instantaneous FIM $I_{az_i}(t)$ for (B.19) results in

$$I_{az_i}(t) = J_{az_i}^T(t)\frac{1}{\sigma^2} J_{az_i}(t) = \frac{1}{\sigma^2}\left(f_\mathrm{w}\frac{\omega_\mathrm{D} R_\mathrm{D} \cos\left(\omega_\mathrm{D} t - az_i\right)}{c_0}\right)^2. \tag{B.22}$$

The total FIM I_{az_i} is given by observation over a time interval T

$$I_{az_i} = \int_0^T I_{az_i}(t)\partial t = \frac{1}{\sigma^2}\left(f_\mathrm{w}\frac{\omega_\mathrm{D} R_\mathrm{D}}{c_0}\right)^2 \int_0^T \cos^2\left(\omega_\mathrm{D} t - az_i\right)\partial t \overset{T \gg \frac{1}{\omega_\mathrm{D}}}{\approx} \frac{1}{\sigma^2}\left(f_\mathrm{w}\frac{\omega_\mathrm{D} R_\mathrm{D}}{c_0}\right)^2 \frac{T}{2}. \tag{B.23}$$

Consequently, the Doppler direction finder AoA estimation standard deviation is bound by

$$\sqrt{\mathrm{Var}\left(\widehat{az_i}\right)} \geq \sqrt{I_{az_i}^{-1}} = \frac{\sigma}{f_\mathrm{w}}\frac{c_0}{\omega_\mathrm{D} R_\mathrm{D}}\sqrt{\frac{2}{T}}. \tag{B.24}$$

AoA estimation precision depends on the relative frequency estimation precision σ / f_w. A higher rotation speed ω_D and a larger disc radius R_D equally improve precision.

B.5 CRLB for Lighthouse Range Estimation

The distance between a receiver/detector and the source can be determined by measuring the time the receiver dwells in the beam T_{beam} and the time the beam needs for a complete rotation T_{turn} according to

$$d \overset{d \gg D}{\approx} \frac{D}{2\sin\left[\pi\left(\frac{T_{\text{beam}}}{T_{\text{turn}}}\right)\right]}. \tag{B.25}$$

The observation variable T_{beam} can be given by rearranging (B.25) as

$$T_{\text{beam}} = \frac{T_{\text{turn}}}{\pi} \arcsin\left(\frac{D}{2d}\right). \tag{B.26}$$

In order to determine the CRLB for the estimation of distance d, it is assumed, that the estimate of the dwell time T_{beam} is unbiased and Gaussian distributed

$$\widehat{T_{\text{beam}}} = T_{\text{beam}} + n, \tag{B.27}$$

with estimation noise $n \sim \mathcal{N}(0, \sigma^2)$. The Jacobian of T_{beam} is given by

$$J_d = \frac{T_{\text{turn}}}{\pi} \frac{1}{\sqrt{1-\left(\frac{D}{2d}\right)^2}} \left(-\frac{D}{2d^2}\right) \tag{B.28}$$

and FIM I_d for (B.26) results in

$$I_d = J_d^T \frac{1}{\sigma^2} J_d = \frac{1}{\sigma^2} \left(\frac{T_{\text{turn}}}{\pi}\right)^2 \frac{1}{1-\left(\frac{D}{2d}\right)^2} \left(-\frac{D}{2d^2}\right)^2. \tag{B.29}$$

Consequently, the lighthouse range estimation standard deviation is bound by

$$\sqrt{\text{Var}\left(\widehat{d}\right)} \geq \sqrt{I_d^{-1}} = \sigma \frac{\pi}{T_{\text{turn}}} \left(1 - \left(\frac{D}{2d}\right)^2\right) \frac{2d^2}{D}. \tag{B.30}$$

For $D \ll d$, (B.30) simplifies to

$$\sqrt{\text{Var}\left(\widehat{d}\right)} \geq \sqrt{I_d^{-1}} \approx \sigma \frac{\pi}{T_{\text{turn}}} \frac{2d^2}{D}. \tag{B.31}$$

B.6 CRLB for Circular Trilateration

For K_{BS} base stations, range observations are given by

$$\widehat{\boldsymbol{d}} = \boldsymbol{d} + \boldsymbol{n}_{\text{Range}}, \tag{B.32}$$

with estimated distances $\widehat{\boldsymbol{d}} = [\widehat{d}_{u,0} \ldots \widehat{d}_{u,K_{\text{BS}}-1}]^T$, real distances $\boldsymbol{d} = [d_{u,0} \ldots d_{u,K_{\text{BS}}-1}]^T$ and the ranging error $\boldsymbol{n}_{\text{Range}} = [n_{\text{Range}_0} \ldots n_{\text{Range}_{K_{\text{BS}}-1}}]^T$ assumed to be normal distributed with $\boldsymbol{\sigma}^2_{\text{Range}} = \left[\sigma^2_{\text{Range}_0} \ldots \sigma^2_{\text{Range}_{K_{\text{BS}}-1}}\right]^T$.

The Jacobian matrix $\boldsymbol{J}_{\boldsymbol{x}_u}(\boldsymbol{x}_u)$ is defined by

$$\boldsymbol{J}_{\boldsymbol{x}_u}(\boldsymbol{x}_u) = \begin{pmatrix} \frac{x_u - x_0}{r_{u0}} & \frac{y_u - y_0}{r_{u0}} & \frac{z_u - z_0}{r_{u0}} \\ & \vdots & \\ \frac{x_u - x_{K_{\text{BS}}-1}}{r_{uK_{\text{BS}}-1}} & \frac{y_u - y_{K_{\text{BS}}-1}}{r_{uK_{\text{BS}}-1}} & \frac{z_u - z_{K_{\text{BS}}-1}}{r_{uK_{\text{BS}}-1}} \end{pmatrix}. \tag{B.33}$$

Assuming equal range estimation error distributions and independent range estimates, the observation covariance matrix simplifies to the diagonal matrix

$$\boldsymbol{\Sigma} = \text{diag}\left(\boldsymbol{\sigma}_{\text{Range}}{}^2\right). \tag{B.34}$$

Consequently, the FIM $\boldsymbol{I}_{\boldsymbol{x}_u}(\boldsymbol{x}_u)$ of the range observation vector $\boldsymbol{d}$ is defined by

$$\begin{aligned}\boldsymbol{I}_{\boldsymbol{x}_u}(\boldsymbol{x}_u) &= \boldsymbol{J}_{\boldsymbol{x}_u}^T(\boldsymbol{x}_u)\,\boldsymbol{\Sigma}^{-1}\boldsymbol{J}_{\boldsymbol{x}_u}(\boldsymbol{x}_u) \\ &= \begin{pmatrix} \sum_{i=0}^{K_{\mathrm{BS}}-1}\left(\frac{x_u-x_i}{\sigma_{\mathrm{Range}_i} d_{u,i}}\right)^2 & \sum_{i=0}^{K_{\mathrm{BS}}-1}\frac{(x_u-x_i)(y_u-y_i)}{\left(\sigma_{\mathrm{Range}_i} d_{u,i}\right)^2} & \sum_{i=0}^{K_{\mathrm{BS}}-1}\frac{(x_u-x_i)(z_u-z_i)}{\left(\sigma_{\mathrm{Range}_i} d_{u,i}\right)^2} \\ \sum_{i=0}^{K_{\mathrm{BS}}-1}\frac{(y_u-y_i)(x_u-x_i)}{\left(\sigma_{\mathrm{Range}_i} d_{u,i}\right)^2} & \sum_{i=0}^{K_{\mathrm{BS}}-1}\left(\frac{y_u-y_i}{\sigma_{\mathrm{Range}_i} d_{u,i}}\right)^2 & \sum_{i=0}^{K_{\mathrm{BS}}-1}\frac{(y_u-y_i)(z_u-z_i)}{\left(\sigma_{\mathrm{Range}_i} d_{u,i}\right)^2} \\ \sum_{i=0}^{K_{\mathrm{BS}}-1}\frac{(z_u-z_i)(x_u-x_i)}{\left(\sigma_{\mathrm{Range}_i} d_{u,i}\right)^2} & \sum_{i=0}^{K_{\mathrm{BS}}-1}\frac{(z_u-z_i)(y_u-y_i)}{\left(\sigma_{\mathrm{Range}_i} d_{u,i}\right)^2} & \sum_{i=0}^{K_{\mathrm{BS}}-1}\left(\frac{z_u-z_i}{\sigma_{\mathrm{Range}_i} d_{u,i}}\right)^2 \end{pmatrix}. \end{aligned} \tag{B.35}$$

Bibliography of Appendix B

[Kay93] S. M. Kay. *Fundamentals of Statistical Signal Processing: Estimation Theory*. 1993.

