UAB
Universitat Autònoma de Barcelona

A study of time and angle-based 5G positioning through simulation and experimental platforms

Alda Xhafa

ADVERTIMENT. L'accés als continguts d'aquesta tesi queda condicionat a l'acceptació de les condicions d'ús establertes per la següent llicència Creative Commons:  https://creativecommons.org/licenses/?lang=ca

ADVERTENCIA. El acceso a los contenidos de esta tesis queda condicionado a la aceptación de las condiciones de uso establecidas por la siguiente licencia Creative Commons:  https://creativecommons.org/licenses/?lang=es

WARNING. The access to the contents of this doctoral thesis it is limited to the acceptance of the use conditions set by the following Creative Commons license:  https://creativecommons.org/licenses/?lang=en

UAB
Universitat Autònoma de Barcelona

Ph.D. Dissertation

A study of time and angle-based 5G positioning through simulation and experimental platforms

Author: Alda Xhafa

Thesis Advisors: Gonzalo Seco-Granados
José A. López-Salcedo

Doctoral Program in Electronic and Telecommunication Engineering
Universitat Autònoma de Barcelona (UAB)

Bellaterra, January 2024

Abstract

The demand for precise and reliable localization is growing rapidly, becoming a topic of high interest in logistics, emergency services, autonomous vehicles, localized sensing, and more. Global Navigation Satellite System (GNSS) has been the main technology used for positioning purposes, but it is known to suffer severe performance degradation in harsh environments, such as densely urbanized areas and indoor environments, where it is difficult to receive GNSS signals. This makes the use of GNSS alone unable to fulfill the demand of positioning accuracy at the cm level, which is required in many applications. Therefore, there have been continuous efforts in recent decades to find equally (or more) scalable and accurate positioning techniques. In this context, the current fifth generation (5G) cellular system has become an aiding source to provide alternative positioning technologies. 5G cellular networks are expected to significantly increase positioning performance through the provision of positioning accuracy down to the centimeter.

This thesis investigates time and angle-based 5G positioning techniques that can fulfill the high-accuracy positioning requirements in challenging environments. The study is done through simulation and experimental platforms providing valuable insights for the development of seamless indoor and outdoor positioning systems.

We start by proposing a methodology to perform simulations that are representative of real-world scenarios. Realistic base station locations and relevant use cases such as IoT and autonomous cars are considered. In particular, we addressed the challenges posed by accurate time synchronization and distance constraints in urban scenarios. Several techniques (from classical to more modern) have been implemented in the simulator and their performance has been analyzed, incorporating 5G network density to enhance accuracy. The results advance the understanding of 5G positioning, focusing on its potential and limitations. It is shown that the positioning accuracy is primarily dependent on the network density, narrow bandwidth, and synchronization issues.

Another factor that hampers the positioning accuracy is the presence of Non Line of Sight (NLoS) conditions. To overcome this problem, a mechanism for detecting NLoS conditions in cellular positioning is proposed. The proposed technique ensures the integrity of the position solution by identifying and excluding erroneous measurements. Beyond NLoS detection, this approach offers a more accurate evaluation of actual cellular positioning compared to the traditional assumptions of ideal propagation or mixing Line of Sight (LoS) and NLoS observations. Our results also emphasize the importance of balancing protection level size and integrity level, stressing the need for tailored algorithms for urban applications.

Additionally, this work introduces a hybrid algorithm for outdoor scenarios, especially effective in challenging environments like urban canyons. This technique consists of combining

timing-based and angle-based methods to leverage the strengths of both techniques and improving the positioning accuracy. An even better localization is achieved by combining the hybrid method with the abovementioned NLoS detection and exclusion mechanism. The study also demonstrates the advantages of using array antennas to enhance the positioning accuracy in deep urban settings.

Finally, in this work, we propose an experimental platform based on Software-Defined Radio (SDR) devices that aims to bridge the gap between simulations and real-world experiments. The objective is to provide accurate Angle of Arrival (AoA) estimation. The proposed platform helps to characterize the effects of propagation conditions, calibration, and array processing on 5G AoA estimation accuracy. Moreover, it seeks to provide insights and a systematic approach for conducting theoretical and experimental 5G localization studies through an accurate and robust AoA estimation process for 5G networks. The results showcase the potential of 5G signals for indoor and outdoor observable estimation and emphasize the practical impact of equipment behaviors.

In conclusion, with this dissertation, we provide insights into the challenges and promises of 5G positioning, propose practical solutions to some limitations that the technology is facing, and suggest directions for future standardization efforts.

Acknowledgements

I would like to express my sincere gratitude to all those who contributed to the completion of this PhD thesis.

First and foremost, I would like to thank my supervisors, Prof. Gonzalo Seco-Granados and Prof. José A. López-Salcedo, for their invaluable guidance, tireless patience in addressing my uncertainties, and encouragement in exploring new research directions independently. Their mentorship has been instrumental in making my PhD journey both productive and intellectually stimulating. I am also grateful for the excellent example they demonstrated as successful investigators and professors. Their enthusiasm for their work was contagious and served as a constant source of motivation, even during challenging phases of the thesis.

I would like to extend my appreciation to Jose del Peral-Rosado for providing me with the opportunity to conduct a three-month international exchange at the Airbus Space and Defense Investigation Center in Munich. The collaborative experience and essential knowledge gained during this period contributed to the realization of the experimental part of my thesis. Special thanks go to Anna from Open Labs UAB for facilitating the indoor experimentation and to Prof. Jordi Bonache for giving access to the anechoic chamber for antenna calibration. Without their support, certain experimental components would not have been possible.

The enjoyable experience of this PhD has been also thanks to the members of the SPCOMNAV group, past and present, including Sergi, Ning, Husnain, Rafa, Guillem, and Lucia. Their warm welcome and great company cultivated a productive working atmosphere. I extend a special thank you to Fran for invaluable assistance with USRPs and to Dani for engaging in fruitful discussions and lending an ear when needed. All these people, sometimes even without noticing, have contributed to the knowledge I gained over the years.

I am also grateful for the time spent with the members of the Navigation department at Airbus Defence, including Iven, François, Nils, Francesco, Pau, Silvia, Cat, Càndia, Oriol, Moritz, Jennifer, Alexandra, and many others. Their hospitality and friendship were a true pleasure.

Lastly, but certainly not least, I want to express my deep appreciation to my parents and sister for their support, encouragement to pursue my dreams, and invaluable advice during challenging moments. A special acknowledgment goes to my sister for always believing in me, even during times of doubt. This thesis is dedicated to her. I extend this gratitude to my extended family, including grandparents, uncles, aunts, and cousins, to Geri, and my dearest friends Melina, Tea, and Bora. Despite the physical distance, I felt their support throughout.

In closing, I extend my sincere thanks to my greatest supporter, my partner Manu. Your unconditional support and willingness to listen, even during challenging discussions about work, played an important role in concluding this thesis. I am grateful for your unconditional support,

and I am very happy to have convinced a physicist that engineering is no easy feat. Thank you for being there to enjoy life beyond work and research.

To all of you and to those whom I have not mentioned unintentionally, thank you from the bottom of my heart!

Alda Xhafa,
Barcelona, January 2024.

This work has been financed by the Ministry of Science, Innovation, and Universities through grant PRE2018-083748 (project TEC2017-89925-R).

Contents

Abstract **iii**

Acknowledgements **v**

List of Figures **xvi**

List of Tables **xviii**

Acronyms **xxiii**

Introduction **1**

Objectives . . . 2

Thesis outline and contributions . . . 3

1 5G NR positioning: overview and challenges **7**

1.1 5G use cases and requirements . . . 8

1.2 Standardization efforts . . . 11

1.3 5G localization architecture . . . 13

1.4 5G technologies for positioning . . . 14

1.5 5G positioning techniques . . . 15

1.6 5G positioning signals . . . 16

2 5G NR Uplink simulator **21**

2.1 Uplink physical layer of 5G NR . . . 22

2.1.1 Modulation . . . 22

2.1.1.1 Frequency selectivity . . . 25

2.1.1.2 Time dispersion . . . 25

2.1.2 Numerology . . . 27

2.1.3 Frame structure . . . 28

2.1.4 Physical resources . . . 30

2.1.4.1 Antenna port . . . 31
2.1.4.2 Resource grid . . . 31
2.1.4.3 Resource elements . . . 31
2.1.4.4 Resource blocks . . . 31
2.1.5 Bandwidth parts . . . 32
2.2 5G NR signal model . . . 33
2.3 System architecture and capabilities . . . 34
2.3.1 System-level simulation . . . 35
2.3.2 Physical-level simulation . . . 38
2.3.3 Observable generation . . . 39
2.3.3.1 Ranging observable . . . 40
2.3.3.2 Angle observable . . . 44
2.3.4 Position computation . . . 45
2.3.4.1 TDoA positioning algorithm . . . 46
2.3.4.2 RTT positioning algorithm . . . 47
2.3.4.3 AoA positioning algorithm . . . 47
2.4 5G parametric elements . . . 48
2.4.1 Dilution of precision . . . 48
2.4.2 Fisher information and bounds for localization . . . 49
2.4.3 5G signal bandwidth . . . 51
2.4.4 Antenna array elements . . . 51
2.A Derivation of the geometry matrix in AoA positioning method . . . 53
2.B Derivation of the covariance matrix in CRB TDoA positioning. . . . 54

3 Assessment of positioning techniques using the 5G NR simulator 57
3.1 A reliable benchmark for 5G localization performance . . . 58
3.1.1 Downlink evaluation: OTDoA . . . 59
3.1.1.1 Scenario 1: UMi . . . 59
3.1.1.2 Scenario 2: UMa . . . 61
3.1.2 Uplink evaluation: UTDoA . . . 63
3.1.2.1 Scenario 1: UMi . . . 64
3.1.2.2 Scenario 2: UMa . . . 65
3.1.3 Round trip time evaluation . . . 66
3.1.3.1 Scenario 1: UMi . . . 67
3.1.3.2 Scenario 2: UMa . . . 68

3.1.4 Uplink evaluation: AoA . . . 69
3.1.4.1 Scenario 1: UMi . . . 70
3.1.4.2 Scenario 2: UMa . . . 71
3.2 5G positioning performance in crucial use cases . . . 73
3.2.1 Low-energy use case: IoT . . . 73
3.2.2 High-accuracy use case: Autonomous car . . . 75
3.3 Bridging simulation and real-world experimentation for high-accuracy 5G positioning solutions . . . 77
3.3.1 Scenario definition and implementation . . . 78
3.3.2 Experimentation evaluation and analysis. . . . 79
3.4 Conclusions . . . 81

4 Measurement characterization, outlier detection and exclusion for 5G positioning 83

4.1 Integrity . . . 84
4.2 Outlier characterization . . . 85
4.2.1 5G signal pseudorange measurements . . . 85
4.2.2 Position computation . . . 86
4.2.3 Computation of test statistic . . . 87
4.2.4 Selection of threshold parameter . . . 88
4.3 Outlier detection and exclusion . . . 88
4.4 Simulation results . . . 89
4.4.1 Results when BW=20 MHz . . . 91
4.4.2 Results when BW=100 MHz . . . 92
4.5 Conclusion . . . 94

5 Joint TDoA and AoA localization in deep urban deployment 97

5.1 Characterization of the observables . . . 98
5.1.1 Observable based on time of arrival . . . 98
5.1.2 Observable based on angle of arrival . . . 99
5.2 Position solution and measurement exclusion . . . 100
5.2.1 Location solution based on Time of Arrival . . . 100
5.2.2 Location solution based on Angle of Arrival . . . 100
5.2.3 Location solution based on joint UTDoA-AoA . . . 101
5.3 Simulation results and evaluation . . . 101
5.3.1 Scenario definition . . . 102

5.3.2 Performance results . . . 102
5.4 Conclusion . . . 108

6 5G SDR receiver and AoA estimation 109

6.1 5G receiver structure . . . 111
6.2 5G NR signal generation and receiver data reception . . . 112
6.3 Techniques for AoA estimation . . . 115
6.3.1 Classical Beamformer . . . 116
6.3.2 MUltiple SIgnal Classification (MUSIC) . . . 116
6.3.3 Estimation of Signal Parameters via Rotational Invariance Techniques (ESPRIT) . . . 118
6.3.4 Iterative Adaptive Approach (IAA) . . . 119
6.3.5 Iterative SAMV Approaches . . . 120
6.3.6 Grid-Free SAMV-SML Approaches . . . 122
6.4 Synchronization . . . 122
6.4.1 Impact of time and frequency error estimation . . . 123
6.4.2 Symbol timing and frequency offset estimation . . . 124
6.4.3 Frame synchronization . . . 125
6.4.4 Residual carrier frequency offset estimation . . . 125
6.5 Calibration . . . 127
6.5.1 RF channel error calibration . . . 128
6.5.1.1 USRP main configuration features . . . 128
6.5.1.2 USRP RF and clock calibration . . . 132
6.5.1.3 USRP experimental calibration and performance evaluation . . . 135
6.5.2 Antenna error calibration . . . 138
6.5.2.1 In-Situ calibration . . . 139
6.5.2.2 Anechoic chamber antenna error calibration . . . 141
6.6 Simulation results on time-delay, carrier frequency offset and angle estimation accuracy . . . 143
6.6.1 Multipath free environment . . . 144
6.6.2 Multipath environment . . . 147
6.7 Experimental results on angle estimation accuracy . . . 153
6.7.1 Experimental hardware and software setup . . . 153
6.7.2 Indoor experimental results . . . 154
6.7.3 Outdoor experimental results . . . 155
6.8 Conclusions . . . 158