C

Jacobian Matrix for the Multi-Channel Ranging Signal Model

In order to derive the CRLB for the signal model presented in Chapter 3.3.2, the Jacobian Matrix (JM) is analytically derived. Based on these analytical expressions, the CRLB is evaluated numerically.

The Jacobian matrix $\boldsymbol{J}[k] \in \mathbb{R}^{4C \times (2C+4)}$ of $\boldsymbol{R}$ is defined by

$$\boldsymbol{J}[k] = \begin{pmatrix} \tilde{\boldsymbol{J}}_{\boldsymbol{R}}[k]^{[T_1,R_2]} \\ \tilde{\boldsymbol{J}}_{\boldsymbol{R}}[k]^{[T_2,R_1]} \end{pmatrix}, \tag{C.1}$$

with

$$\left[\tilde{\boldsymbol{J}}_{\boldsymbol{R}}[k]^{[X]}\right]_{(c,i)} = \frac{\partial \tilde{r}_c^{[X]}[k]}{\partial \theta_i}, \tag{C.2}$$

where $c \in [0, 2C-1]$ and $i \in [0, 2C+3]$.

In order to simplify the notation of partial derivatives, parameters in the final receive signal $\tilde{r}_c^{[X]}$ from (3.28) are redefined as

$$\tilde{r}_c^{[X]}[k] = \alpha_c^{[X]}\, s_0\left(\underbrace{\delta_{\mathrm{T}}^{[X]}\left(kT_{\mathrm{Samp}} - t_{\mathrm{A}c}^{[X]}\right)}_{\mathcal{A}}\right) \cdot e^{j\left(\underbrace{2\pi\delta_f^{[X]}\left(f_{\mathrm{w}c} + f_c\right)kT_{\mathrm{Samp}} + \phi_{\mathrm{A}c}^{[X]}[k]}_{\mathcal{B}}\right)}. \tag{C.3}$$

Omitting sampling index k and the argument of the transmit waveform s_0 for clarity, the partial derivatives are given by

- Delay, time offset and frequency offset i.e. $\theta_i \in \{\tau_0, t_0, \delta_f\}$

$$\frac{\partial \tilde{r}_c^{[X]}}{\partial \theta_i} = \alpha_c^{[X]}\left[\frac{\partial s_0}{\partial \mathcal{A}_c^{[X]}}\frac{\partial \mathcal{A}_c^{[X]}}{\partial \theta_i} + j s_0 \frac{\partial \mathcal{B}^{[X]}}{\partial \theta_i}\right] e^{j\mathcal{B}_c^{[X]}}. \tag{C.4}$$

- Center multipath propagation channel amplitude and phase i.e. $\theta_i \in \{a_{\mathrm{x}}, \phi_{\mathrm{x}}\}$

$$\frac{\partial \tilde{r}_c^{[X]}}{\partial \theta_i} = \begin{cases} s_0\left(\mathcal{A}_c^{[X]}\right) e^{j\mathcal{B}_c^{[X]}} & \text{if} \quad \theta_i = a_{\mathrm{x}}, \\ j\,\tilde{r}_c^{[X]} & \text{if} \quad \theta_i = \phi_{\mathrm{x}}. \end{cases} \tag{C.5}$$

- Relative multipath propagation channel amplitude and phase offsets i.e. $\theta_i \in \{\Delta a_i, \Delta\phi_i\}$ and $i = c \neq \left\lceil \frac{C}{2} \right\rceil - 1$

$$\frac{\partial \tilde{r}_c^{[X]}}{\partial \theta_i} = \begin{cases} s_0\left(\mathcal{A}_c^{[X]}\right) e^{j\mathcal{B}_c^{[X]}} & \text{if} \quad \theta_i = \Delta a_i, \\ j\tilde{r}_c^{[X]} & \text{if} \quad \theta_i = \Delta\phi_i. \end{cases} \tag{C.6}$$

- Initial oscillator phase offset sum-difference i.e. $\theta_i = \Delta\phi_{\mathrm{R}}$

$$\frac{\partial \tilde{r}_c^{[X]}}{\partial \theta_i} = j\,\tilde{r}_c^{[X]} \quad \text{if} \quad [X] = [T_2, R_1]. \tag{C.7}$$

All other terms are zero. Auxiliary derivatives are given in the following with upper choice if $[X] = [T_1, R_2]$ and lower choice if $[X] = [T_2, R_1]$

- Partial derivatives with respect to delay τ_0

$$\frac{\partial \mathcal{A}_c^{[X]}}{\partial \tau_0} = -\delta_{\mathrm{T}}^{[X]} \begin{cases} 1+\delta_f, \\ 1, \end{cases} \tag{C.8}$$

$$\frac{\partial \mathcal{B}_c^{[X]}}{\partial \tau_0} = \frac{\partial \phi_{\mathrm{A}c}^{[X]}}{\partial \tau_0} = -2\pi \left(f_{\mathrm{w}c} + f_c\right) \begin{cases} 1, \\ 1+\delta_f, \end{cases} \tag{C.9}$$

- Partial derivatives with respect to time offset t_0

$$\frac{\partial \mathcal{A}_c^{[X]}}{\partial t_0} = -\delta_{\mathrm{T}}^{[X]} \begin{cases} -1, \\ \frac{1}{1+\delta_f}, \end{cases} \tag{C.10}$$

$$\frac{\partial \mathcal{B}_c^{[X]}}{\partial t_0} = \frac{\partial \phi_{\mathrm{A}c}^{[X]}}{\partial t_0} = 2\pi \begin{cases} \frac{-\delta_f f_{\mathrm{w}} + f_c}{1+\delta_f}, \\ f_c, \end{cases} \tag{C.11}$$

- Partial derivatives with respect to frequency offset δ_f

$$\frac{\partial \mathcal{A}_c^{[X]}}{\partial \delta_f} = \begin{cases} -\frac{1}{\left(1+\delta_f\right)^2} \left(kT_{\mathrm{Samp}} - t_{\mathrm{A}c}^{[X]}\right) - \delta_{\mathrm{T}}^{[X]} \tau_0, \\ kT_{\mathrm{Samp}} - t_{\mathrm{A}c}^{[X]} - \delta_{\mathrm{T}}^{[X]} \frac{t_0 - K_{\mathrm{S}} T_{\mathrm{Samp}}}{\left(1+\delta_f\right)^2}, \end{cases} \tag{C.12}$$

$$\frac{\partial \mathcal{B}_c^{[X]}}{\partial \delta_f} = 2\pi \left(f_{\mathrm{w}c} + f_c\right) \begin{cases} -\frac{-kT_{\mathrm{Samp}} + t_0}{(1+\delta_f)^2}, \\ kT_{\mathrm{Samp}} - \tau_0 + K_{\mathrm{S}} T_{\mathrm{Samp}}. \end{cases} \tag{C.13}$$

Bibliography of Appendix C

Bibliography

[3GP08] 3GPP. *Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); Base Station (BS) radio transmission and reception (Release 8)*. 3rd Generation Partnership Project (3GPP), 2008.

[3GP15] 3GPP. *3GPP Release 12*. http://www.3gpp.org/specifications/releases/68-release-12. 2015.

[3GP16] 3GPP. *3GPP Release 13*. https://www.3gpp.org/release-13. 2016.

[Abr70] N. Abramson. "THE ALOHA SYSTEM: another alternative for computer communications". In: *Proceedings of the November 17-19, 1970, fall joint computer conference*. ACM. 1970, pp. 281–285.

[Act] Actility. *Carrier grade IoT connectivity platform to manage your LoRaWAN/LPWA networks and build IoT solutions*. https://www.actility.com/. Accessed: 2020/07/31.

[AMB18] S. Aditya, A. F. Molisch, and H. M. Behairy. "A Survey on the Impact of Multipath on Wideband Time-of-Arrival Based Localization". In: *Proceedings of the IEEE* 106.7 (2018), pp. 1183–1203.

[ABBW18] M. Aernouts, B. Bellekens, R. Berkvens, and M. Weyn. "A Comparison of Signal Strength Localization Methods with Sigfox". In: *2018 15th Workshop on Positioning, Navigation and Communications (WPNC)*. 2018, pp. 1–6.

[ABVVW18] M. Aernouts, R. Berkvens, K. Van Vlaenderen, and M. Weyn. "Sigfox and LoRaWAN Datasets for Fingerprint Localization in Large Urban and Rural Areas". In: *Data* 3.2 (2018), p. 13.