Conclusions and future work **159**

Conclusions 159

Future work 161

Bibliography **169**

List of Figures

1.1 UE Positioning Architecture applicable to NG-RAN [21] 14
1.2 Expected horizontal accuracy of localization methods for indoor, outdoor urban, and rural scenarios [23]. 16

2.1 Transmitter block diagram for CP-OFDM with optional DFT-spreading. 23
2.2 OFDM representation. 23
2.3 OFDM transmission process. 25
2.4 Radio frame structure. 28
2.5 Uplink resource grid [24]. 32
2.6 5G NR bandwidth parts. 33
2.7 General architecture of the simulation tool. 35
2.8 Architecture of the system-level simulation tool. 35
2.9 Physical-level simulation tool 39
2.10 Architecture of the observable generation tool. 40
2.11 2D-interpolated CDF of ranging errors over UMa environments. 41
2.12 5G positioning performance over UMa environments. 42
2.13 5G positioning performance over UMi environments. 42
2.14 UPA structure and AoA representation. 44

3.1 Results of OTDoA for UMi deployment for FR1. 61
3.2 Results of OTDoA for UMa deployment for FR1. 63
3.3 Results of UTDoA for UMi deployments for FR1 with perfect synchronization. . 65
3.4 Results of UTDoA for UMa deployments for FR1 with perfect synchronization. . 66
3.5 Results of RTT for UMi deployments for FR1. 68
3.6 Results of RTT for UMa deployments for FR1. 69
3.7 Results of AoA for UMi deployments for FR1. 71
3.8 Results of AoA for UMa deployments for FR1. 72
3.9 IoT use case environment implementation. 74
3.10 IoT use case 5G horizontal positioning error. 75

3.11 Autonomous cars use case environment implementation. 76
3.12 Autonomous cars use case 5G horizontal positioning error. 77
3.13 Loading Zone environment experimentation. 78
3.14 ToA error relative to SNR. 79
3.15 Experimental results. 79

4.1 NLoS BS exclusion mechanism. 89
4.2 CDF of the NLoS test T for BW=20 MHz with an 30 m bias. 92
4.3 CDF of the NLoS test T for BW=20 MHz with an 5 m bias. 92
4.4 CDF of the NLoS test T of BW=100 MHz with an 30 m bias. 93
4.5 CDF of the NLoS test T for BW=100 MHz with an 5 m bias. 93
4.6 UE error positions when using RAIM or not. 94
4.7 UE error positions when using RAIM or not. 94

5.1 Simulation scenario 103
5.2 CDF of the HDOP for UTDoA, AoA and hybrid solution. S1 refers to first scenario and S2 refers to the second scenario. 104
5.3 Results for 20 MHz bandwidth with 50 ns sync. err. 105
5.4 Results for 50 MHz bandwidth with 50 ns sync. err. 106
5.5 Results for 20 MHz bandwidth with perfect sync. 106
5.6 Results for 50 MHz bandwidth with perfect sync. 107

6.1 Block diagram of the testbed. On the left side is depicted the transmitter and on the right is depicted the receiver. The inverted black triangles represent antenna elements. The red cables represent the power-based type, the orange ones represent the Ethernet cables and the green one represents the MXIe cable. . . . 112
6.2 5G SDR receiver top-level block diagram. 112
6.3 Data generation and extraction process. The 5G NR waveform is saved in a binary file, where the I and Q samples are interleaved and transmitted periodically for 2 sec. 113
6.4 5G NR RF signal transmission characteristics. 114
6.5 ULA with M elements for AoA estimation. 115
6.6 Subarray arrangement for the ESPRIT algorithm [64]. 118
6.7 Constellation diagram: Residual carrier frequency offset estimation and compensation. 127
6.8 TwinRx block diagram. Image source: [76] 134

6.9 RF channel error calibration, where USRP N200 or N310 serves as TX and USRPs: N310, X300-2TwinRx or NI-2955 serve as RX. Note that, for the case of NI-2955, MXIe cables are used instead of 10 Gigabit Ethernet cables to connect with the PC. 135

6.10 Phase coherence with X300-2TwinRx. 137

6.11 Phase coherence with N310 (internal LO). 137

6.12 Phase coherence with N310 (external LO). 138

6.13 Phase coherence with NI-2955. 138

6.14 Set-ups for In-Situ calibration and AoA estimation experiments in a 56 m^2 room size. The X and Y positions in 6.14(b) correspond to the width and length of the room size respectively. The receiver is placed near the wall at one extreme of the room length and the transmitter is placed 3 m away from the other extreme of the room length (see 6.14(a), 6.14(b)). The Tx and Rx are placed within a distance of 5m and each antenna element on the receiver side has a spacing of 0.0603 m in between. 140

6.15 Example of the presence of interference in the received baseband signal. 141

6.16 Ins-Situ Calibration: Antenna phase errors at the pilot direction of arrival. . . . 142

6.17 Antenna calibration using an Anechoic Chamber. A horn antenna is used as a transmitter for better antenna directivity and higher transmit power. The receiver is a four-element antenna array composed by monopole antennas and mounted on a rotary stand. Fixed angular positions are achieved by moving the rotary structure with small angular steps. The Tx and Rx are placed within a distance of 3m and each antenna element on the receiver side has a spacing of 0.0603 m in between. 143

6.18 Anechoic-Chamber: Calibration: Antenna phase errors at the pilot direction of arrival. 144

6.19 Evaluating the accuracy of carrier frequency offset estimation. 147

6.20 Evaluating the accuracy of time offset and angle of arrival estimation. In (a) it is presented the angle error estimation versus SNR values and in (b) the range delay error estimation versus SNR values. 148

6.21 Angle estimation error for different angle spread. 150

6.22 Angle estimation error for different angle spread using sparse asymptotic minimum variance approaches. 151

6.23 Time delay error estimation. 152

6.24 Setup of an outdoor experiment for AoA estimation in the presence of a reflection forming a 45° angle of arrival. Note that, for an experiment where the reflector forms a 30° angle of arrival, it is placed near the TX side. For the scenario without multipath, i.e., the TX and RX are in LoS conditions, the reflector is removed and the rest of the setup has remained the same. 154

6.25 Estimation angle of arrival accuracy using In-Situ calibration in indoor environment. 155

6.26 RMSE angle estimation in LoS conditions. 156
6.27 Evaluating the accuracy of the angle of arrival estimation in the presence of multipath. 158

List of Tables

2.1 Supported transmission numerologies [27]. 27
2.2 Radio frame configuration based on numerology. 29
2.3 Slot formats for normal cyclic prefix [28]. 30
2.4 Propagation conditions based on the type of scenario. 37
2.5 Configuration parameters of the NR positioning support. 39

3.1 Parameters details for FR1 with perfect and realistic synchronization using OTDoA method [40] 60
3.2 Summary of evaluation results in UMi scenario with perfect synchronization: OTDoA at FR1 60
3.3 Summary of evaluation results in UMi scenario with 50-ns synchronization error: OTDoA at FR1 60
3.4 Parameters details for FR1 with no synchronization error[41] 62
3.5 Parameters details for FR1 with 50 ns synchronization error [41] 62
3.6 Summary of evaluation results in UMa scenario with perfect synchronization: OTDoA at FR1 62
3.7 Summary of evaluation results in UMa scenario with perfect synchronization: OTDoA at FR1 62
3.8 Parameters details for FR1 with perfect synchronization: UTDoA at FR1 [42]. . 64
3.9 Summary of evaluation results in UMi scenario: UTDoA at FR1. 64
3.10 Parameters details for FR1 with perfect synchronization: UTDoA at FR1 [42]. . 66
3.11 Summary of evaluation results in UMa scenario: UTDoA at FR1. 66
3.12 Parameters details for FR1 of UMi deployment [40]. 67
3.13 Summary of evaluation results in UMi scenario: RTT at FR1. 67
3.14 Parameters details for FR1 with no synchronization error: RTT [40]. 68
3.15 Summary of evaluation results in UMa scenario: RTT at FR1. 69
3.16 Parameters details for FR1 with no synchronization error:AoA [41]. 70
3.17 Summary of evaluation results in UMi scenario: UAoA at FR1 [41]. 70
3.18 Parameters details for FR1 with no synchronization error: UAoA [41]. 71

3.19 Summary of evaluation results in UMa scenario: UAoA at FR1 [41]. 72
3.20 Positioning accuracy of IoT use case for a UMa deployment. 74
3.21 Positioning accuracy of Autonomous cars use case for a UMi deployment. 77
3.22 Mean TDoA Error in meters. 80
3.23 Median TDoA Error in meters. 80
3.24 Positioning accuracy KPIs for the 5G FR1 downlink measurements. All KPIs are expressed in meters. 80

5.1 Simulation parameters. 103
5.2 Performance of BS exclusion mechanism in positioning accuracy. 107

6.1 5G NR Uplink signal specifications. 114
6.2 The SAMV approaches 122
6.3 The SAMV-SML approaches 122
6.4 USRP main features comparison 129
6.5 Experimental parameter configuration. 136
6.6 AoA estimation performance 155
6.7 Table with AoA estimation averages and standard deviation for estimation of the reflection angle at 30°. 157
6.8 Table with AoA estimation averages and standard deviation for estimation of the reflection angle at 45°. 158

Acronyms

3GPP 3rd Generation Partnership Project. 1–3, 7, 8, 11, 12, 15, 21, 22, 29, 31, 34, 35, 40, 57–59, 70, 73, 75, 78, 80, 98, 102, 103

ADC Analog-to-Digital Converter. 112, 130, 131

AMF Access&mobility Management Function. 13

AoA Angle of Arrival. iv, 1, 2, 4, 15, 21, 44–53, 57, 59, 69, 71, 97, 99–105, 109–113, 115–117, 119, 121–123, 126–128, 132, 139–144, 146, 148–150, 154, 155, 157, 158, 160

AoD Angle of Departure. 15, 51

AWGN Additive White Gaussian Noise. 38, 44, 51, 99, 116, 117, 145

BS Base Station. 1, 3, 14–16, 19, 29–31, 33–38, 41, 43–47, 50, 52–55, 58, 59, 61, 63, 64, 66, 69–71, 73–76, 78, 83, 85–94, 97–102, 104–108, 111, 160

BW Bandwidth. 91, 102

BWP BandWidth Part. 32, 33

CA Carrier Aggregation. 12

CDF Cumulative Density Function. 38, 40, 59, 73, 76, 78, 88, 91, 104

CFO Carrier Frequency Offset. 4, 80, 110, 114, 123–125, 144, 145

CID Cell IDentity. 15, 46, 57, 73, 74, 76, 81, 159

CP Cycle Prefix. 23, 24, 27, 28, 112, 114, 125, 144, 145

CRB Cramér-Rao Bound. 22, 39, 44, 45, 48–51, 70, 99, 144–146

CSI-RS Channel Status Information Reference Signal. 15, 17–19

DAC Digital-to-Analog Converter. 130, 131

DAS Delay And Sum. 151

DC Dual Connectivity. 12

DFT Discrete Fourier Transform. 18, 19, 22, 125, 126

DL Downlink. 13, 15, 17–19, 21, 28, 29, 31, 33, 34, 38, 39, 43, 45–47, 54, 59, 98, 99

DMRS Demodulation Reference Signal. 17–19

DOP Dilution of Precision. 22, 48

DSS Dynamic Spectrum Sharing. 12

EFIM Equivalent Fisher Information Matrix. 49, 50

eMBB Enhanced Mobile Broadband. 11

eMTC Enhanced Machine-Type Communications. 11

ESPRIT Estimation of Signal Parameters via Rotational Invariance Techniques. 115, 118, 119, 148, 150, 156, 157

FCC Federal Communication Commission. 8, 9

FD Fault Detection. 83, 88

FDE Fault Detection and Exclusion. 83, 85, 88, 90, 105

FFO Fractional Frequency Offset. 123

FFT Fast Fourier Transform. 23, 24, 26, 27, 112, 114, 123–125, 140

FIM Fisher Information Matrix. 49, 55, 56

FR1 Frequency Range 1. 14, 15, 38, 51, 59, 61, 73, 75, 78, 91, 102

FR2 Frequency Range 2. 14, 15

GDOP Geometric Dilution of Precision. 48, 49, 103

GN Gauss-Newton. 46–48, 70, 86, 88

gNB 5G NodeB. 13, 17, 29, 33

GNSS Global Navigation Satellite System. iii, 1, 7, 10, 11, 43, 83, 84, 95

HDOP Horizontal Dilution of Precision. 48, 90, 103, 104

IAA Iterative Adaptive Approaches. 115, 119, 149, 151, 152, 157

IFFT Inverse Fast Fourier Transform. 23, 24, 27, 113, 145

IFO Integer Frequency Offset. 123, 124

IIoT Industrial Internet of Things. 8, 12

IoT Internet of Things. 1, 3, 9–12, 28, 57, 73–76, 81, 159

IoT-NTN IoT Connectivity Non-Terrestrial Networks. 11

ISD Inter-Site Distance. 35, 36, 58, 59, 61, 64, 70, 73, 75, 102

ITS Intelligent Transport Systems. 8

KPI Key Performance Indicators. 80

LMF Location Management Function. 13

LO Local Oscillator. 111, 129, 132–137

LoS Line of Sight. iii, 2, 9, 14, 15, 21, 26, 35–37, 40, 41, 43, 45, 48, 50, 51, 59, 61, 65, 70, 71, 73, 78–80, 83–85, 90, 91, 98, 101, 105, 139, 141, 145, 149, 153

LS Least Squares. 46, 91, 95, 150, 157

LTE Long Term Evolution. 11, 13, 14, 27–29, 31, 32, 85

LTE-M Long Term Evolution - category M1. 10

MDL Minimum Descriptive Length. 156

MIMO Multiple-Input Multiple-Output. 12, 15, 17, 18, 22

mMTC Massive Machine-Type Communications. 11, 12

MUSIC MUltiple SIgnal Classification. 115–119, 140, 148, 149, 152, 156, 157

NB-IoT NarrowBand IoT. 10, 11

ng-eNB Next-generation enhanced NodeB. 13

NG-RAN Next Generation Radio Access Network. 13

NLoS Non Line of Sight. iii, iv, 2, 3, 9, 12, 15, 37, 40, 41, 51, 61, 74, 78, 79, 81, 83, 84, 88, 89, 91–94, 97–100, 102, 104, 105, 107–109, 159, 160

NR New Radio. 1, 3, 7, 11–13, 16–19, 21, 27–29, 31–33, 51, 57, 58, 61, 63–65, 67–70, 72, 73, 76–80, 91, 97, 102, 111, 113, 126, 135, 159

NR-NTN NR Enhancements Non-Terrestrial Networks. 11

NTN Non-Terrestrial Networks. 11, 12

OFDM Orthogonal Frequency Division Multiplexing. 17–19, 21–28, 31, 33, 34, 38, 59, 63, 65, 69, 70, 73, 101, 102, 110, 112–116, 122–126, 145

OTDoA Observed Time Difference of Arrival. 41, 45, 46, 59–61, 63, 64, 67, 69, 73, 74, 76, 78, 85, 86, 89–91, 93, 98–100

PAPR Peak-to-Average Power Ratio. 22, 33, 63

PDSCH Physical Downlink Shared CHannel. 17

PL Protection Level. 84, 95

PRS Positioning Reference Signal. 15, 17, 19, 33, 34, 38, 40, 43, 59, 61, 63, 67, 73, 78, 85, 91, 101, 102

PRU Physical Resource Unit. 33, 34

PT-RS Phase Tracking Reference Signal. 18, 19

PUSCH Physical Uplink Shared Channel. 22

QAM Quadrature Amplitude Modulation. 23, 24

QoS Quality of Service. 11, 13

RAIM Receiver Autonomous Integrity Monitoring. 83, 90, 91, 161

RAT Radio Access Technology. 12

RB Resource Block. 30–34

RF Radio Frequency. 4, 109–115, 123–128, 132, 133, 135, 140, 141, 143, 147, 154, 160

RMa Rural Macro. 35

RMSE Root-Mean-Square Error. 49, 59–61, 78, 102, 146, 156

RRC Radio Resource Control. 22, 33

RSS Received Signal Strength. 15

RTT Round Trip Time. 1, 15, 16, 21, 41, 43, 44, 46, 47, 57, 59, 66–69, 73, 74, 76, 81, 98–100, 105, 159, 160

SAMV Sparse Asymptotic Minimum Variance. 115, 120, 121, 149, 151, 152, 157

SAMV-SML SAMV-Stochastic ML. 115, 122, 149, 151, 152, 157

SCO Sampling Clock Offset. 4, 110

SDR Software-Defined Radio. iv, 4, 109–111, 127, 128, 130, 131, 133, 135, 136, 160

SNR Signal-to-Noise Ratio. 36, 38–40, 43, 45, 46, 50–52, 59, 70, 73–76, 78, 79, 85, 91, 98, 99, 102, 144–146, 148–152, 157

SRS Sounding Reference Signal. 15, 19, 33, 34, 37, 38, 40, 43, 59, 63–65, 67, 69, 70, 73, 98, 101, 102, 111–113, 116, 126, 128, 135, 140, 144–146, 153

SSB Synchronization Signal Block. 15, 18

SSR Sum of Squared Residuals. 87

STO Symbol Timing Offset. 4, 110

TDD Time Division Duplex. 29, 33

TDE Time-Delay Estimation. 43, 46, 47, 85, 91

TDoA Time Difference of Arrival. 1, 15, 43, 45, 46, 48–50, 54, 55, 57, 59, 63, 66, 67, 78–80, 85–89, 98, 101–104

TLS Total Least Squares. 150, 157

ToA Time of Arrival. 1, 15, 49, 50, 78–80, 85, 90, 98, 158

TRP Transmitting Reference Point. 78–80

UAV Unmanned Aerial Vehicles. 10, 11, 14, 52

UE User Equipment. 3, 8, 9, 11–16, 29–34, 36, 37, 41, 44, 48, 50, 52, 53, 58–61, 63–66, 68, 70, 73–76, 78, 81, 85, 86, 88–93, 95, 97–99, 101, 102, 104–106, 111, 159, 160

UHD USRP Hardware Driver. 130–133

UL Uplink. 13, 15, 17–19, 21, 22, 28, 29, 31, 33, 38–40, 43, 45–47, 54, 98, 99

ULA Uniform Linear Array. 51, 115–118, 139, 147, 149, 153, 157

UMa Urban Macro. 36, 40, 41, 59, 61, 63, 65, 68–71, 73, 89–91, 97, 98, 102

UMi Urban Micro. 36, 41, 59, 63–65, 69–71, 75, 78, 97, 98, 102

UPA Uniform Plannar Array. 44, 99

URA Uniform Rectangular Array. 49, 51, 53

URLLC Ultra-Reliable and Low-Latency Communications. 9, 11, 12

USRP Universal Software Radio Peripheral. 110–112, 127–133, 135, 136, 138, 140, 153

UT User Terminal. 37, 38

UTDoA Uplink Time Difference of Arrival. 21, 41, 45, 46, 63–65, 67, 69, 73, 74, 76, 81, 97–101, 104, 105, 108, 159, 160

V2X Vehicle-to-Everything. 10, 12

VDOP Vertical Dilution of Precision. 48

WLS Weighted Least Squares. 45–48, 59, 63, 86–88

XR eXtended Reality. 8

Introduction

Location-based services have become essential for our daily lives, leading to an increase in the demand for reliable and accurate positioning systems. In this context, recent advancements in 5G and other radio access technologies are poised to revolutionize positioning, impacting various societal and industrial use cases both today and in the foreseeable future.

The evolution of positioning in cellular networks began with basic estimates of distance and direction between base stations and devices, primarily to facilitate connection establishment. The progression from Global System for Mobile Communication (GSM) to subsequent cellular generations has consistently improved the accuracy of position estimates, opening doors to new applications and use cases. 5G, the fifth generation of cellular technology, has brought even more transformative changes in communication and object localization through mobile devices. In fact, the 5G cellular system seamlessly integrates various technologies, including WiFi, 4G, and New Radio (NR), creating a suitable environment for services like massive Internet of Things (IoT), autonomous vehicle communication, drone connectivity, etc. Moreover, in challenging environments, such as densely urbanized areas and indoor spaces where Global Navigation Satellite System (GNSS) signals are hard to receive, 5G steps in as a crucial alternative positioning technology, surpassing the limitations of GNSS alone. For all these reasons, 5G is expected to have a crucial role in several location-based services, including navigation, mapping, geo-marketing, advertising, and asset tracking. Furthermore, 5G is becoming instrumental in emerging technologies such as sustainable urban mobility and autonomous vehicles.

Various localization methods, such as timing-based techniques (Time of Arrival (ToA), Time Difference of Arrival (TDoA), and Round Trip Time (RTT)) and angle-based techniques (Angle of Arrival (AoA)), are under study. All these methods are expected to play a significant role in achieving accurate user positioning as they possess desirable attributes, namely large bandwidth, massive antenna arrays, centimeter-wave (cmWave), and millimeter-wave (mmWave) transmissions, among others. The challenge lies in identifying the ones that perform optimally in the main 5G use cases. Each localization method comes with its own set of limitations: ToA and TDoA methods require precise time synchronization, and the AoA method excels only when the target is in close proximity to Base Station (BS)s. These methods, when applied individually, fall short of achieving the baseline positioning accuracy outlined in the 5G 3rd Generation Partnership Project (3GPP) standard, a horizontal positioning error at decimeter-level or even centimeter-level, especially in the challenging conditions of urban scenarios. A promising advancement is the simultaneous use of time-based and angle-based techniques, an approach known as hybridization.

As already mentioned, an underlying aspect that hampers the positioning capabilities of many technologies, including 5G, is the difficulty of achieving accurate positioning in demanding

environments, such as urban canyons. In such scenarios, it is the inherent complexities of the environment, such as multipath and Non Line of Sight (NLoS) propagation, to create inaccuracies in positioning measurements. These circumstances could cause poor accuracy and reliability of the computed position, and they should be therefore monitored to preserve the overall positioning performance. Some contributions in the literature do acknowledge the presence of multipath and NLoS, but a mechanism to effectively distinguish between Line of Sight (LoS) and NLoS situations is still lacking.

Even though a lot of effort is made by researchers to the joint design of localization accuracy and communication metrics toward 5G positioning, those theoretical analyses fail to consider current implementation issues. This causes a huge gap between theoretical expectations and real-case scenarios. 5G commercial infrastructure does not modify significantly to enhance localization despite the precise localization accuracy being requested by the 3GPP standards. Therefore, to achieve high-accurate localization, the disadvantages of practical 5G systems must be overcome.

Objectives

This thesis intends to contribute to the field of 5G positioning, with special emphasis on investigating the potential and limitations that 5G positioning can bring. The main objectives of this thesis are summarized in the following.

- To propose a representative methodology to simulate standalone and hybrid techniques and assess the positioning capabilities in challenging scenarios. Moreover, to integrate the network density of 5G deployments to improve accuracy.
- To improve the positioning performance of 5G positioning by developing methods for detecting and mitigating the presence of NLoS conditions, which seriously degrade the positioning performance in urban environments.
- To explore the use of angular measurements as an additional degree of freedom and its integration with time measurements that could mitigate the degradation introduced by NLoS propagation, since signal fading has remained one of the key factors causing the detriment of positioning accuracy.
- To evaluate the performance of the signal parameter estimation algorithms needed for localization, analyzing the impact of propagation with/without direct LoS, the impact of geometry and the orientation of user terminals when using a multi-array antenna, and the impact of synchronization clock errors of the user terminal.
- To perform experimental evaluations with actual 5G signals and open-source platforms for a comprehensive understanding of the system's performance unlocking the full potential of 5G localization with precise AoA estimation.
- To combine array processing and calibration techniques in order to incorporate AoA estimation into 5G positioning, especially in complex environments.

Thesis outline and contributions

This dissertation is organized as follows.

Chapter 1 This chapter gives a brief overview of 5G NR positioning. First, it begins with a summary of positioning in cellular networks. It explores the primary verticals and relevant use cases. It continues with a discussion of the technical challenges arising from the applications and the expected features. The limitations of 5G concerning positioning and its requirements, including those defined by the 3GPP standard are also covered. This is an important step before going into more detail on specific problems and suggest possible solutions.

Chapter 2 This chapter introduces a software simulator that can be used to explore the potential of 5G systems and the capabilities of multicarrier signals. The simulator assesses the most relevant positioning technologies defined by the 5G standard, especially those challenging to measure in lab or field settings. It allows to perform simulations utilizing models and configurations representative of real-world scenarios based on base station locations and 2D/3D maps, considering the type of environment. By featuring realistic base station locations and assumptions, it enables a comprehensive exploration of the possibilities offered by 5G in enhancing time-delay and angle-of-arrival estimation in harsh environments, culminating in the development of a versatile positioning module. The work done in this chapter has been presented in the event:

- "Signal Processing, Information Theory and Communications Webinar 2021", organized by the Spain Chapter of the IEEE Information Theory Society held on July 13-16, 2021.

Chapter 3 This chapter evaluates the achievable accuracy of 5G localization in the context of the NR channel model for two main use cases: IoT and autonomous cars. Through simulations of different scenarios, it analyzes time-based and angle-based techniques for the User Equipment (UE) location estimation. The challenges posed by accurate time synchronization and distance constraints in urban scenarios are also addressed. Additionally, an evaluation of the positioning performance and its feasibility through a comparison with a real experiment is performed. Some of the simulation studies on the positioning performance of 5G technologies presented in this chapter have been done in the framework of the "GNSS Integration into 5G Wireless Networks" project (GINTO5G) funded by the European Space Agency (ESA). Part of the results of this chapter have been presented in the workshop:

- GINTO5G Workshop: "The role of GNSS in 5G and beyond", organized by GMV and the European Space Agency held on 12 March 2021.

Chapter 4 This chapter describes a method for detecting faulty measurements from BS affected by NLoS propagation. The method monitors the residuals resulting from the least-squares positioning solution. The method has been tested through simulations based on a deep urban deployment. Additionally, it presents the main integrity monitoring approaches and analyses the limitations of the proposed method. The results of this chapter have been published in the following international conference paper:

- **Alda Xhafa,** J. A. del Peral-Rosado, G. Seco-Granados, J. A. Lopez-Salcedo, "Performance of NLOS Base Station Exclusion in cmWave 5G Positioning", Proc. *IEEE Vehicular Technology Conference (VTC)* Spring, Apr 25 2021.

Chapter 5 This chapter addresses the achievable positioning performance by using hybrid techniques. These techniques involve combining timing-based and angle-based methods to leverage the strengths of both technologies, aiming for a substantial improvement in positioning accuracy. The synergy of these approaches becomes particularly crucial in mitigating the impact of harsh urban working conditions on standalone methods. Moreover, the characterization of 5G cmWave observables effect in 5G positioning and the use of advanced antennas is presented. The results of this chapter have been published in the following journal paper:

- **Xhafa, A.**; del Peral-Rosado, J.A.; López-Salcedo, J.A.; Seco-Granados, G. Evaluation of 5G Positioning Performance Based on UTDoA, AoA and Base-Station Selective Exclusion. *Sensors* 2022, 22, 101. https://doi.org/10.3390/s22010101.