[AB17] H. Ahmadi and R. Bouallegue. "Exploiting machine learning strategies and RSSI for localization in wireless sensor networks: A survey". In: *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*. 2017, pp. 1150–1154.

[All83] D. W. Allan. *Clock characterization tutorial*. National Aeronautics, Space Administration, Office of Management, Scientific, and Technical Information Division, 1983.

[AW08] A. Amar and A. J. Weiss. "Localization of Narrowband Radio Emitters Based on Doppler Frequency Shifts". In: *IEEE Transactions on Signal Processing* 56.11 (2008), pp. 5500–5508.

[AEY10] W. Ammar, A. ElDawy, and M. Youssef. "Secure Localization in Wireless Sensor Networks: A Survey". In: *CoRR* abs/1004.3164 (2010). URL: http://arxiv.org/abs/1004.3164.

[AK19] G. G. Anagnostopoulos and A. Kalousis. "A Reproducible Comparison of RSSI Fingerprinting Localization Methods Using LoRaWAN". In: *16th Workshop on Positioning, Navigation and Communications (WPNC)*. 2019.

[Ana13] Analog Devices. *RF Agile Transceiver AD9361*. http://www.analog.com/media/en/technical-documentation/data-sheets/AD9361.pdf. 2013.

[Ang+12] M. Angermann et al. "Characterization of the Indoor Magnetic Field for Applications in Localization and Mapping". In: *2012 International Conference on Indoor Positioning and Indoor Navigation (IPIN)*. 2012, pp. 1–9.

[ARLH17] E. Aras, G. S. Ramachandran, P. Lawrence, and D. Hughes. "Exploring the Security Vulnerabilities of LoRa". In: *2017 3rd IEEE International Conference on Cybernetics (CYBCONF)*. 2017, pp. 1–6.

[Ash+13] R. Ashkar et al. "A Low-Cost Shoe-Mounted Inertial Navigation System with Magnetic Disturbance Compensation". In: *International Conference on Indoor Positioning and Indoor Navigation*. 2013, pp. 1–10.

[Atm13] Atmel. *Atmel AVR2152: RTB Evaluation Application Software User's Guide*. Accessed: 2020/07/31. Feb. 2013.

[Atm14] Atmel. "System, method, and circuit for distance measurement between two nodes of a radio network". Pat. 8,644,768. 2014.

[BKLL17] W. Bakkali, M. Kieffer, M. Lalam, and T. Lestable. "Kalman Filter-Based Localization for Internet of Things LoRaWAN™ End Points". In: *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*. 2017, pp. 1–6.

[Bek+18] M. R. Bekkar et al. "Constant modulus hybrid beamforming for multi-user systems in the presence of blockers". In: *2018 25th International Conference on Telecommunications (ICT)*. 2018, pp. 378–382.

[BFT19] M. A. Ben Temim, G. Ferre, and R. Tajan. "Analysis of the Coexistence of Ultra Narrow Band and Spread Spectrum Technologies in ISM Bands". In: *5th International Symposium on Ubiquitous Networking (UNet)*. 2019.

[BP17] M. Bertanha and R. W. Pazzi. "JLPR: Joint Range-Based Localization Using Trilateration and Packet Routing in Wireless Sensor Networks with Mobile Sinks". In: *2017 IEEE Symposium on Computers and Communications (ISCC)*. 2017, pp. 645–650.

[BGL18] O. Bialer, N. Garnett, and D. Levi. "A Deep Neural Network Approach for Time-Of- Arrival Estimation in Multipath Channels". In: *2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. 2018, pp. 2936–2940.

[BPE18] P. Bianchi, F. Portier, and K. Elgui. "A semi parametric model for RSSI-based localization, Modele semi parametrique pour la localisation par RSSI". In: (2018).

[BLJ13] M. Bkassiny, Y. Li, and S. K. Jayaweera. "A Survey on Machine-Learning Techniques in Cognitive Radios". In: *IEEE Communications Surveys Tutorials* 15.3 (2013), pp. 1136–1159.

[BCN18] L. Bottou, F. E. Curtis, and J. Nocedal. "Optimization Methods for Large-Scale Machine Learning". In: *SIAM Review* 60.2 (2018), 223–311. URL: http://dx.doi.org/10.1137/16M1080173.

[BR07] Y. d. J. Bultitude and T. Rautiainen. "IST-4-027756 WINNER II D1. 1.2 V1. 2 WINNER II Channel Models". In: *EBITG, TUI, UOULU, CU/CRC, NOKIA, Tech. Rep., Tech. Rep* (2007).

[Cam16] Campbell Scientific. "Application Note: Line of Sight Obstruction". In: (2016).

[CZBL19] J. L. Carrera Villacrés, Z. Zhao, T. Braun, and Z. Li. "A Particle Filter-Based Reinforcement Learning Approach for Reliable Wireless Indoor Positioning". In: *IEEE Journal on Selected Areas in Communications* 37.11 (2019), pp. 2457–2473.

[CL] CEA-Leti. *Hyloc - Une plateforme materielle embarquee flexible, analyse des algorithmes de surveillance de mouvement et de localisation multimodale*. http://www.leti-cea.fr/cea-tech/leti/Pages/innovation-industrielle/Demonstrateurs/HYLOC.aspx. Accessed: 2020/07/31.

[CEP18] CEPT. *ERC Recommendation 70-03*. Aug. 2018.

[CZZ75] D. Chazan, M. Zakai, and J. Ziv. "Improved Lower Bounds on Signal Parameter Estimation". In: *IEEE transactions on Information Theory* 21.1 (1975), pp. 90–93.

[CFT07] A. Chehri, P. Fortier, and P. Tardif. "On the TOA Estimation for UWB Ranging in Complex Confined Area". In: *2007 International Symposium on Signals, Systems and Electronics*. 2007, pp. 533–536.

[Chu72] D. Chu. "Polyphase Codes With Good Periodic Correlation Properties (Corresp.)" In: *IEEE Transactions on Information Theory* 18.4 (1972), pp. 531–532.

[Cro17] CrowdSupply. *LimeSDR: Flexible, Next-generation, Open Source Software Defined Radio*. https://www.crowdsupply.com/lime-micro/limesdr. 2017.

[dBLD19] A. P. da Silva, I. H. Brahmi, S. Leirens, and B. Denis. "System-level Simulation of Cooperative Sensor Data Fusion Strategies for Improved Vulnerable Road Users Safety". In: *16th Workshop on Positioning, Navigation and Communications (WPNC)*. 2019.

[DW09] D. Dardari and M. Z. Win. "Ziv-Zakai Bound on Time-Of-Arrival Estimation with Statistical Channel Knowledge at the Receiver". In: *2009 IEEE International Conference on Ultra-Wideband*. 2009, pp. 624–629.

[dM06] F. A. de Leon and J. J. S. Marciano. "Application of MUSIC, ESPRIT and SAGE Algorithms for Narrowband Signal Detection and Localization". In: *TENCON 2006 - 2006 IEEE Region 10 Conference*. 2006, pp. 1–4.

[Dec15] DecaWave. *DWM1000 Ultra Wideband (UWB) transceiver IC*. http://www.decawave.com/sites/default/files/resources/dwm1000-datasheet-v1.3.pdf. Accessed: 2020/07/31. 2015.

[Dem06] A. Demir. "Computing Timing Jitter From Phase Noise Spectra for Oscillators and Phase-Locked Loops With White and 1/f Noise". In: *IEEE Transactions on Circuits and Systems I: Regular Papers* 53.9 (2006), pp. 1869–1884. URL: http://ieeexplore.ieee.org/document/1703773/.

[Di85] A. Di. "Multiple Source Location - A Matrix Decomposition Approach". In: *IEEE Transactions on Acoustics, Speech, and Signal Processing* 33.5 (1985), pp. 1086–1091.

[Dio+19] C. Diouf et al. "A 400 Msps SDR platform for prototyping accurate wideband ranging techniques". In: *16th Workshop on Positioning, Navigation and Communications (WPNC)*. 2019.

[Dog17] M. Dogotari. "Hardware Design and RF Performance Evaluation of a Long Range 2.4 GHz Radio Module". MA thesis. 2017.

[DCM18] I. Dotlic, A. Connell, and M. McLaughlin. "Ranging Methods Utilizing Carrier Frequency Offset Estimation". In: *2018 15th Workshop on Positioning, Navigation and Communications (WPNC)*. 2018, pp. 1–6.

[Eff] Effigis. *The Smart City And The Importance Of The "Where"*. https://www.effigis.com/en/smart-city-importance-of-the-where/. Accessed: 2020/07/31.

[Enc] Encyclopaedia Britannica. *Sextant*. https://www.britannica.com/technology/sextant-instrument. Accessed: 2020/07/31.

[Enc12] Encyclopaedia Britannica. *Calculating the Distance to a Lightning Strike*. 2012. URL: http://blogs.britannica.com/2012/07/calculating-the-distance-to-a-lightning-strike/.

[ETS10] ETSI. *Universal Mobile Telecommunications System (UMTS); Deployment aspects (3GPP TR 25.943 version 9.0.0 Release 9)*. European Telecommunications Standards Institute (ETSI), 2010.

[ETS17] ETSI. *LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) radio transmission and reception (3GPP TS 36.101 version 13.6.1 Release 13)*. European Telecommunications Standards Institute (ETSI), 2017.

[Ett] Ettus Research - A National Instruments Brand. *USRP Bus Series*. https://www.ettus.com/product-categories/usrp-bus-series/. Accessed: 2020/07/31.

[Fed02] Federal Communications Commission (FCC). *Revision of Part 15 of the Commission's Rules Regarding Ultra-Wideband Transmission Systems* First Report and Order. Feb. 2002.

[FZH62] R. Frank, S. Zadoff, and R. Heimiller. "Phase Shift Pulse Codes With Good Periodic Correlation Properties (Corresp.)" In: *IRE Transactions on Information Theory* 8.6 (1962), pp. 381–382.

[FJ18] H. Frid and B. L. G. Jonsson. "Determining Installation Errors for DOA Estimation with Four-Quadrant Monopulse Arrays by Using Installed Element Patterns". In: *2018 2nd URSI Atlantic Radio Science Meeting (AT-RASC)*. 2018, pp. 1–4.

[Fri46] H. T. Friis. "A Note on a Simple Transmission Formula". In: *Proceedings of the IRE* 34.5 (1946), pp. 254–256.

[GR17] O. Georgiou and U. Raza. "Low Power Wide Area Network Analysis: Can LoRa Scale?" In: *IEEE Wireless Communications Letters* 6.2 (2017), pp. 162–165.

[Gha+18] G. Ghatak et al. "Positioning Data-Rate Trade-Off in mm-Wave Small Cells and Service Differentiation for 5G Networks". In: *2018 IEEE 87th Vehicular Technology Conference (VTC Spring)*. 2018, pp. 1–5.

[GM99] E. Gonen and J. M. Mendel. "Subspace-Based Direction Finding Methods". In: *Madisetti, VK and Williams DB, editeur, The Digital Signal Processing Handbook, chapitre* 62 (1999).

[GJ18] P. Gotthard and T. Jankech. "Low-Cost Car Park Localization Using RSSI in Supervised LoRa Mesh Networks". In: *2018 15th Workshop on Positioning, Navigation and Communications (WPNC)*. 2018, pp. 1–6.

[Gre] Great Scott Gadgets. *HackRF One*. https://greatscottgadgets.com/hackrf/one/. Accessed: 2020/07/31.

[Gro13] P. D. Groves. *Principles of GNSS, Inertial, and Multisensor Integrated Navigation Systems*. Artech House, 2013.

[GGD14] F. Guidi, A. Guerra, and D. Dardari. "Millimeter-Wave Massive Arrays for Indoor SLAM". In: *2014 IEEE International Conference on Communications Workshops (ICC)*. 2014, pp. 114–120.

[Guo+11] S. Guo et al. “A novel density-based geolocation algorithm for a noncooperative radio emitter using power difference of arrival”. In: *Wireless Sensing, Localization, and Processing VI*. Vol. 8061. International Society for Optics and Photonics. 2011, 80610E.

[Hat80] M. Hata. “Empirical Formula for Propagation Loss in Land Mobile Radio Services”. In: *IEEE Transactions on Vehicular Technology* 29.3 (1980), pp. 317–325.

[He+03] T. He et al. “Range-Free Localization Schemes For Large Scale Sensor Networks”. In: *Proceedings of the 9th annual international conference on Mobile computing and networking*. ACM. 2003, pp. 81–95.

[HBLR17] S. Hu, A. Berg, X. Li, and F. Rusek. “Improving the Performance of OTDOA Based Positioning in NB-IoT Systems”. In: *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*. 2017, pp. 1–7.

[HFJK19] C. Hungar, J. Fricke, S. Juergens, and F. Koester. “Detection of Feature Areas for Map-based Localization Using LiDAR Descriptors”. In: *16th Workshop on Positioning, Navigation and Communications (WPNC)*. 2019.

[Huy+19] K. Huy et al. “iLoc: A Low-Cost Low-Power Outdoor Localization System for Internet of Things”. In: *GlobeCom 2019*. 2019.

[IRM15] A. Ibrahim, S. K. A. Rahim, and H. Mohamad. “Performance Evaluation of RSS-based WSN Indoor Localization Scheme using Artificial Neural Network SchemesJahn,” in: *2015 IEEE 12th Malaysia International Conference on Communications (MICC)*. 2015, pp. 300–305.

[IEE13] IEEE. “IEEE Standard for Local and metropolitan area networks— Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)—Amendment 5: Physical Layer Specifications for Low Energy, Critical Infrastructure Monitoring Networks.” In: *IEEE Std 802.15.4k-2013 (Amendment to IEEE Std 802.15.4-2011 as amended by IEEE Std 802.15.4e-2012, IEEE Std 802.15.4f-2012, IEEE Std 802.15.4g-2012, and IEEE Std 802.15.4j-2013)* (2013), pp. 1–149.

[Ing] Ingenu. *Random Phase Multiple Access (RPMA)*. https://www.ingenu.com/. Accessed: 2020/07/31.

[Inn+16] A. Innac et al. “Reliability testing for multiple GNSS measurement outlier detection”. In: *2016 European Navigation Conference (ENC)*. 2016, pp. 1–8.

[ITU97] ITU. *Rec. ITU-R M.1225 1, Recommendation ITU-R M.1225, Guidelines For Evaluation Of Radio Transmission Technologies For IMT-2000*. International Telecommunication Union (ITU), 1997.

[JWI11] B. Jackson, S Wang, and R Inkol. “Emitter geolocation estimation using power difference of arrival”. In: *Defence R&D Canada Technical Report DRDC Ottawa TR* 40 (2011), p. 51.

[JBH96] A. Jahn, H. Bischl, and G. Heiss. “Channel Characterisation for Spread Spectrum Satellite Communications”. In: *Proceedings of ISSSTA’95 International Symposium on Spread Spectrum Techniques and Applications*. Vol. 3. 1996, 1221–1226 vol.3.

[JABW18] T. Janssen, M. Aernouts, R. Berkvens, and M. Weyn. “Outdoor Fingerprinting Localization Using Sigfox”. In: *2018 International Conference on Indoor Positioning and Indoor Navigation (IPIN)*. 2018, pp. 1–6.

[JWB17] T. Janssen, M. Weyn, and R. Berkvens. “Localization in Low Power Wide Area Networks Usering Wi-Fi Fingerprints”. In: *Applied Sciences* 7.9 (2017), p. 936.

[JYL01] Y. Jeong, H. You, and C. Lee. “Calibration of NLOS Error for Positioning Systems”. In: *IEEE VTS 53rd Vehicular Technology Conference, Spring 2001. Proceedings (Cat. No.01CH37202)*. Vol. 4. 2001, 2605–2608 vol.4.

[Jim+16] E. Jimenez et al. “Investigation on Radio Wave Propagation in Shallow Seawater: Simulations and Measurements”. In: *2016 IEEE Third Underwater Communications and Networking Conference (UComms)*. 2016, pp. 1–5.

[KH06] E. Kaplan and C. Hegarty. *Understanding GPS: Principles and Applications*. Second Edition. Artech House, 2006.

[Kar+11] Y. Karisan et al. “Range Estimation in Multicarrier Systems in the Presence of Interference: Performance Limits and Optimal Signal Design”. In: *IEEE Transactions on Wireless Communications* 10.10 (2011), pp. 3321–3331.

[Kay93] S. M. Kay. *Fundamentals of Statistical Signal Processing: Estimation Theory*. 1993.

[KRJd19] T. Kazaz, R. T. Rajan, G. J. M. Janssen, and A. v. der Veen. “Multiresolution Time-of-arrival Estimation from Multiband Radio Channel Measurements”. In: *ICASSP 2019 - 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. 2019, pp. 4395–4399.

[Kaz+18] T. Kazaz et al. “Joint Ranging and Clock Synchronization for Dense Heterogeneous IoT Networks”. In: *2018 52nd Asilomar Conference on Signals, Systems, and Computers*. 2018, pp. 2169–2173.