Chapter 6 This chapter presents an experimental platform testbed based on versatile Software-Defined Radio (SDR) devices that can easily customize the transmission and reception processes. The developed platform consists of an SDR-based transmitter and receiver where the signal configuration and baseband signal processing are incorporated. A Carrier Frequency Offset (CFO), Symbol Timing Offset (STO), Sampling Clock Offset (SCO), and time offset compensation scheme are implemented. Firstly, our study sheds light on the challenging problem of achieving coherent phase reception between the Radio Frequency (RF) channels of existing multi-channel SDR. Moreover, two main antenna calibration methods are considered: in-situ calibration and calibration performed in an anechoic chamber. Secondly, an in-depth investigation of potential AoA estimation algorithms is performed, with the aim to evaluate their practical applicability in real-world settings. Finally, the results of some indoor and outdoor experiments are presented. Part of this work started during a research stay in Airbus Defense and Space, Munich, Germany. Some results of this chapter have been published in the following international conference and journal papers:

- **A. Xhafa**, F. Fabra, J. A. Lopez-Salcedo, G. Seco-Granados, I. Lapin, "Pathway to Coherent Phase Acquisition in Multi-channel USRP SDRs for Direction of Arrival Estimation", in *10th International Conference on Software Defined Systems (SDS)*, IEEE, 2023, pp. 1–8.

- **A. Xhafa**, F. Fabra, J. A. Lopez-Salcedo, G. Seco-Granados, "Preliminary Results of 5G Direction of Arrival Estimation using In-Situ Calibration with USRP", Proc. *International Conference on Localization and GNSS (ICL-GNSS)*, Jun 08 2023.

- **A. Xhafa**, F. Fabra, D. Egea-Roca, J. A. Lopez-Salcedo, G. Seco-Granados, "Experimental Investigation of AoA Estimation and Antenna Calibration Using a URSP Device", (In preparation to be submitted to IEEE Transactions on Wireless Communications).

Other publication Contribution not directly related to this dissertation:

- Q. Liu, C. Gao, **A. Xhafa**, W. Gao, J. A. López-Salcedo and G. Seco-Granados, "Performance Analysis of GNSS+5G Hybrid Positioning Algorithms for Smartphones in Urban Environments," in *IEEE Transactions on Instrumentation and Measurement*, doi: 10.1109/TIM.2023.3338677, 1 December 2023.

Chapter 1

5G NR positioning: overview and challenges

Despite the fact that, for a significant portion of its history, satellite-based positioning technologies, i.e. Global Navigation Satellite System (GNSS), have efficiently served outdoor location services, ensuring seamless applications like vehicle navigation and cargo tracking, they stumble when faced with the challenges posed by indoor and dense urban environments. Here, signal obstructions and multipath effects become formidable enemies, compromising accuracy and demanding the use of alternative positioning techniques. This fact propelled a plethora of research lines with the aim to find scalable and accurate non-satellite-based (or non-GPS) positioning systems [1, 2, 3]. Among them, the 5G New Radio (NR) technology [4, 5] is one of the most promising in delivering high-precision positioning within indoor environments and in offering superior positioning accuracy outdoors, surpassing the capabilities of GNSS. In this chapter, we will outline an overview of the 5G technology for positioning, its potential in improving positioning accuracy [6, 7] for several use cases, and the challenges that the technology is facing.

A wide range of commercial and industrial use cases require improved positioning capabilities. These use cases span from the localization and tracking of pedestrians and vehicles to the monitoring of assets, even in challenging environments such as indoor industrial facilities and deep urban outdoor settings. Moreover, the applications of precise positioning extend to network-internal usages, facilitating location-aware handovers and supporting the resilience of 5G and future 6G communication systems [8]. A list of the most important use cases where 5G positioning promises significant improvements is reported in Section 1.1.

The foundation of basic positioning capabilities within cellular networks was laid down several decades ago to serve regulatory services. Over the years, these capabilities have steadily evolved and their potential for many applications was soon discovered. This is reflected in the increasing importance given to positioning capabilities in the Releases of the 3rd Generation Partnership Project (3GPP), which sets the cellular network standards. A summary of the most important steps in the capabilities evolution is reported in Section 1.2, together with the aspirations that the community holds for the current 5G and future 6G frameworks in terms of location services. Moreover, the 3GPP has also defined procedures, signals, and architectural elements for 5G positioning, as well as specialized network functions. The reference standard architecture for the exposure of location-based methods are presented in Section 1.3.

5G's remarkable positioning capabilities are supported by a set of key enablers. These include the utilization of cmWave/mmWave frequency bands, facilitating wideband signals, beamforming, and precise angle estimation through multiple antennas [9]. The 5G perspective offers innovative technologies outlined in Section 1.4, that can substantially improve the user positioning performance. Importantly, many of these features are not limited to high-frequency mmWave bands and can be harnessed in lower and mid-frequency ranges as well. Thus, we can say that 5G has pushed the boundaries of technology [10], introducing crucial innovations for precise positioning. The broader bandwidths in 5G enable finer timing resolutions, and additional improvements in time resolution result from the integration of methods for measuring, reporting, and compensating for processing delays into the radio protocol.

Through extensive work on time, distance, and angular precision, the most advanced 5G positioning techniques, presented in Section 1.5, will offer centimeter-level accuracy, while 6G is expected to surpass even this level of precision. This heightened precision is crucial for realizing the 6G vision, which involves a seamless real-time integration of the physical and digital worlds, two areas that were relatively less explored in 5G: positioning and deterministic communications.

Another intriguing aspect lies in the potential surplus of useful features that can be derived from 5G's standard elements. Beyond their intended use, elements such as fingerprinting, radio network optimization, and soft information extraction [11] could extend their utility in the realm of positioning. Furthermore, signals presented in Section 1.6 and measurements originally defined for mobility and radio resource management can also serve the cause of positioning. The full realization of the positioning potential embedded in these standards hinges on seamless collaboration between User Equipment (UE) and the network. Even when such cooperation is limited, individual elements from the specifications can still prove beneficial. Given this overarching significance, to achieve this comprehensiveness, we offer a concise overview of 5G positioning, an important step for comprehensive coverage of the technologies and methodologies before going into more detail on specific problems and solution suggestions.

1.1 5G use cases and requirements

In this section, we will discuss various use cases and applications that leverage location information. Historically, the primary use case for positioning was emergency call location in earlier cellular generations. However, the evolution of the 5G network has paved the way for precise and timely positioning in advanced applications. These include safety-critical Intelligent Transport Systems (ITS) like advanced warning systems, protection for vulnerable road users, and scenarios within the Industrial Internet of Things (IIoT). Furthermore, with the advent of advanced technologies like positioning in eXtended Reality (XR) cases, which may fall under 5G and 6G, the possibilities for positioning have expanded.

A comprehensive range of use cases, verticals, and applications that benefit from positioning services are reported in the following list.

- **Emergency calls**

  The primary driving force behind positioning studies in 3GPP standardization was the need to accurately locate mobile devices making emergency calls. In 1996 the Federal Communication Commission (FCC) claimed that mobile phones dialing the emergency

number 911 had to be localized within 100 meters in 67% of cases. However, this requirement has evolved over the years. In 2015, the FCC set the demand that the UE should achieve horizontal positioning accuracy below 50 meters for 80% of all 911 calls. Furthermore, in recent years, the FCC introduced a target for vertical positioning accuracy, aiming for the precision of 3 meters at the floor level for 80% of indoor wireless 911 calls. The traditional positioning systems are not able to provide sufficiently accurate location data, especially in urban areas with tall buildings or in remote locations. Moreover, emergency situations often occur indoors, where GPS signals may be weak or unavailable. 5G technology introduces advancements in positioning capabilities that can significantly enhance emergency response scenarios. The use of 5G's capabilities for improved indoor positioning through technologies like small cells, beamforming, and indoor mapping, ensures that emergency responders can locate individuals inside buildings with greater accuracy. Additionally, communication delays can be critical, impacting the ability to coordinate and respond quickly. For this reason, 5G networks aim at offering low latency, enabling real-time communication between emergency responders, command centers, and Internet of Things (IoT) devices. However, several challenges remain to be faced. The network environment may change rapidly during emergencies, affecting signal strength and quality. Here comes the need for 5G networks to dynamically optimize their parameters, such as frequency and power, to adapt to changing conditions, ensuring reliable connectivity and positioning information even in dynamic and challenging environments. Even with these limitations, there is no doubt that 5G positioning capabilities in emergency response systems can significantly improve the effectiveness and efficiency of first responders in critical situations.

- **Intelligent transportation systems and autonomous vehicles**

  The evolution of vehicular systems [12] is rapidly progressing towards highly connected and fully automated vehicles. This high level of autonomy relies on two primary drivers: precise location awareness through accurate positioning and sensing, and Ultra-Reliable and Low-Latency Communications (URLLC) among vehicles within a shared network infrastructure. These capabilities enable vehicles to create a collective understanding of their surroundings and make informed decisions based on local observations and the expected actions of nearby users. Another important capability to enable real-time updates and coordination with other vehicles and infrastructure is low-latency communication. This characteristic can be addressed by enabling near-instantaneous communication between vehicles and the surrounding infrastructure. Edge computing at the network's edge can further reduce communication delays. The integration of URLLC with accurate positioning and sensing is a major step towards a safer transportation system, aiming to achieve zero road fatalities and improved traffic management [13]. 5G technology is uniquely positioned to meet the stringent requirements of road safety applications, thanks to its combination of URLLC and high localization accuracy. Moreover, urban environments with tall buildings and obstacles can lead to signal blockages and challenges in maintaining Line of Sight (LoS) communication. Here 5G can help by leveraging technologies such as beamforming and small cells to address Non Line of Sight (NLoS) issues and improve signal penetration in urban canyons. In addition to accuracy and low latency, positioning integrity is a crucial aspect. It refers to the level of trust one can have in the correctness of information provided by a positioning system. This integrity is essential for use

cases such as rail and maritime operations, unmanned autonomous vehicles like drones, autonomous driving, and Vehicle-to-Everything (V2X) communication. It helps minimize safety risks, accidents, and legal disputes involving liabilities. In these contexts, ensuring accurate positioning is essential to prevent potential harm and ensure safety.

- **Internet of things**

  Positioning is a pivotal concept in enabling low-power wide-area IoT connectivity, ushering in a transformative shift for individuals, businesses, and society as a whole. The applications benefiting from IoT positioning are diverse. Firstly, some devices require high-precision positioning, such as wearables, machinery control systems, safety monitoring equipment, etc. These devices rely on accurate location information to function effectively. Secondly, some applications involve continuous position tracking as devices move across geographic areas. This category includes asset tracking in logistics, tracking white goods and appliances, etc. Lastly, many IoT devices remain in fixed positions throughout their lifecycle, primarily used for environmental monitoring. While these devices may not require high-precision positioning, they play a crucial role in various applications. The emergence of reduced capability devices, which are designed for broadband IoT use cases and offer greater bandwidth compared to older technologies like NarrowBand IoT (NB-IoT) and Long Term Evolution - category M1 (LTE-M), will further enhance the accuracy and capabilities of IoT services.

  5G-enabled IoT positioning should meet the diverse needs of various applications. IoT devices often use a combination of technologies for positioning, such as GPS, Wi-Fi, and sensors. Integrating these technologies seamlessly with 5G for a cohesive and accurate positioning system poses a challenge that needs to be addressed for comprehensive IoT solutions. Moreover, balancing the need for accurate positioning with privacy concerns is crucial. Striking the right balance to protect user privacy while enabling useful applications is a challenge in the 5G-enabled IoT landscape. Additionally, establishing industry-wide standards for location services in 5G is essential for consistent and reliable positioning across diverse devices and applications in IoT.

- **Aerial vehicles**

  Unmanned Aerial Vehicles (UAV) [14] are becoming increasingly vital in both civilian and military applications, including remote sensing, search and rescue missions, environmental monitoring, aerial communications, and networking. Precise localization and tracking are essential for UAV navigation and control. Traditionally, this is achieved by combining data from inertial sensors and GNSS. However, GNSS-based position estimates face challenges in urban or suburban environments due to factors like signal multipath interference, satellite signal blockages, and interference from sources such as jamming and spoofing. 5G technologies, including beamforming and small cells, can mitigate signal interference in urban environments. UAV navigation is even more complex in indoor settings like warehouses or GNSS-denied areas such as forests and mines. Vision-based navigation is a promising alternative that can partially overcome these limitations. Future autonomous UAV navigation applications [15] must meet strict requirements for precision, low latency, and safety. Terrestrial radio localization techniques are envisioned to play a crucial role in achieving these objectives. This includes ad-hoc solutions like ultra-wideband ranging or opportunistic solutions that leverage existing radio transmissions, such as those in WiFi

or cellular networks, for trilateration or triangulation using antenna arrays. Additionally, aerial vehicles often have limited battery life and continuous communication for positioning updates can impact endurance. One solution can be by implementing energy-efficient communication protocols and optimizing communication intervals to balance the need for accurate positioning with battery life constraints. Finally, mobile radio network-based positioning, as provided by 5G communications, can also support UAV navigation.