[KOL15] S. Kim, D. Oh, and J. Lee. “Joint DFT-ESPRIT Estimation for TOA and DOA in Vehicle FMCW Radars”. In: *IEEE Antennas and Wireless Propagation Letters* 14 (2015), pp. 1710–1713.

[KNT00] E. M. Knorr, R. T. Ng, and V. Tucakov. “Distance-based outliers: algorithms and applications”. In: *The VLDB Journal* 8.3 (2000), pp. 237–253. URL: https://doi.org/10.1007/s007780050006.

[Koi+20] R. Koirala et al. “Simultaneous Localization and Mapping in Millimeter Wave Networks with Angle Measurements”. In: *submitted to IEEE ICC, Dublin*. 2020.

[Kor+18] M. Korb et al. “A Dual-Mode NB-IoT and EC-GSM RF-SoC Achieving -128-dBm Extended-Coverage and Supporting OTDOA and A-GPS Positioning”. In: *ESSCIRC 2018 - IEEE 44th European Solid State Circuits Conference (ESSCIRC)*. 2018, pp. 286–289.

[KC94] H. Krim and J. H. Cozzens. “A Data-Based Enumeration Technique for Fully Correlated Signals”. In: *IEEE Transactions on Signal Processing* 42.7 (1994), pp. 1662–1668.

[Lac+17] D. Lachartre et al. “A TCXO-Less 100Hz-Minimum-Bandwidth Transceiver for Ultra-Narrow-Band Sub-GHz IoT Cellular Networks”. In: *2017 IEEE International Solid-State Circuits Conference (ISSCC)*. 2017, pp. 134–135.

[LRV11] R. Lacoste, M. Robiolle, and X. Vital. *L’ecoconception en electronique*. Dunod, 2011.

[LZP11] S. Lanzisera, D. Zats, and K. S. J. Pister. “Radio Frequency Time-of-Flight Distance Measurement for Low-Cost Wireless Sensor Localization”. In: *IEEE Sensors Journal* 11.3 (2011), pp. 837–845.

[Lao+18] C. Laoudias et al. “A Survey of Enabling Technologies for Network Localization, Tracking, and Navigation”. In: *IEEE Communications Surveys Tutorials* 20.4 (2018), pp. 3607–3644.

[Las14] T. Lassen. *White paper: Long-range RF communication: Why narrowband is the de facto standard*. Texas Instruments. 2014.

[Le 19] K. Le Déroff. “Conception d’une Architecture de Test et Analyse Comparative de Systèmes de Mesures de Distance par Ondes Radio Bande Étroite”. MA thesis. Université de Savoie Mont-Blanc and CEA-Leti Grenoble, 2019.

[LVST08] A. Ledeczi, P. Volgyesi, J. Sallai, and R. Thibodeaux. “A Novel RF Ranging Method”. In: *2008 International Workshop on Intelligent Solutions in Embedded Systems*. 2008, pp. 1–12.

[Lei15] E. Leitinger. “Cognitive Indoor Positioning and Tracking using Multipath Channel Information”. PhD thesis. Graz University of Technology, 2015.

[LPCY06] J. Li, L. Pei, M. Cao, and D. Yu. “Super-Resolution Time Delay Estimation Algorithm Based on the Frequency Domain Channel Model in OFDM Systems”. In: *2006 6th World Congress on Intelligent Control and Automation*. Vol. 1. 2006, pp. 5144–5148.

[Lia+18] F. Liang et al. “A Survey on Big Data Market: Pricing, Trading and Protection”. In: *IEEE Access* 6 (2018), pp. 15132–15154.

[LF14] W. Liao and A. Fannjiang. “MUSIC for Single-Snapshot Spectral Estimation: Stability and Super-resolution”. In: *CoRR* abs/1404.1484 (2014). arXiv: 1404.1484.

[Lin+17] X. Lin et al. “Positioning for the Internet of Things: A 3GPP Perspective”. In: *IEEE Communications Magazine* 55.12 (2017), pp. 179–185.

[Lon19] Longman. *Longman Dictionary of Contemporary English Online*. 2019. URL: https://www.ldoceonline.com/.

[Lor] Lora Alliance. *What is the LoRaWAN Specification?* https://lora-alliance.org/about-lorawan. Accessed: 2020/07/31.

[LoR18] LoRaAlliance. *Geolocation Whitepaper*. https://lora-alliance.org/resource-hub/lora-alliance-geolocation-whitepaper. Accessed: 2020/07/31. 2018.

[Loy99] M. Loy. *Understanding and Enhancing Sensitivity in Receivers for Wireless Applications*. Texas Instrument, Wireless Communication Business Unit, Technical Brief SWRA030. 1999.

[Lu07] D. Lu. “Multipath Mitigation in TOA Estimation Based on AOA”. PhD thesis. Department of Electrical and Computer Engineering, Calgary, Alberta, 2007.

[Luo+19] N. C. Luong et al. “Applications of Deep Reinforcement Learning in Communications and Networking: A Survey”. In: *IEEE Communications Surveys Tutorials* 21.4 (2019), pp. 3133–3174.

[MDDU17] J. Maceraudi, F. Dehmas, B. Denis, and B. Uguen. “Multipath-Aided Direct Path ToA Reconstruction for Integrated UWB Receivers in Generalized NLoS”. In: *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)*. 2017, pp. 1–5.

[Mal+19] M. E. Malmström et al. “5G Positioning -A Machine Learning Approach”. In: *16th Workshop on Positioning, Navigation and Communications (WPNC)*. 2019.

[MHH18] Q. Mao, F. Hu, and Q. Hao. “Deep Learning for Intelligent Wireless Networks: A Comprehensive Survey”. In: *IEEE Communications Surveys Tutorials* 20.4 (2018), pp. 2595–2621.

[MGWW10] S. Marano, W. M. Gifford, H. Wymeersch, and M. Z. Win. “NLOS Identification and Mitigation for Localization based on UWB Experimental Data”. In: *IEEE Journal on Selected Areas in Communications* 28.7 (2010), pp. 1026–1035.

[Mar+05] M. Maróti et al. “Radio Interferometric Geolocation”. In: *Proceedings of the 3rd international conference on Embedded networked sensor systems*. ACM. 2005, pp. 1–12.

[McL97] B. McLarnon. “VHF/UHF/microwave radio propagation: A primer for digital experimenters”. In: *TAPR/ARRL Digital Communications Conference*. 1997.

[Mei14] P. Meissner. “Multipath-Assisted Indoor Positioning”. PhD thesis. Graz University of Technology, 2014.

[MM97] U. Mengali and M. Morelli. “Data-Aided Frequency Estimation for Burst Digital Transmission”. In: *IEEE Transactions on Communications* 45.1 (1997), pp. 23–25.

[Mol+06] A. F. Molisch et al. “A Comprehensive Standardized Model for Ultrawideband Propagation Channels”. In: *IEEE Transactions on Antennas and Propagation* 54.11 (2006), pp. 3151–3166.

[MS15] M. V. Moreno and A. F. Skarmeta. “An Indoor Localization System Based on 3D Magnetic Fingerprints for Smart Buildings”. In: *The 2015 IEEE RIVF International Conference on Computing Communication Technologies - Research, Innovation, and Vision for Future (RIVF)*. 2015, pp. 186–191.

[Myr] Myriad RF. *LimeSDR USB*. https://myriadrf.org/projects/component/limesdr/. Accessed: 2020/07/31.

[Nan] Nanotron. *Location-Aware IoT Sensors*. https://nanotron.com/. Accessed: 2020/07/31.

[NCAC18] A. Navarro, W. Cruz, C. Amu, and Y. Castano. “Broadcast Emitters Localization Using Power Difference of Arrival”. In: *2018 IEEE MTT-S Latin America Microwave Conference (LAMC 2018)*. 2018, pp. 1–3.

[NGM15] NGMN 5G Initiative. *5G White Paper*. 2015.

[NN01] D. Niculescu and B. Nath. “Ad Hoc Positioning System (APS)”. In: *GLOBECOM’01. IEEE Global Telecommunications Conference (Cat. No.01CH37270)*. Vol. 5. 2001, 2926–2931 vol.5.

[Nii+19] A. Niitsoo et al. “A Deep Learning Approach to Position Estimation from Channel Impulse Responses”. In: *Sensors* 19.5 (2019), p. 1064.

[Obj] Objenious Bouygues Telecom. *Le Reseau Dedie Aux Objets Connectes*. https://objenious.com/reseau/. Accessed: 2020/07/31.

[OSMD18] M. N. Ochoa, L. Suraty, M. Maman, and A. Duda. “Large Scale LoRa Networks: From Homogeneous to Heterogeneous Deployments”. In: *2018 14th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. 2018, pp. 192–199.