- **Non-terrestrial network technology**

  The evolution of Non-Terrestrial Networks (NTN) [16] has taken two major directions. The first one is the 5G NR Enhancements Non-Terrestrial Networks (NR-NTN) that incorporate non-terrestrial communications within the 5G system, mainly focusing on Enhanced Mobile Broadband (eMBB) services. The second is the IoT Connectivity Non-Terrestrial Networks (IoT-NTN) that extends IoT or Massive Machine-Type Communications (mMTC) through non-terrestrial connectivity. The focus on eMBB and mMTC is derived from the challenges in providing URLLC services due to satellite propagation delays. For eMBB, NTN aims to provide broadband connectivity in underserved areas, on moving platforms, and enhance network resilience. It is also utilized to offload terrestrial networks by enabling broadcast channels to deliver content and public safety messages. In mMTC, NTN facilitates wide and local area IoT services, supporting connectivity for telematics applications in wide areas (e.g., automotive, energy, agriculture) and local areas with groups of sensors deployed under cell coverage.

  Unlike NR-NTN, IoT-NTN is designed with lower complexity. It continues the radio link with adaptations of NB-IoT or Enhanced Machine-Type Communications (eMTC) for NTN connections. However, it emphasizes energy efficiency and power saving rather than Quality of Service (QoS) support. IoT-NTN operates on a best-effort basis, suitable for latency-tolerant applications. The standalone deployment is prioritized, using a transparent bent-pipe satellite architecture. UE is assumed to have GNSS capabilities for time and frequency pre-compensation. The 3GPP standard requirements encompass a wide range of use cases, from indoor hotspots to satellite-based extensions of the 5G system. Satellite-based communications have been categorized into broadcast satellite services (BSS), fixed satellite services (FSS), and mobile satellite services (MSS).

1.2 Standardization efforts

Over the years, 3GPP has actively engaged in standardizing positioning capabilities, with considerable advances achieved already with the Long Term Evolution (LTE) and 4G technologies. In this section, however, we will focus only on the recent advances of 5G NR, and we will look forward, analyzing the 3GPP ambitious aspirations for the advancement of positioning technology within the 5G framework and the future 6G.

3GPP introduced 5G technology with Release 15 [17], setting the stage for global commercial 5G deployments and, since then, it has been actively working on advancing 5G technology, aimed at improving performance and addressing new use cases. In Release 15, 3GPP introduced the basic positioning features for non-standalone deployment. Additionally, it laid the foundation for the NR air interface, designed to support various usage scenarios, including eMBB (requiring

very high data speeds, low delays in communication, and strong reliability, meaning giving users faster and more reliable internet access), URLLC (requiring low communication delays and high reliability, crucial for applications like remote surgery or autonomous vehicles) and mMTC (characterized by the need of connecting a massive number of devices, like sensors or IoT devices, that requires low power consumption, long communication range, and high-accuracy positioning). Moreover, NR brought features like high-frequency operation, spectrum flexibility, low latency support, and advanced antenna technologies.

Release 16 [18] marked the first major step in 5G evolution. Several Radio Access Technology (RAT)-dependent techniques were introduced to enhance positioning capabilities. These techniques including Multiple-Input Multiple-Output (MIMO), Dynamic Spectrum Sharing (DSS), Dual Connectivity (DC), Carrier Aggregation (CA) and UE power-saving. They addressed new use cases and deployment scenarios, such as IIoT, unlicensed spectrum operation, V2X communications, positioning services, and integrated access and backhaul (IAB). Another important focus of Release 16 was the emergency call use case. However, positioning in 5G NR has broader applications. These applications primarily target indoor factory scenarios, necessitating improvements and enhancements to positioning solutions introduced in Release 16.

In Release 17 [19], existing features were further enhanced, including MIMO, DSS, UE power saving, coverage, positioning, and URLLC. Efforts are directed at refining tools available in Release 16 to achieve better accuracy. This includes handling NLoS scenarios and carrier aggregation for positioning. Discussions are ongoing to meet latency requirements, particularly for scenarios requiring rapid positioning (100 milliseconds or less). Enhancements are aimed at strengthening trust levels associated with positioning information. Moreover, new use cases covered reduced capabilities UE, operation in frequency bands beyond 52 GHz, multicast and broadcast service (MBS), and NTN.

The next phase, known as 5G Advanced, will be the 3GPP Release 18 [20]. Release 18 will be the result of intense discussions and diverse proposals that are taking place in these years within 3GPP. This release will encompass a 27 study or work items aimed at enhancing network performance and addressing new use cases. A significant focus is the incorporation of artificial intelligence and machine learning technologies into the evolution of 5G Advanced.

All in all, 5G NR continues to evolve, and future enhancements and expansions are likely. Some areas that may see improvement or introduction include:

- **Carrier-Phase-Based Positioning**: Promising higher accuracy.
- **Positioning Using Unlicensed Spectrum (NR-U)**: Expanding the positioning capabilities of 5G NR.
- **Very-Low-Cost and Low-Complexity Positioning**: For asset tracking and cost-effective solutions.
- **Sidelink and V2X Positioning**: Addressing use cases like autonomous driving.
- **Positioning and Pose Estimation for Extended Reality Applications**: Enabling augmented and virtual reality experiences.

Looking ahead, 6G networks are expected to integrate communications, positioning, and sensing over a single network, unlocking even more use cases. Machine learning is anticipated to

play a crucial role, in enhancing traditional positioning methods and enabling more advanced solutions in future network generations. These releases represent significant milestones in the development and improvement of 5G positioning capabilities. Each step brings about enhancements in positioning technology and aims to address a wider range of use cases, laying the foundation for more advanced features in 5G and beyond.

1.3 5G localization architecture

In the context of positioning a UE, Figure 1.1 illustrates the overarching 5G System (5GS) network architecture outlined in detail in [21]. The UE establishes connections successively with the core Access&mobility Management Function (AMF) and subsequently the Location Management Function (LMF) via NR or LTE access. However, it is important to note that the presented architecture does not mandate the simultaneous presence of both 5G NodeB (gNB) and Next-generation enhanced NodeB (ng-eNB). In instances where both gNB and ng-eNB coexist, the Next-Generation Core (NG-C) interface is configured for one of them.

Thus, the implementation of 5G positioning relies on an optimized architectural design that facilitates the exchange of location signals and measurements between various network components. To get a better understanding of the roles and interactions of these components, we will now break out each component of the 5G network architecture for UE positioning and analyze their respective roles. The UE is responsible for measuring Downlink (DL) signals from the Next Generation Radio Access Network (NG-RAN). These measurements can be either time-based or angle-based, depending on the chosen positioning method. NG-RAN comprises gNB and ng-eNB elements whose role affects calculating position estimates through radio signal measurements and conveying these measurements to the LMF. LMF itself is a central entity that interacts with the serving AMF and NG-RAN to obtain both Uplink (UL) and DL position measurements. It may also directly engage with the target UE to provide assistance data or calculate a location estimate. The LMF determines the positioning methods based on various factors, including the type of LoCation Service (LCS) Client, desired QoS, UE and NG-RAN positioning capabilities, and invokes these methods within the UE and serving NG-RAN. The outcome of these positioning methods can be location estimates for UE-based methods and positioning measurements for UE-assisted and network-based methods. The AMF handles connection and mobility management tasks, including positioning, for a target UE, while LMF is a pivotal component responsible for managing a range of location services for target UEs. This includes computing user positions and delivering assistance data. Moreover, the Enhanced Serving Mobile Location Center (E-SMLC) provides location information to the network, processes and consolidates data from multiple sources, and transmits position information to the requesting entity. Finally, SUPL Location Platform (SLP) is a server-based technology designed to offer secure and accurate location services to mobile devices. It is part of the Secure User Plane Location (SUPL) specification developed by the Open Mobile Alliance (OMA) for delivering Location-Based Services (LBS) in mobile networks.

All in all this architecture ensures that 5G positioning is orchestrated effectively, taking into account various parameters and requirements, to provide accurate and timely location information.

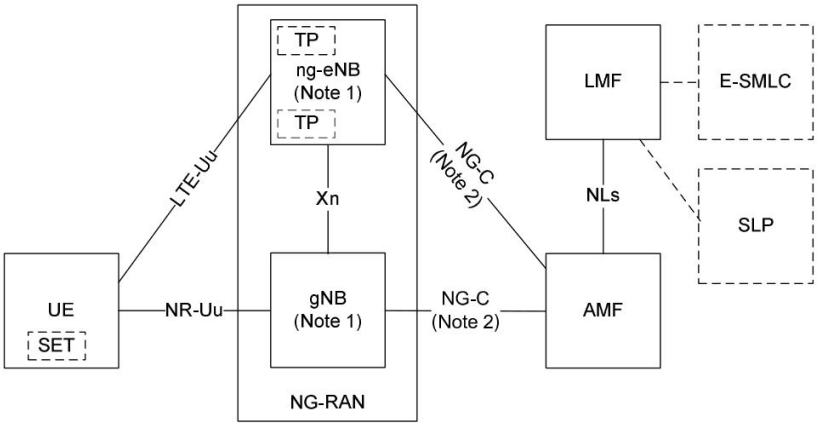


Figure 1.1: UE Positioning Architecture applicable to NG-RAN [21]

1.4 5G technologies for positioning

In the context of 5G technologies for positioning, the choice of frequency range plays a crucial role in determining the benefits and drawbacks of such technologies [22]. Frequency Range 1 (FR1) operating below 6 GHz, aligns with mature technologies similar to 4G LTE. This familiarity allows for readily available hardware and software tools, including open-source options. However, the limited spectrum in FR1 constrains bandwidth allocations, which are essential for high-accuracy ranging measurements. The relatively longer wavelengths in FR1 lead to antenna arrays with fewer elements, limiting the accuracy of angle measurements. On the other hand, the Frequency Range 2 (FR2) operating above 24 GHz introduces significant benefits for positioning. The ample spectrum availability permits large bandwidth transmissions, facilitating high-accuracy ranging that goes up to 400 MHz. High carrier frequencies in FR2 enable the use of massive antenna arrays for precise angle measurements. The adoption of highly directional antennas and beam training schemes in mmWave technologies enables to efficient capture and process of the signals. The dense deployment in FR2 enhances the probability of LoS, contributing to highly accurate measurements. Analog beamformers further enhance angle estimations. However, even in FR2, challenges arise, particularly concerning real-time baseband processing due to the high sampling rates and angle-based positioning. This is related to the beam misalignment and the potentially unknown orientations of moving Base Station (BS)s or UEs. FR2's limited coverage restricts its deployment to local hotspots and the equipment used is expected to be more expensive compared to FR1.

Another pivotal consideration for high-accuracy positioning in 5G is the high network density. Dedicated 5G network deployments, which may involve ground and UAV-based BSs, provide flexibility, expanded coverage, and optimal BS positioning for enhanced accuracy. However, these dedicated deployments may be temporary and entail additional infrastructure costs, although the potential revenue from critical positioning services justifies these expenses. Additionally, an emerging area is the exploration of carrier aggregation and full-duplex communications for positioning. Here the challenges consist in managing synchronization offsets between multiple carrier bands and addressing self-interference.

1.5 5G positioning techniques

5G positioning methods defined in 3GPP are foundational for dedicated 5G networks, with potential non-standard solutions utilizing complementary measurements such as carrier phase or Doppler frequency measurements. In these cellular-based localization technologies for both UL and DL positioning, there are four primary categories.

- **Cell-Identity-Based Localization Techniques**:

  Cell IDentity (CID) revolves around checking if the object to be located is within a specific radio coverage area. To estimate the UE's location, knowledge of the serving BS's location and the cell's area is required. The CID method can be directly applied in any cellular network, without requiring any extra resources. Thus, the CID-based method is considered as a fall-back or backup positioning procedure, in case other methods cannot be applied. Even though it is relatively simple, the main drawback is the coarse accuracy achieved compared to other techniques. Therefore, it may necessitate multiple BSs for comparable precision.

- **Angle-Based Localization Techniques**:

  These techniques utilize Angle of Arrival (AoA) and Angle of Departure (AoD) to determine positioning. With 5G's massive MIMO and beam-based operations, AoA and AoD measurements are increasingly relevant. These methods are performed using antenna arrays or beamformers, with the configuration of a number of antenna elements and distance to the UE influencing in this way in the positioning accuracy. When performing in FR1, the reduced antenna arrays limit angle resolution, which can be compensated with a shorter distance between the BS and UE in LoS conditions. In FR2, when beamforming is employed, measuring AoA and AoD based on the current beams is possible. UE orientation changes can be addressed using sensors in hybrid methods if the UE incorporates an Inertial Measurement Unit (IMU). However, in dense multipath environments, LoS measurements are critical for accuracy, leading to a two-step approach for LoS/NLoS identification.

- **Range-Based Localization Techniques**:

  These methods estimate UE positions based on range measurements between transmitters and a receiver (or vice versa). Range measurements include Received Signal Strength (RSS), Time of Arrival (ToA), and Time Difference of Arrival (TDoA). To estimate the position, the trilateration method is used and measurements from a minimum of three BSs are required. RSS based positioning utilizes RSS measurements from either the UE (using DL reference symbols like Synchronization Signal Block (SSB) or Channel Status Information Reference Signal (CSI-RS)) or the BS (using UL reference symbols such as Sounding Reference Signal (SRS)). More on the positioning signals will be detailed in Section 1.6. While this method offers relatively low positioning accuracy, it can complement hybrid positioning solutions. TDoA-based positioning achieves high-accuracy positioning and benefits from high bandwidth and LoS probability in 5G FR1 and FR2 deployments. Tight synchronization of BSs is required, and TDoA can be based on DL Positioning Reference Signal (PRS) or UL SRS. Finally, Round Trip Time (RTT)-based positioning overcomes the synchronization challenges of TDoA-based positioning by using two-way

ranging, measuring the RTT between the BS and the UE. However, it involves more signaling between the BS and UE, limited simultaneous UE servicing, and additional ranging errors, which can be mitigated with calibration.

- **Fingerprinting-Based Localization Techniques**:

  Fingerprinting involves creating an offline (training) phase database of known signal attributes at specific locations. This database is used to build models via machine-learning techniques. During the online (positioning) phase, the UE's attributes are compared to the models to estimate its position. Fingerprinting excels in cluttered multipath environments but requires significant human and resource investments for fingerprint collection. Changes in the environment or access points can necessitate updates to the fingerprint database, impacting accuracy.

Each of these techniques has its strengths and limitations, making them suitable for different scenarios and environments in the context of positioning methods. The positioning accuracy of each of these methods for outdoor and indoor scenarios has been summarized in Figure 1.2. The methods are typically based on a two-step procedure, i.e., first to obtain signal measurements and then to use these measurements to compute the mobile radio position. All the presented location methods make use of common communication network features. The location methods are placed for the different generations based on proximity, scene analysis, trilateration, and hybrid. The location methods are classified among technology generation, type of localization, and category (i.e., mobile- and network-based). The expected positioning accuracy increases with the technology generation. In later generations, the hybridization of cellular measurements with GNSS ones is of interest.

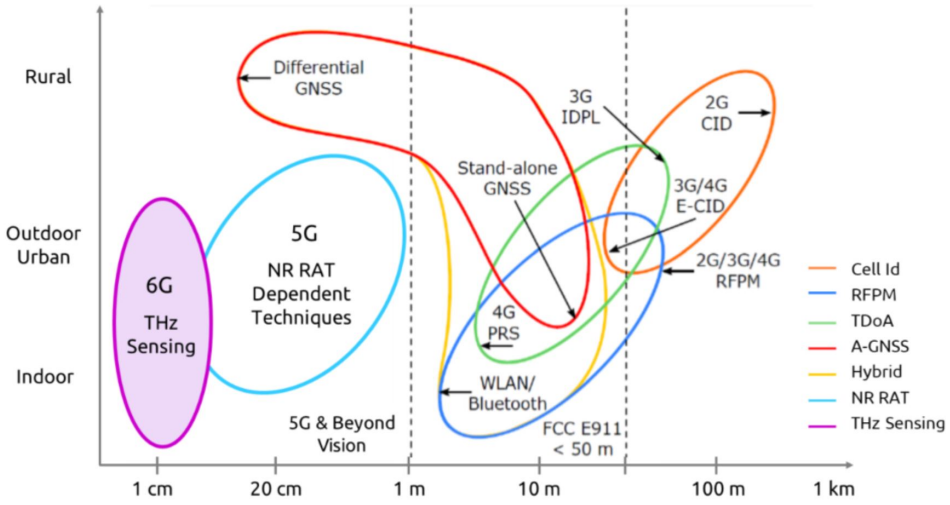


Figure 1.2: Expected horizontal accuracy of localization methods for indoor, outdoor urban, and rural scenarios [23].

1.6 5G positioning signals

Understanding the allocation of reference signals in 5G NR specifications is crucial for their use in positioning services. The 5G NR specifications offer various reference signals for both the

DL and UL that serve different purposes. These signals employ a waveform structure based on Orthogonal Frequency Division Multiplexing (OFDM) modulation with a flexible setup. In this section, we will break down the key reference signals in a concise and understandable manner. The reference signals for positioning in the DL are the following.

- **Positioning Reference Signal (PRS)**

  The PRS provides superior accuracy through the use of a diagonal or staggered physical layer resource element scheme and superior coverage and interference suppression through the coordinated transmission of gNBs. This coordinated transmission avoids interference from adjacent cells and maximizes signal strength over multiple symbols across the entire NR bandwidth. PRS is based on Gold sequences, which are pseudo-random sequences with constant amplitude and orthogonal to each other. The 5G NR PRS features are defined in [24].

- **Demodulation Reference Signal (DMRS)**:

  The DMRS is a crucial DL reference signal used for channel estimation and coherent demodulation at the receiving device. It is specific to a particular mobile terminal (MT) and can be transmitted with or without beamforming, following a scheduled pattern, and only when necessary. In terms of placement, DMRS is found in resource blocks intended for Physical Downlink Shared CHannel (PDSCH) transmission. Its early placement within the transmission is significant because it enables the receiver to obtain channel estimates promptly, facilitating the processing of the received signal. For scenarios with rapid channel variations, up to three DMRS occasions can be configured within a single OFDM slot. This flexibility in DMRS allocation supports different use cases, such as MIMO and beamforming with up to 12 orthogonal antenna ports. The DMRS also accommodates various transmission durations and symbols per slot. There are two classifications of DMRS within PDSCH allocation: Type A and Type B. Type A involves DMRS placed in the second or third symbol of a slot, adjacent to a Control Resource Set (CORESET) at the slot's beginning, while Type B positions DMRS in the first symbol of data allocation. Additionally, DMRS can be categorized into Type 1 and Type 2 sequences based on their frequency domain allocation, with Type 1 occupying every other resource element in the frequency domain and Type 2 occupying two consecutive resource elements within each group of six. Furthermore, in terms of time domain allocation, DMRS symbols can be either single-symbol or double-symbol DMRS, contributing to their adaptability and effectiveness in different scenarios

- **Channel State Information Reference Signal (CSI-RS)**:

  The CSI-RS serves the purpose of channel sounding, offering valuable insights into radio channel properties, including path loss, amplitude, and phase, across time, frequency, and spatial domains. Unlike DMRS, which is tightly associated with data transmission, CSI-RS is more versatile. It can be configured for up to 32 different antenna ports, each linked to a specific channel for sounding and potential beamforming. In the frequency domain, CSI-RS can be dense (referred to as CSI-RS density one) or less dense (CSI-RS density half), depending on whether it is present in every resource block or every second resource block. The choice of density impacts the bandwidth coverage. The time domain allocation of CSI-RS offers three options: periodic, semi-persistent, and aperiodic. Periodic CSI-RS

is received at specific intervals, with the frequency of these intervals varying depending on the scenario. Semi-persistent CSI-RS resembles periodic transmission but with the added ability to activate or deactivate the transmission. Aperiodic CSI-RS has no defined periodicity, and the mobile terminal receives notification for each transmission instance via downlink control information (DCI).

- **Synchronization Signal Block (SSB)**

  The Synchronization Signal Block (SSB) plays a vital role in helping new devices connect to the network by assisting them in locating a suitable cell. It comprises two essential components: the Primary Synchronization Signal (PSS) and the Secondary Synchronization Signal (SSS), which, together with the Physical Broadcast Channel (PBCH), form the SS block. Each SSB occupies a specific portion of the frequency domain (240 subcarriers) and time domain (4 OFDM symbols). The PSS is transmitted in the first OFDM symbol, using 127 subcarriers from the center of the SS block. The SSS is transmitted in the third OFDM symbol and occupies the same 127 central subcarriers. The PBCH transmission takes place in the second and fourth OFDM symbols and covers the entire 240 subcarriers. The number and periodicity of SSBs vary depending on the frequency band. In bands below 3 GHz, up to 4 SSBs can be present in a single half-frame. For bands between 3 GHz and 6 GHz, up to 8 SSBs are possible, while in higher frequency bands, a maximum of 64 resource blocks can be configured within a single SSB burst.

- **Phase Tracking Reference Signal (PT-RS)**:

  The Phase Tracking Reference Signal (PT-RS) is a new addition to 5G NR and serves the purpose of tracking phase deviations introduced by phase noise during transmission, particularly at higher carrier frequencies. PT-RS is characterized by its dense presence in the frequency domain and sparse allocation in the time domain. It is scheduled alongside DMRS and is only used when required by the network. PT-RS is repeated every L-th OFDM symbol in the time domain, starting with the first OFDM symbol in the allocation. The density in the time domain is associated with the scheduling of the modulation coding scheme (MCS). In the frequency domain, PT-RS is transmitted sparsely, occurring either in every second or fourth resource block. The density of PT-RS in the frequency domain is directly related to the transmitted bandwidth, with lower bandwidths having higher PT-RS density and the smallest bandwidth having no PT-RS at all.

The UL reference signals for positioning in 5G NR are the following.

- **Demodulation Reference Signal (DMRS)**:

  The UL DMRS serves a similar purpose to its DL counterpart. It is used for UL channel estimation and is found in resource blocks designated for Physical Uplink Shared Channel (PUSCH) transmission. However, there is a significant difference in that UL DMRS uses Discrete Fourier Transform (DFT)-precoded OFDM and supports single-layer transmission only. Unlike the DL, the UL does not require extensive multiuser MIMO support. The key distinction is that multiplexing reference signals with other UL transmissions from the same device are not ideal for the UL because it can negatively impact the power-amplifier efficiency of the system due to increased cubic metric. Therefore, the UL DMRS follows a similar mapping configuration to Type 1 in DL DMRS transmission.

- **Sounding Reference Signal (SRS)**:

  SRS in the UL is conceptually similar to the CSI-RS in the DL. Its purpose is to provide information about the channel, but there are fundamental structural differences between them. SRS supports a limited number of antenna ports, up to four, compared to CSI-RS's 32 ports. Furthermore, SRS is designed for power efficiency, as it is transmitted by the MT, whereas CSI-RS is transmitted by the BS. SRS follows a comb-like structure and is transmitted in every M-th subcarrier, with M being either two or four. Additionally, multiple devices can transmit SRS in the same frequency resources by assigning different comb structures for different devices. A deeper understanding of this signal can be found in Chapter 2. Note that this signal together with PRS are the ones to be used in this thesis.

- **Phase Tracking Reference Signal (PT-RS)**:

  In the UL, the PT-RS is used in conjunction with DFT-precoded OFDM. Its time domain allocation is the same as PT-RS in the DL, where it is repeated in every L-th OFDM symbol, with the counter resetting after each DMRS transmission.

In summary, these reference signals play a crucial role in 5G NR, supporting various communication and positioning services by providing essential channel information,power-efficient transmission from both mobile terminals and BSs, and synchronization capabilities. Their flexibility and adaptability make them valuable tools in the 5G network.

Chapter 2

5G NR Uplink simulator

There is no doubt that 5G networks are bringing significant changes in how we communicate and locate objects using mobile devices. Further improvements can be facilitated by research on the 5G localization algorithms, especially in harsh environments. This research can significantly benefit from the creation of a unified and effective simulation platform. In our research group, a platform in which the positioning signal modeling for Downlink (DL) had already been developed [25]. In this work, we have extended it by incorporating the positioning signal modeling for Uplink (UL), UL channel models with the latest New Radio (NR) physical-layer standards [26] and positioning methods such as the ones relying on timing-based techniques (Uplink Time of Arrival (UToA), Uplink Time Difference of Arrival (UTDoA) and Round Trip Time (RTT)), the ones relying on angle-based techniques (Angle of Arrival (AoA)) and their combinations (hybrid techniques). This software simulator is created to assess some of the most relevant positioning technologies under study by the 5G standard, especially the ones that are difficult to access with real experiments. The platform allows us to perform software simulations using models and configurations that are fully representative of real use cases and user environments. The challenge is to find methods that perform well in semi-close or close spaces such as urban canyons, assessing the positioning performance of various methods, for a particular choice of base station locations. Realistic base station locations and reasonable assumptions on these locations are considered.

This chapter begins with a description of the physical layer in Section 2.1, including the UL signal generation and modulation, and continues with a detailed explanation of the main features of the physical layer of 5G NR such as frequency selectivity, time dispersion, numerology, and frame structure. Additionally, the physical resources of the Orthogonal Frequency Division Multiplexing (OFDM) signal are described in 2.1.4. In Section 2.2, the signal model of the reference signal used in the 5G NR simulator is explained. The system architecture of the simulator and its capabilities are presented in Section 2.3. The architecture is divided into four main blocks: system-level simulation, physical-level simulation, observable generation, and position computation. The first block, described in 2.3.1, includes the 5G network parameters that will be used to determine the link budget, the Line of Sight (LoS) propagation conditions, and the power consumption levels. The physical-layer simulation, presented in 2.3.2, includes the 5G ranging and angle errors modeled using 3rd Generation Partnership Project (3GPP) channel models. The observable generation, described in 2.3.3, includes the generation of ranging and angle observables by considering the 5G ranging and angle error models. Finally, the position

computation, outlined in 2.3.4, computes the position solution with the available observables for the 3GPP positioning techniques. Additionally, the 5G parametric elements such as Dilution of Precision (DOP), Cramér-Rao Bound (CRB) of positioning, bandwidth, and antenna arrays are analyzed in 2.4 to check the feasibility of positioning performance and its impact on the localization resolution.

2.1 Uplink physical layer of 5G NR

In this section, the description of the 5G system and its architecture is carried out with a focus on the UL physical layer, where the 5G signal is defined. The general presentation will include the physical channel structure and modulation schemes.

2.1.1 Modulation

The 5G system employs a waveform structure based on OFDM modulation with a flexible setup, allowing for various subcarrier spacings and cycle prefixes. In the UL transmission (see Figure 2.1), the waveform is a conventional OFDM using a cyclic prefix. But it also supports a method called Discrete Fourier Transform (DFT)-spread-OFDM (DFT-s-OFDM) with a cycle prefix. The choice to use one of the two is determined by following the Radio Resource Control (RRC) parameters. In terms of functionality, Transform Precoding is to spread UL data in a special way to reduce Peak-to-Average Power Ratio (PAPR) of the waveform. In terms of mathematics, Transform Precoding is just a form of DFT as already specified. The mathematical representation of it is expressed through the equation shown in 2.2.