[ODDM17] B. Oniga, V. Dadarlat, E. De Poorter, and A. Munteanu. “Analysis, design and implementation of secure LoRaWAN sensor networks”. In: *2017 13th IEEE International Conference on Intelligent Computer Communication and Processing (ICCP)*. 2017, pp. 421–428.

[Pal+16] M. R. Palattella et al. “Internet of Things in the 5G Era: Enablers, Architecture, and Business Models”. In: *IEEE Journal on Selected Areas in Communications* 34.3 (2016), pp. 510–527.

[Pan17] Panasonic. *microSD/SDHC Memory Card, Consumer Plus pSLC Model - RP-SMPE32DA1*. 2017.

[PMCM15] M. Passafiume, S. Maddio, A. Cidronali, and G. Manes. “MUSIC algorithm for RSSI-based DoA estimation on standard IEEE 802.11/802.15. x systems”. In: *World Sci. Eng. Acad. Soc. Trans. Signal Process* 11 (2015), pp. 58–68.

[PRK85] A. Paulraj, R. Roy, and T. Kailath. "Estimation Of Signal Parameters Via Rotational Invariance Techniques- Esprit". In: *Nineteeth Asilomar Conference on Circuits, Systems and Computers, 1985*. 1985, pp. 83–89.

[Pea05] K. Pearson. "Das Fehlergesetz Und Seine Verallgemeinerungen Durch Fechner Und Pearson. A Rejoinder". In: *Biometrika* 4.1-2 (1905), pp. 169–212.

[PO97] D. Peavey and T. Ogumfunmi. "The Single Channel Interferometer Using a Pseudo-Doppler Direction Finding System". In: *1997 IEEE International Conference on Acoustics, Speech, and Signal Processing*. Vol. 5. 1997, 4129–4132 vol.5.

[Pen17a] M. Peng. "System And Method For Robust And Accurate RSSI Based Location Estimation". Pat. 3 173 807. 2017.

[Pen17b] M. Peng. "System And Method For Robust And Efficient TDOA Based Location Estimation In The Presence Of Various Multipath Delay". Pat. 3 173 809. 2017.

[Pen18] M. Peng. "Positioning System And Method With Multipath Mitigation". Pat. 404 440. 2018.

[PSSV09a] M. Pichler, S. Schwarzer, A. Stelzer, and M. Vossiek. "Multi-Channel Distance Measurement With IEEE 802.15.4 (ZigBee) Devices". In: *IEEE Journal of Selected Topics in Signal Processing* 3.5 (2009), pp. 845–859.

[PSSV09b] M. Pichler, S. Schwarzer, A. Stelzer, and M. Vossiek. "Positioning with moving IEEE 802.15.4 (ZigBee) transponders". In: *2009 IEEE MTT-S International Microwave Workshop on Wireless Sensing, Local Positioning, and RFID*. 2009, pp. 1–4.

[Pod+18] N. Podevijn et al. "TDoA-Based Outdoor Positioning with Tracking Algorithm in a Public LoRa Network". In: *Wireless Communications and Mobile Computing* (2018).

[Pod+19] N. Podevijn et al. "Experimental TDoA Localisation in Real Public LoRa Networks". In: *2019 International Conference on Indoor Positioning and Indoor Navigation (IPIN)*. 2019.

[PS11] A. Povalac and J. Sebesta. "Phase Difference of Arrival Distance Estimation for RFID Tags in Frequency Domain". In: *2011 IEEE International Conference on RFID-Technologies and Applications*. 2011, pp. 188–193.

[Pro01] J. G. Proakis. *Digital Communications*. Ed. by F. Edition. McGraw-Hill Higher Education, 2001.

[Rad+17] K. Radnosrati et al. "Performance of OTDOA Positioning in Narrowband IoT Systems". In: *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*. 2017, pp. 1–7.

[Raj+18] S. Rajendran et al. "Deep Learning Models for Wireless Signal Classification With Distributed Low-Cost Spectrum Sensors". In: *IEEE Transactions on Cognitive Communications and Networking* 4.3 (2018), pp. 433–445.

[Rak17] Rakon. *Single chip oscillator RPT7050A*. 2017.

[Rap+96] T. S. Rappaport et al. *Wireless Communications: Principles and Practice*. Vol. 2. prentice hall PTR New Jersey, 1996.

[RKS17] U. Raza, P. Kulkarni, and M. Sooriyabandara. "Low Power Wide Area Networks: An Overview". In: *IEEE Communications Surveys Tutorials* 19.2 (2017), pp. 855–873.

[Rob19] S. Robinson. *Semtech SX1280 2.4GHz LoRa Ranging Tranceivers*. https://github.com/LoRaTracker/SX1280_Testing. Accessed: 2020/07/31. 2019.

[Röm03] K. Römer. "The Lighthouse Location System for Smart Dust". In: *Proceedings of the 1st international conference on Mobile systems, applications and services*. ACM. 2003, pp. 15–30.

[Rot17] Y. Roth. "The Physical Layer for Low Power Wide Area Networks: A Study of Combined Modulation and Coding Associated with an Iterative Receiver". PhD thesis. Université Grenoble Alpes, 2017.

[RK89] R. Roy and T. Kailath. "ESPRIT-Estimation of Signal Parameters Via Rotational Invariance Techniques". In: *IEEE Transactions on Acoustics, Speech, and Signal Processing* 37.7 (1989), pp. 984–995.

[SGG08] Z. Sahinoglu, S. Gezici, and I. Guvenc. "Ultra-Wideband Positioning Systems". In: *Cambridge, New York* (2008).

[SCRP19] H. Sallouha, A. Chiumento, S. Rajendran, and S. Pollin. "Localization in Ultra Narrow Band IoT Networks: Design Guidelines and Trade-Offs". In: *IEEE Internet of Things Journal* (2019), pp. 1–1.

[Sch86] R. Schmidt. “Multiple Emitter Location and Signal Parameter Estimation”. In: *IEEE Transactions on Antennas and Propagation* 34.3 (1986), pp. 276–280.

[SD07] S. Schon and F. DilBner. “Challenges for GNSS-based high precision positioning – some geodetic aspects”. In: *2007 4th Workshop on Positioning, Navigation and Communication*. 2007, pp. 229–237.

[SZW15] Y. Schröder, G. von Zengen, and L. Wolf. “Poster: NLOS-aware Localization Based on Phase Shift Measurements”. In: *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*. ACM. 2015, pp. 224–226.

[SRW18] Y. Schroeder, D. Reimers, and L. Wolf. “Accurate and Precise Distance Estimation from Phase-Based Ranging Data”. In: *2018 International Conference on Indoor Positioning and Indoor Navigation (IPIN)*. 2018, pp. 1–8.

[SVPS08] S. Schwarzer, M. Vossiek, M. Pichler, and A. Stelzer. “Precise distance measurement with IEEE 802.15.4 (ZigBee) devices”. In: *2008 IEEE Radio and Wireless Symposium*. 2008, pp. 779–782.

[Sch11] S. Schwarzer. “Entwicklung eines industriellen Funkortungssystems basierend auf der kohaerenten Kombination von Kommunikationssignalen mit IEEE-802.15.4-Geraeten”. PhD thesis. Technischen Universitaet Clausthal, 2011.

[SS10] S. Schwarzer and C. Saisenberger. “Verfahren zur Ortung von drahtlos kommunizierenden Funkteilnehmern”. Pat. 10 2008 034 567. 2010.

[SDR16] C. R. Sekhar, V. S. I. Dutt, and G. S. Rao. “GDoP estimation using Simulated Annealing for GPS and IRNSS combined constellation”. In: *Engineering Science and Technology, an International Journal* 19.4 (2016), pp. 1881 –1886. URL: http://www.sciencedirect.com/science/article/pii/S221509861630739X.

[Sel14] O. Seller. “Ranging and Positioning System”. Pat. 2 767 847. 2014.

[Sel16] O. Seller. “Low Complexity, Low Power And Long Range Radio Receiver”. Pat. 3 264 622. 2016.

[Sel18] O. Seller. “Method And System Of Timing And Localizing A Radio Signal”. Pat. 3 273 607. 2018.

[SF13] L. Sellier and C. Fourtet. “Procede De Synchronisation De Mesures De Temps Realisees Dans Un Reseau De Radiocommunication Aux Fins De Geolocalisation”. Pat. 2986680. 2013.

[SF16] L. Sellier and C. Fourtet. “Method For Synchronizing Time Measurements Carried Out In A Radio Communication Network For Geolocation Purposes”. Pat. 9341701. 2016.