In case of using a multi-layer, i.e., UL Multiple-Input Multiple-Output (MIMO), the equation for one layer is as below:

$$y^{(0)}(l \cdot M_{sc}^{PUSCH} + k) = \frac{1}{\sqrt{M_{sc}^{PUSCH}}} \sum_{i=0}^{M_{sc}^{PUSCH}-1} x^{(0)}(l \cdot M_{sc}^{PUSCH} + i) e^{-j\frac{2\pi ik}{M_{sc}^{PUSCH}}}, \tag{2.1}$$

where $y^{(0)}$ and $x^{(0)}$ are the complex-valued modulation symbols to be received and transmitted respectively, M_{sc}^{PUSCH} being the total number of subcarriers across the whole allocated Physical Uplink Shared Channel (PUSCH) bandwidth, $k = 0, \cdots, M_{sc}^{PUSCH} - 1$, and $l = 1, \cdots, M_{symb}^{layer}/M_{sc}^{PUSCH} - 1$ with M_{symb}^{layer} being the number of modulation symbols per layer. Note also that $x^{(0)}(l \cdot M_{sc}^{PUSCH} + i)$ corresponds to OFDM symbol l prior to transform precoding, with $i \in \{0, 1, \cdots, M_{sc}^{PUSCH} - 1\}$. As it can be seen, the transform precoding is just a form of DFT that has the form:

$$X(k) = \sum_{n=0}^{N-1} x(n) e^{-i2\pi nk/N}. \tag{2.2}$$

In the case of using a single layer, the equation can be simplified as below. Compared with the general expression of DFT in 2.2, it is more clear that Transform Precoding is basically DFT.

$$y^{(0)}(k) = \frac{1}{\sqrt{M_{sc}^{PUSCH}}} \sum_{i=0}^{M_{sc}^{PUSCH}-1} x^{(0)} e^{-j\frac{2\pi ik}{M_{sc}^{PUSCH}}}. \tag{2.3}$$

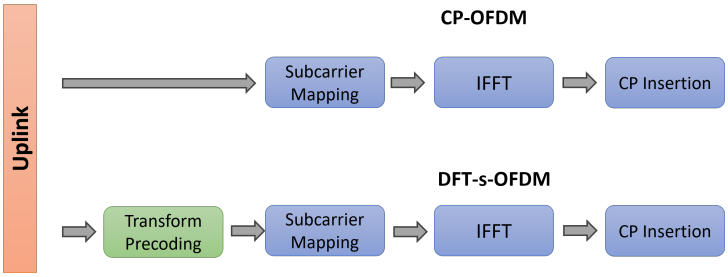
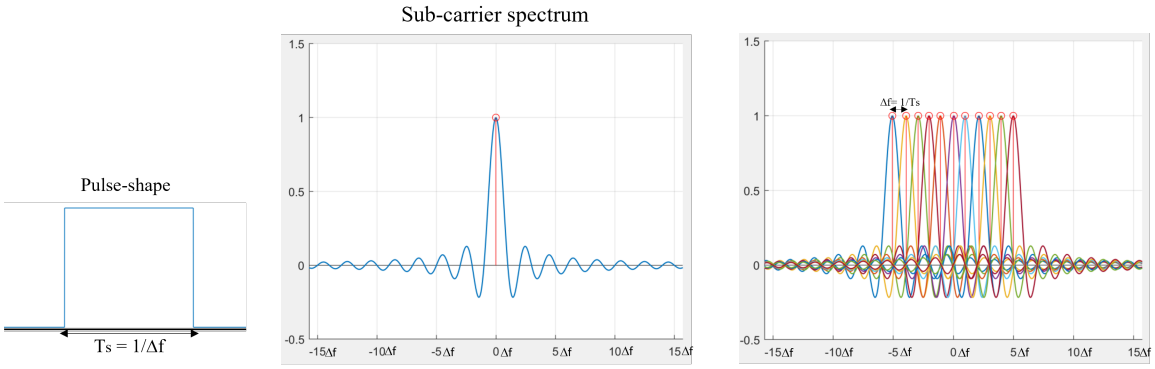


Figure 2.1: Transmitter block diagram for CP-OFDM with optional DFT-spreading.

In this thesis, the Cycle Prefix (CP)-OFDM option is considered.

OFDM is a key technology in telecommunications, particularly in multi-carrier modulation. It works by sending N complex data symbols simultaneously over M narrowband subcarriers (see Figure 2.2), each of which operates at a lower data rate compared to the entire OFDM signal bandwidth. The shape of the signal transmitted by each subcarrier resembles a rectangular pulse when observed in the time domain (resembling a "sinc" function in the frequency domain). In OFDM, these subcarriers are carefully spaced in the frequency domain to ensure that the nulls (zeros) in the spectrum of one subcarrier align with the peaks of neighboring subcarriers. This strategic arrangement is what makes the subcarriers "orthogonal" to each other. By doing this, OFDM prevents interference between subcarriers. To implement digital modulation using OFDM, we use an Inverse Fast Fourier Transform (IFFT), and, for demodulation, a Fast Fourier Transform (FFT) is applied. One of the primary advantages of OFDM modulation is its straightforward implementation.



(a) Subcarrier in time domain.

(b) Subcarrier's spectrum in frequency domain.

(c) OFDM spectrum with subcarrier spacing.

Figure 2.2: OFDM representation.

We will now break down the mathematical aspects of the OFDM transmission process depicted in Figure 2.3. This process involves a series of steps. First, a stream of data symbols b_k^l, which have been previously modulated using a scheme like M-Quadrature Amplitude Modulation (QAM), is processed. These symbols are then converted from a serial format to a parallel format through a device called a series-to-parallel converter (S/P). Next, each data symbol undergoes OFDM modulation by applying an IFFT. This transforms the data into the appropriate format for transmission as OFDM symbols. Subsequently, a CP is added to the signal. The cycle prefix involves repeating a portion of the signal, and it serves several important purposes, which will be discussed later on in this thesis. After the CP is included and the signal has been

converted back from parallel to serial using a parallel-to-series converter (P/S), the prepared signal is ready for transmission through the communication channel. At the receiver's side, these steps are carried out in reverse order to demodulate and decode the signal accurately.

During the transmission of data in the 5G OFDM system, the signal, denoted as $x(n)$, can be divided into specific time periods corresponding to individual OFDM symbols. We represent the signal for the lth OFDM symbol within the time interval $[(l-1)\cdot T_{\text{OFDM}}, l\cdot T_{\text{OFDM}}]$ as $x^l(n)$. Here, T_{OFDM} represents the duration of an OFDM symbol, and $x^l(n)$ contains the information for the l-th OFDM symbol.

The construction of $x^l(n)$ is done by combining all the modulated subcarriers used for transmitting data during the time period $[(l-1)\cdot T_{\text{OFDM}}, l\cdot T_{\text{OFDM}}]$. Each subcarrier carries symbols that have been modulated, for example, using QAM. We denote these symbols as b_k^l, where k represents the subcarrier index. These symbols b_k^l are typically used to encode information. The composition of $x^l(n)$ is detailed and visually represented in Figure 2.3.

$$x^l(n) = \sum_{k=0}^{M-1} x_k^l(n) = \sum_{k=0}^{M-1} b_k^l e^{i2\pi kn\Delta f}, \tag{2.4}$$

where $x_k^l(n)$ is the k-th modulated subcarrier of the l-th modulated OFDM symbol, b_k^l being the l-th modulated symbol carried by the k-th modulated subcarrier, M is the number of transmitted subcarriers, Δf is the subcarrier spacing, k is the subcarrier index, and n is the sample index.

Having a time-discrete (sampled) OFDM signal during the time period $[(l-1)\cdot T_{\text{OFDM}}, l\cdot T_{\text{OFDM}}]$ and f_s the sampling rate that is a multiple of the subcarrier spacing ($T_s = 1/f_s = 1/(M\cdot\Delta f)$), the transmitted complex symbol x_k^l can be expressed as in 2.4 using the Inverse Fourier Transform (IFT):

$$x^l(n) = \text{IFT}_M(b_k^l)[n] = x(nT_s) = \sum_{k=0}^{M-1} x_k^l(nT_s) = \sum_{k=0}^{M-1} b_k^l e^{i2\pi k\Delta f nT_s} = \sum_{k=0}^{M-1} b_k^l e^{\frac{i2\pi nk}{M}}, \tag{2.5}$$

for $n \in [0, N-1]$. When IFFT is used instead, the transmitted complex data has the form:

$$x^l(n) = \text{IFFT}_{N_{\text{FTT}}}(b_k^l)[n] = x(nT_s) = \sum_{k=0}^{N_{FFT}-1} {b'}_k^l e^{\frac{i2\pi nk}{N_{\text{FTT}}}}, \tag{2.6}$$

for $n \in [0, N_{\text{FTT}}-1]$, where $N_{\text{FTT}} > M$ and $N_{\text{FTT}} = 2^K, K \in \mathbb{Z}$ with n being the sample index, N_{FTT} being the IFFT size, ${b'}_k^l = \begin{cases} b_k^l & for\ \ 0 \le k < M \\ 0 & for\ \ M \le k < N_{\text{FTT}} \end{cases}$ being the complex data symbol carried by the k-th subcarrier.

The demodulation process is performed the FFT after CP is removed. Considering that the channel maintains the signal, without perturbing, so that $x^l(n) = \sum_{k=0}^{M-1} x_k^l(n) = y^l(n)$ (see Figure 2.3), the demodulated signal is expressed as:

$$\tilde{b}_{k'}^l = \text{FFT}_{N_{\text{FFT}}}(y_n^l)[k'] = \sum_{n=0}^{N_{\text{FFT}}-1} y_n^l e^{-i2\pi\frac{nk'}{N_{\text{FFT}}}} \tag{2.7}$$

$$= \sum_{n=0}^{N_{\mathrm{FFT}}-1} \sum_{k=0}^{N_{\mathrm{FFT}}-1} {b'}_k^l e^{\frac{i2\pi nk}{N_{\mathrm{FFT}}}} e^{-i2\pi \frac{nk'}{N_{\mathrm{FFT}}}}$$

$$= \sum_{k=0}^{N_{\mathrm{FFT}}-1} {b'}_m^k \sum_{n=0}^{N_{\mathrm{FFT}}-1} e^{\frac{i2\pi n(k-k')}{N_{\mathrm{FFT}}}} = \sum_{k=0}^{N_{\mathrm{FFT}}-1} {b'}_k^l \delta(k-k') = b_{k'}^l$$

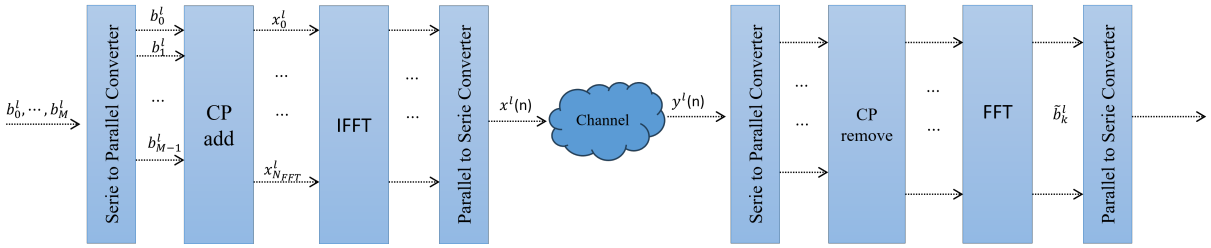


Figure 2.3: OFDM transmission process.

Above all, OFDM modulation offers a significant advantage in multipath environments due to its inherent robustness. It effectively mitigates two key characteristics of multipath environments: frequency selectivity and time dispersion. Frequency selectivity refers to the distortion of the signal caused by echoes of a symbol interfering with itself. This phenomenon can result in signal degradation. Time dispersion, on the other hand, is related to the distortion of the signal due to echoes of a symbol overlapping with the following one. This characteristic can also introduce signal interference and deterioration. Below, the two critical characteristics are explained in detail.

2.1.1.1 Frequency selectivity

Frequency selectivity becomes noticeable when signal replicas arrive at the receiver with a delay that exceeds the inverse of the signal's bandwidth. In simpler terms, this occurs when multipath components reach the receiver with significant delays. Thus, the multipath components arrive with minimal delay, causing only minor distortion in the signal. This type of distortion is referred to as "flat" fading, as it appears relatively constant in the spectral domain and can be corrected with ease.

However, a more challenging scenario occurs when the multipath components arrive with considerable delays, leading to severe distortion in the received signal. Correcting this kind of distortion requires significant computational effort and resources, making it particularly problematic for wideband telecommunications, especially in urban or indoor environments where large bandwidths are utilized. In this context, OFDM is uniquely positioned to combat frequency selectivity effectively. By using narrow bandwidths for each subcarrier, OFDM ensures that fading appears "flat" on each subcarrier, even when the multipath delays are significant. This simplifies the process of channel estimation and correction, also known as channel equalization, enabling more efficient and accurate signal recovery.