[Sema] Semtech. *SX1257 - Low Power Digital I and Q RF Multi-PHY Mode Analog Front End 860-1000 MHz*. https://www.semtech.com/uploads/documents/DS_SX1257_V1.2.pdf. Accessed: 2020/07/31.

[Semb] Semtech. *SX1280DVK1ZHP Development Kit for the SX1280 and SX1281 Transceivers*. https://www.semtech.com/products/wireless-rf/24-ghz-transceivers/sx1280. Accessed: 2020/07/31.

[Semc] Semtech. *SX1301 - Digital Baseband Chip for outdoor LoRaWAN macro gateways*. https://www.semtech.com/uploads/documents/sx1301.pdf. Accessed: 2020/07/31.

[Sem15] Semtech. *Application Note: LoRa Modulation Basics*. 2015.

[Sem16] Semtech. *SX1276/77/78/79 - 137 MHz to 1020 MHz Low Power Long Range Transceiver*. http://www.semtech.com/images/datasheet/sx1276.pdf. Accessed: 2020/07/31. Aug. 2016.

[Sem17a] Semtech. *Application Note: An Introduction to Ranging with the SX1280 Transceiver*. 2017.

[Sem17b] Semtech. *SX1280/SX1281 Long Range, Low Power, 2.4 GHz Transceiver with Ranging Capability*. 2017.

[Sha48] C. Shannon. “A Mathematical Theory of Communication”. In: *The Bell System Technical Journal* 27.3 (1948), pp. 379–423.

[Sig] Sigfox. *Sigfox, a 0G Network*. https://www.sigfox.com/. Accessed: 2020/07/31.

[Sig17] Sigfox. *Sigfox Spot’it, the simplest and most efficient IoT location service*. https://www.sigfox.com/en/sigfox-spot-it. 2017.

[Sil16] Silicon Labs. *High-Performance, Low-Current Transceiver: Si4464/63/61/60*. 2016.

[Sim+06] Y. Simard et al. “Development and experimentation of a satellite buoy network for real-time acoustic localization of whales in the St. Lawrence”. In: *OCEANS 2006*. 2006, pp. 1–6.

[Sit+11] Y. L. Sit et al. “The OFDM Joint Radar-Communication System: An Overview”. In: *The Third International Conference on Advances in Satellite and Space Communications, Budapest, Hungary* (2011).

[Sit17] Y. L. Sit. "MIMO OFDM Radar-Communication System with Mutual Interference Cancellation". PhD thesis. Karlsruhe Institute of Technology, 2017.

[Sko90] M. Skolnik. *Radar Handbook*. 2nd ed. McGrawHill, 1990.

[Sky18] Skyworks. *SKY66423-11: 860 to 930 MHz RF Front-End Module*. 2018.

[SA87] J. Smith and J. Abel. "Closed-Form Least-Squares Source Location Estimation From Range-Difference Measurements". In: *IEEE Transactions on Acoustics, Speech, and Signal Processing* 35.12 (1987), pp. 1661–1669.

[Spi01] M. A. Spirito. "On the Accuracy of Cellular Mobile Station Location Estimation". In: *IEEE Transactions on Vehicular Technology* 50.3 (2001), pp. 674–685.

[STM16] STMicroelectronics. *S2-LP Ultra-low power, high performance, sub-1GHz transceiver*. http://www.st.com/content/ccc/resource/technical/document/datasheet/group3/bd/26/62/81/3d/86/4d/15/DM00339133/files/DM00339133.pdf/jcr:content/translations/en.DM00339133.pdf. Nov. 2016.

[Sun+17] M. Sun et al. "Signal Subspace Smoothing Technique for Time Delay Estimation Using MUSIC Algorithm". In: *Sensors* 17.12 (2017), p. 2868.

[SB+98] R. S. Sutton, A. G. Barto, et al. *Introduction to reinforcement learning. Vol. 135*. 1998.

[Tai17] Taitien. *3.2 x 2.5 mm SMD Voltage Controlled Temperature Compensated Crystal Oscillator (VCTCXO) - TX Type*. 2017.

[TKL11] Y. Taniguchi, T. Kitani, and K. Leibnitz. "A uniform airdrop deployment method for large-scale wireless sensor networks". In: *International Journal of Sensor Networks* 9.3-4 (2011), pp. 182–191.

[Tex16] Texas Instruments. *CC1125 Ultra-High Performance RF Narrowband Transceiver*. http://www.ti.com/lit/ds/swrs120e/swrs120e.pdf. 2016.

[The] The Things Network. *Building a global open LoRaWAN network*. https://www.thethingsnetwork.org/. Accessed: 2020/07/31.

[TVVH16] X. L. Tran, J. Vesely, S. Van Doan, and P. Hubacek. "UHF/C-band Testing of AOA Estimation Using MUSIC Algorithm". In: *2016 New Trends in Signal Processing (NTSP)*. 2016, pp. 1–6.

[Ubl] Ublox. *High precision GNSS performance for the mass market: NEO-M8P series*. https://www.u-blox.com/en/product/neo-m8p-series. Accessed: 2020/07/31.

[URGW16] M. Ulmschneider, R. Raulefs, C. Gentner, and M. Walter. "Multipath Assisted Positioning in Vehicular Applications". In: *2016 13th Workshop on Positioning, Navigation and Communications (WPNC)*. 2016, pp. 1–6.

[Uni] University Grenoble Alpes. *Need for IoT - Anticipate and support sustainable transition in nanoelectronic industry*. https://need.univ-grenoble-alpes.fr/. Accessed: 2020/07/31.

[VT04] H. L. Van Trees. *Detection, Estimation, and Modulation Theory*. John Wiley and Sons, 2004.

[Var12] U. Varshney. "4G Wireless Networks". In: *IT Professional* 14.5 (2012), pp. 34–39.

[VKK16] D. Vasisht, S. Kumar, and D. Katabi. "Decimeter-Level Localization with a Single WiFi Access Point". In: (2016).

[Vig16] J. R. Vig. *Quartz Crystal Resonators and Oscillators - For Frequency Control and Timing Applications - A Tutorial*. https://ieee-uffc.org/download/quartz-crystal-resonators-and-oscillators-for-frequency-control-and-timing-applications-a-tutorial-2/. Accessed: 2020/07/31. 2016.

[VFF19] C. Villien, A. Frassati, and B. Flament. "Evaluation of An Indoor Localization Engine". In: *2019 International Conference on Indoor Positioning and Indoor Navigation (IPIN)*. 2019, pp. 1–8.

[WA86] F. L. Walls and D. W. Allan. "Measurements of Frequency Stability". In: *Proceedings of the IEEE* 74.1 (1986), pp. 162–168.

[Wei] Weightless. *Weightless*. http://www.weightless.org/. Accessed: 2020/07/31.

[Wi6] Wi6Labs. *Iot And Geo-Tracking : The Feedback Of A French Start-Up From Bretagne*. http://www.wi6labs.com/2018/08/02/iot-et-geolocalisation-le-retour-dexperience-dune-startup-bretonne/. Accessed: 2020/07/31.

[WdDC19a] F. Wolf, S. de Rivaz, F. Dehmas, and J. P. Cances. "Field Trials on Accurate Multi-Channel Ranging for Narrowband LPWAN". In: 2019, pp. 1–6.

[Wol+18a] F. Wolf et al. “Coherent Multi-Channel Ranging for Narrowband LPWAN: Simulation and Experimentation Results”. In: *15th Workshop on Positioning, Navigation and Communications (WPNC)*. 2018, pp. 1–6.

[Wol+18b] F. Wolf et al. “Improved Multi-Channel Ranging Precision Bound for Narrowband LPWAN in Multipath Scenarios”. In: *2018 IEEE Wireless Communications and Networking Conference (WCNC)*. 2018, pp. 1–6.

[WdDC19b] F. Wolf, S. de Rivaz, F. Dehmas, and J.-P. Cances. “Méthode d’Estimation de Distance dans un Réseau LPWA et Méthode d’Estimation de Position Associée”. FR. Pat. Application N° 1910165. 2019.

[Wd15] F. Wolf and S. de Rivaz. *Characterisation of the Long Range (LoRa) technology’s physical layer and medium access control layer study of a demonstrator Long Range Wide Area Network (LoRaWAN)*. Tech. rep. Commissariat a l’energie atomique et aux energies alternatives (CEA) Centre de Grenoble - France, 2015.

[WSdD19] F. Wolf, M. Sana, S. de Rivaz, and F. Dehmas. “Méthode d’Estimation de Distance dans un Réseau LPWA et Méthode d’Estimation de Position Associée”. FR. Pat. Application N° 1910164. 2019.

[Wol+19a] F. Wolf et al. “Benchmarking of Narrowband LPWA Physical Layer Ranging Technologies”. In: *16th Workshop on Positioning, Navigation and Communications (WPNC)*. 2019.

[Wol+19b] F. Wolf et al. “Comparison of Multi-Channel Ranging Algorithms for Narrowband LPWAN Localization”. In: *2019 The International Symposium on Ubiquitous Networking (UNet)*. 2019, pp. 1–6.

[Xil15] Xilinx. *Zynq-7000 All Programmable SoC (Z-7030, Z-7035, Z-7045, and Z-7100): DC and AC Switching Characteristics*. https://www.xilinx.com/support/documentation/data_sheets/ds191-XC7Z030-XC7Z045-data-sheet.pdf. 2015.

[Yan+19] J. Yan et al. “Joint localisation and tracking for autonomous underwater vehicle: a reinforcement learning-based approach”. In: *IET Control Theory Applications* 13.17 (2019), pp. 2856–2865.

[Zap+18] A. Zappone et al. “Model-Aided Wireless Artificial Intelligence: Embedding Expert Knowledge in Deep Neural Networks Towards Wireless Systems Optimization”. In: *arXiv preprint arXiv:1808.01672* (2018).

[Zha+19] G. Zhang et al. “Millimeter-Wave Channel Characterization in Large Hall Scenario at the 10 and 28 GHz Bands”. In: *2019 13th European Conference on Antennas and Propagation (EuCAP)*. 2019, pp. 1–4.

[ZSL13] J. Zhang, J. Salmi, and E. Lohan. “Analysis of Kurtosis-Based LOS/NLOS Identification Using Indoor MIMO Channel Measurement”. In: *IEEE Transactions on Vehicular Technology* 62.6 (2013), pp. 2871–2874.

[Zha+16] Y.-X. Zhang et al. “A novel monopulse angle estimation method for wideband LFM radars”. In: *Sensors* 16.6 (2016), p. 817.

[ZYLS06] F. Zhao, W. Yao, C. C. Logothetis, and Y. Song. “Comparison of Super-Resolution Algorithms for TOA Estimation in Indoor IEEE 802.11 Wireless LANs”. In: *2006 International Conference on Wireless Communications, Networking and Mobile Computing*. 2006, pp. 1–5.

[Zhe+19] C. Zheng et al. “Copula-Based Interference Models for IoT Wireless Networks”. In: *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*. 2019, pp. 1–6.

[Zhu+18] Y. Zhuang et al. “A Survey of Positioning Systems Using Visible LED Lights”. In: *IEEE Communications Surveys Tutorials* 20.3 (2018), pp. 1963–1988.

[ZVL17] K. Zoubert-Ousseni, C. Villien, and F. Le Gland. “Post-processing optimization of piecewise indoor trajectories based on IMU and RSS measurements”. In: *2017 International Conference on Indoor Positioning and Indoor Navigation (IPIN)*. 2017, pp. 1–8.

Multi-Channel Ranging System for the Localization of Wireless Connected Objects in Low Power Wide Area Networks: from Modeling to Field Trials

The Internet of Things (IoT) is an enabler to new applications, such as smart metering and environmental monitoring, intended to address current and future societal and ecological challenges. Things, possibly mobile or in distant locations, require wireless connectivity for data collection and remote control. Low Power Wide Area (LPWA) networks provide city-scale long-range, narrowband radio transmissions respecting the energy constraints of battery-powered low-cost objects.

Being capable to localize these objects will add value to their data, enables tracking applications and is therefore a demanded and recent research topic. Precise and accurate radio signal delay based positioning without integrating additional hardware but taking advantage of intrinsic wireless communication signals is appealing in terms of device complexity, cost and energy consumption. However, radio localization within LPWA networks is challenging due to narrowband transmissions, resulting in a lack of delay precision as well as due to radio propagation channels, which degrade the accuracy of location estimates.

This work addresses both challenges by investigating a multi-channel ranging system for LPWA networks. Coherently combining multiple sequentially transmitted narrowband signals on different radio channels improves delay estimation precision and allows resolving multipath channels for refined positioning accuracy. This scheme, based on instantaneous narrowband signals, conserves the LPWA long-range feature and is hence compatible with LPWA networks. A detailed signal model considering hardware imperfections as well as the required protocol exchanges for time, frequency and phase synchronization is developed. Based on this model, the requirements on radio transceiver architectures regarding the necessary phase coherence for multi-channel ranging are discussed. Lower bounds on the ranging precision are derived for both, free-space and multipath propagation channels, illustrating the improved precision compared to narrowband single channel ranging. Numerical simulations of radio signals for the two-way multi-channel ranging protocol illustrate that the performance of developed range estimators attains the theoretical precision bound and pave the way towards implementation. A flexible Software Defined Radio (SDR) based demonstrator is implemented to validate simulation results. Field trials in real urban outdoor environments are in accordance with simulation results and prove how scalable multi-channel ranging, in combination with advanced signal processing methods, will be an enabler towards precise and accurate localization in LPWA networks.

Keywords: Internet of Things (IoT); Low Power Wide Area (LPWA); Radio localization; Ranging; Frequency hopping; Phase of Arrival (PoA); Coherent processing; Narrow-Band IoT (NB-IoT), LoRa, Sigfox

Système de Mesure Multicanaux de Distances pour la Localisation des Objets Connectés dans les Réseaux Longue Portée et Basse Consommation: de la Modélisation jusqu'aux Tests Terrain

L'Internet des objets (IoT, pour Internet of Things, en anglais) ouvre la porte vers la réalisation de nouvelles applications, telles que les compteurs intelligents et le suivi environnemental, destinées à adresser nos défis sociétaux et écologiques actuels et futurs. Les objets, possiblement mobiles ou distants, nécessitent une connectivité sans fil pour la centralisation des données et le contrôle à distance. Les réseaux longue portée et basse consommation (LPWA, pour Low Power Wide Area, en anglais) offrent des transmissions radio bande étroite avec une couverture à l'échelle typique d'une ville, tout en respectant les contraintes de consommation énergétique bas coût des objets.

Intégrer la possibilité de localiser ces objets ajouterait de la valeur à leurs données et permettrait leur suivi géographique. Voilà pourquoi c'est un domaine de recherche très actif actuellement. L'utilisation du temps de propagation des signaux radio de communication, sans intégration supplémentaire de modules matériels dédiés à la localisation, est une approche très intéressante pour la complexité, la consommation et le coût des objets. Néanmoins la radio localisation dans les réseaux LPWA pose des défis liés d'une part aux transmissions à bande étroite qui n'offrent pas une résolution temporelle suffisante et d'autre part aux canaux de propagation qui peuvent introduire des biais sur les estimées de position.

Cette thèse adresse ces défis en étudiant un système de mesure multicanaux de distance pour les réseaux LPWA. La combinaison cohérente des signaux bande étroite transmis séquentiellement sur des canaux différents améliore la précision d'estimation des temps de propagation et permet de résoudre en partie les multi-trajets pour une meilleure précision de localisation. Cette technique basée sur les signaux à bande instantanée étroite conserve la capacité longue portée des transmissions et reste compatible avec les réseaux LPWA. Un modèle détaillé prenant en compte les imperfections matérielles ainsi que les besoins protocolaires pour la synchronisation en temps, fréquence et phase est développé. Basé sur ce modèle, les variantes des architectures des émetteurs-récepteurs radios et leurs impacts sur la cohérence de phase pour l'estimation multicanaux de distance sont discutés. Les limites théoriques de précision sont dérivées pour la propagation en espace libre et dans des canaux de propagation multi-trajets, illustrant l'amélioration de précision possible entre l'approche multicanaux et l'approche monocanal pour l'estimation de distance. Des estimateurs de distance sont développés et appliqués aux signaux radio simulés afin de montrer que leurs performances atteignent les limites théoriques. Ces résultats de simulation sont validés avec des expérimentations menées avec un démonstrateur implémenté avec une radio logicielle (SDR, pour Software Defined Radio, en anglais). Les tests terrains réalisés en environnement urbain permettent de confirmer l'apport d'un système d'estimation multicanaux de distance, en combinaison avec du traitement de signal avancé, pour fournir une fonctionnalité de localisation intrinsèque et précise pour les réseaux LPWA.

Mots clés: Internet des objets (IoT); Réseaux longue portée et basse consommation (LPWA); Radio localisation; Estimation de distance; Sauts de fréquence; Phase d'arrivée (PoA); Traitement cohérent; Narrow-Band IoT (NB-IoT), LoRa, Sigfox