2.1.1.2 Time dispersion

Time dispersion, a phenomenon associated with the multipath environment, occurs due to the spreading of the power of symbols over time. To address this distortion, a common solution is

to introduce an interval between consecutive symbols, which helps prevent inter-symbol interference. In the case of OFDM, this interval is filled with a cyclic prefix that precedes the actual OFDM symbol. The cyclic prefix consists of the last N_{CP} samples of the OFDM symbol, effectively extending the total length of the OFDM symbol to $N_{CP} + N_{FFT}$. The specific samples within the cyclic prefix are expressed as:

$$x_n^l = x_{n+N_{\mathrm{FFT}}}^l \qquad -N_{CP} \leqslant n < 0 \tag{2.8}$$

This property plays a crucial role in the demodulation process. Ideally, under perfect synchronization, the start of the FFT window aligns precisely with the beginning of the symbol. In this case, the received signal can be expressed as:

$$y_n^l = \sum_{k=-N_{CP}}^{N_{\mathrm{FFT}}-1} x_k^l(nT_s), \tag{2.9}$$

and with the cyclic prefix removed, leading to the following equation:

$$y_n^l = \sum_{k=0}^{N_{\mathrm{FFT}}-1} x_k^l(nT_s). \tag{2.10}$$

However, if there is a delay in the alignment of the FFT window (synchronization delay), it results in a phase shift during the demodulation process. This phase shift is accounted for:

$$\tilde{b}_{k'}^l = \mathrm{FFT}_{N_{\mathrm{FFT}}}(y_n^l)[k'] = \sum_{n=0}^{N_{\mathrm{FFT}}-1} y_{n+N_s}^l e^{-i2\pi\frac{nk'}{N_{\mathrm{FFT}}}}, \tag{2.11}$$

which depends on the number of samples (N_s) by which the synchronization is delayed. This phase shift in the demodulated symbol can be compensated for effectively using training sequences or pilot symbols, as indicated below:

$$\tilde{b}_{k'}^l = b_{k'}^l e^{\frac{-i2\pi N_s k'}{N_{\mathrm{FFT}}}}. \tag{2.12}$$

Notably, this property can be applied in scenarios involving multipath components, provided that these components fall within the cyclic prefix. The time delay associated with multipath then translates into a phase shift. To recover the signal in the presence of multipath components, suppose the FFT window starts just after the cyclic prefix and has a size of N_{FFT}. The presence of a multipath component in addition to LoS path leads to the received signal model:

$$y_n^l = x_n^l + x_{n-N_\tau}^l, \tag{2.13}$$

where N_τ is the delay in samples between the direct and reflected paths. The corresponding demodulated symbol is derived considering the effect of both LoS and multipath components as:

$$\tilde{b}_{k'}^l = \mathrm{FFT}_{N_{\mathrm{FFT}}}(y_n^l)[k'] = \sum_{n=0}^{N_{\mathrm{FFT}}-1} x_n^l e^{-i2\pi\frac{nk'}{N_{\mathrm{FFT}}}} + \sum_{n=-N_\tau}^{N_{\mathrm{FFT}}-1-N_\tau} x_n^l e^{-i2\pi\frac{(n+N_\tau)k'}{N_{\mathrm{FFT}}}}. \tag{2.14}$$

The result is a demodulated symbol affected by a complex factor, which can be conveniently compensated for using pilot symbols and channel estimation techniques. This property allows

for effective signal recovery even in the presence of multipath components, as long as they fall within the cyclic prefix, effectively converting time delay into manageable phase shifts. The effects and mitigation of both problems with frequency selectivity and time dispersion will be seen implemented in Chapter 6.

2.1.2 Numerology

The characteristics of the OFDM modulation technique discussed earlier are defined by parameters collectively known as "numerology." These numerology parameters include the window size (N_{FFT}), subcarrier spacing (Δf), and the cycle prefix. The subcarrier spacing plays a crucial role in determining the receiver's sampling frequency. This sampling frequency is typically expressed as shown below:

$$f_s = N_{\text{FFT}} \Delta f, \tag{2.15}$$

where f_s represents the sampling frequency, Δf is the subcarrier spacing, N_{FFT} is the total number of subcarriers per symbol used for transmission that coincides with the number of IFFT points used in the OFDM modulatation. The cycle prefix serves as a guard interval to mitigate inter-symbol interference from the previous symbol. Because 5G is designed to operate in a broad frequency range, spanning from below 1 GHz to as high as 100 GHz and supporting a wide range of deployment scenarios and diverse services, single waveform numerology can not fulfill effectively all the requirements of scenarios and services. Therefore, 5G necessitates the support of multiple OFDM numerologies. Table 2.1 provides an overview of the various numerologies supported.

Table 2.1: Supported transmission numerologies [27].

μ	$\Delta f = 2^{\mu} \cdot 15$ [kHz]	Cyclic prefix	OFDM Symbol Duration (μ)	CP Duration (μs)	OFDM Symbol including CP (μs)	Frequency Band
0	15	Normal	66.7	4.7	71.35	FR1
1	30	Normal	33.3	2.3	35.68	FR1
2	60	Normal, Extended	16.7	1.2 (Normal CP)	17.84	FR1/FR2
3	120	Normal	8.33	0.59	8.92	FR2
4	240	Normal	4.17	0.29	4.46	FR2

It is worth noting that in 4G-Long Term Evolution (LTE), a fixed 15 kHz subcarrier spacing is used. However, in 5G, higher subcarrier spacings are introduced, which are particularly suitable for higher carrier frequencies where wider bandwidth is available, and multipath delay is shorter. A reference FFT window size of 2048 is specified in [27]. The maximum bandwidth limited to 400 MHz corresponds to the highest numerology. The following Δf: 15 kHz, 30 kHz, 60 kHz, and 120 kHz lead to corresponding maximum carrier bandwidths of 50 MHz, 100 MHz, 200 MHz, and 400 MHz, respectively. The calculation for the subcarrier spacing is based on the type of numerology and it is given by the formula $\Delta f = 2^{\mu} \cdot 15$ (refer to Table 2.1). Note that, contrary to LTE, where only a single $\Delta f = 15$ kHz was available, in NR, multiple values of Δf are introduced to support frequency ranges and latency constraints. As the numerology value increases, so does the Δf. Importantly, despite variations in subcarrier spacing, the frame duration remains consistent at 10 ms. Consequently, the number of slots and symbols increases with higher Δf values. While lower Δf values require longer CP intervals in absolute time, higher Δf values are better equipped to manage increased phase noise associated with higher frequencies. Moreover, it is also seen how the frame evolves based on different numerologies. Assuming a fixed FFT length of 2048, it is possible to compute the symbol and CP duration of the OFDM from the Table 2.1. It is also worth noting that while higher Δf values are

advantageous in mitigating phase noise effects and frequency errors, they introduce relatively more overhead.

2.1.3 Frame structure

In NR, each frame is structured into 10 subframes, each with a duration of 1 ms. This arrangement combines to form a complete frame of 10 ms. Moreover, each frame can be further divided into two equal halves, creating two half-frames. The first half-frame encompasses the first 5 subframes, while the second half-frame comprises the remaining 5 subframes (see Figure 2.4).

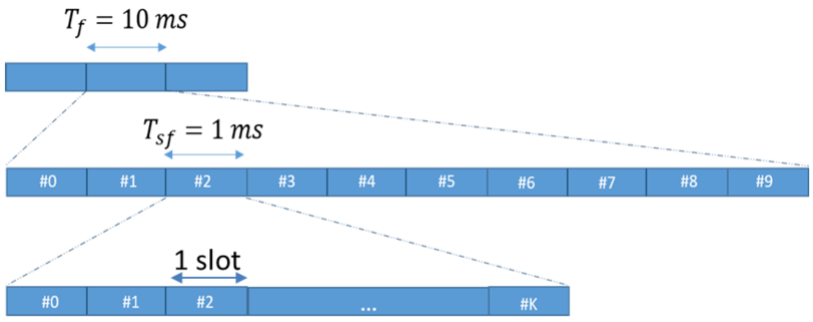


Figure 2.4: Radio frame structure.

Each of these subframes is further subdivided into slots, and the exact number of slots depends on the chosen numerology. Within each slot, there are 14 OFDM symbols, or 12 symbols if an extended CP is employed. As the numerology increases, the number of slots per subframe also increases, and consequently, the number of OFDM symbols varies. Thus, the slot length gets shorter as subcarrier spacing gets wider. This tendency comes from the nature of OFDM. Since the length of one radio frame (10 ms) and one subframe (1 ms) remains consistent, the accommodation for the physical properties of different numerologies is achieved by varying the number of slots within one subframe. This evolution is depicted in Table 2.2. The number of OFDM symbols per subframe is given by the following relation:

$$N_{\text{symb}}^{\text{subframe},\mu} = N_{\text{symb}}^{\text{slot}} N_{\text{slot}}^{\text{subframe},\mu}, \tag{2.16}$$

where $N_{\text{symb}}^{\text{slot}}$ is the number of symbols per slot, i.e. 14 for a normal cycle prefix and 12 for the extended one, and $N_{\text{slot}}^{\text{subframe},\mu}$ is the number of slot per subframe that depends on the subcarrier spacing.

Unlike LTE, which employed a fixed subcarrier spacing of 15 kHz, NR offers the flexibility to choose numerologies, including the initial numerology of $\mu = 0$, which maintains the same subcarrier spacing as LTE. This uniformity in subcarrier spacing ensures compatibility and coexistence between the two generations of technology. Such compatibility is advantageous for devices with a long lifespan, such as Internet of Things (IoT) devices.

Moreover, in NR, the utilization of symbols within each slot is highly flexible, as opposed to the more rigid slot configurations in LTE. In LTE, each slot was dedicated exclusively to either UL or DL, and the allocation of symbols had to conform to these fixed categories. NR, however, introduces a more adaptable approach. In a given slot, each symbol can be independently configured, allowing for a diverse and versatile use of symbols, as depicted in Table 2.3. For

Table 2.2: Radio frame configuration based on numerology.

μ	N_{symb}^{slot}	$N_{slot}^{frame,\mu}$	$N_{slot}^{subframe,\mu}$	T_{slot} [**ms**]
0	14	10	1	1
1	14	20	2	0.5
2	14	40	4	0.25
3	14	80	8	0.125
4	14	160	16	0.0625

instance, in a DL slot format, DL transmissions are confined to "downlink" or "flexible" symbols, ensuring efficient resource utilization for DL data. Similarly, in an UL slot, UL transmissions are restricted to "uplink" or "flexible" symbols, providing the flexibility needed to cater to different communication requirements. This enhanced flexibility in symbol configuration within slots is a distinctive feature of NR, allowing for more efficient use of resources and adaptability to various communication scenarios.

Thus, when operating in Time Division Duplex (TDD) mode, it becomes crucial to precisely establish when transmission and reception phases occur. In LTE TDD, this was achieved through the definition of seven predefined patterns for UL and DL allocation within a radio frame. However, in 5G/NR, the approach differs significantly. Instead of relying on predefined patterns, 5G/NR offers a considerably more flexible method for defining these patterns. This flexibility is achieved by utilizing a set of various parameters, as already illustrated in Table 2.3. Getting into a deeper explanation [29], it can be said that the TDD-UL-DL-configurationCommon parameter plays a critical role in defining the UL and DL configuration within a TDD system. This configuration is determined by several key parameters, including the period, the number of slots in a radio frame, and the number of symbols in each slot. The choice of TDD-UL-DL-configurationCommon can vary significantly based on the specific network requirements, including factors such as traffic patterns, the number of users, and available bandwidth. While most networks typically configure a single pattern within a given period, it is worth noting that 3GPP allows for the configuration of two patterns within the same period, and some real-world networks do make use of this option. Interestingly, it is also permissible by 3GPP standards to forego the configuration of TDD-UL-DL-configurationCommon altogether. However, in practice, most networks do configure this pattern. To ensure smooth operation, it is crucial to allocate sufficient guard time for DL-to-UL switching, also known as the DL-to-UL switching gap. The reason is that some time is needed for DL signal to reach (propagate to) User Equipment (UE). So UE needs some additional time from the end of DL signal. Otherwise, UE may transmit UL signal before it completes the reception of DL signal and, as a result, there would be interference between DL and UL signal. Note that no guard time is needed when switching from UL to DL because DL and UL are always properly aligned thanks to timing advance. That is, 5G NodeB (gNB) referring to Base Station (BS) in NR technology, sends timing advance to make UL signal perfectly aligned in the time domain. The guard time (symbol gabs) value depends on various factors [30], especially the distance between gNB and UE, e.g., a guard period (GP) of 2 symbols would cater for cell sizes of up to 10.7 km, GP of 4 symbols for cell sizes of up to 21.4 km, a GP of 6 symbols for cell sizes of up to 32.1 km etc.

Table 2.3: Slot formats for normal cyclic prefix [28].

	Symbol number in a slot													
Format	0	1	2	3	4	5	6	7	8	9	10	11	12	13
0	D	D	D	D	D	D	D	D	D	D	D	D	D	D
1	U	U	U	U	U	U	U	U	U	U	U	U	U	U
2	F	F	F	F	F	F	F	F	F	F	F	F	F	F
3	D	D	D	D	D	D	D	D	D	D	D	D	D	F
4	D	D	D	D	D	D	D	D	D	D	D	D	F	F
5	D	D	D	D	D	D	D	D	D	D	D	F	F	F
6	D	D	D	D	D	D	D	D	D	D	F	F	F	F
7	D	D	D	D	D	D	D	D	D	F	F	F	F	F
8	F	F	F	F	F	F	F	F	F	F	F	F	F	U
9	F	F	F	F	F	F	F	F	F	F	F	F	U	U
10	F	U	U	U	U	U	U	U	U	U	U	U	U	U
11	F	F	U	U	U	U	U	U	U	U	U	U	U	U
12	F	F	F	U	U	U	U	U	U	U	U	U	U	U
13	F	F	F	F	U	U	U	U	U	U	U	U	U	U
14	F	F	F	F	F	U	U	U	U	U	U	U	U	U
15	F	F	F	F	F	F	U	U	U	U	U	U	U	U
16	D	F	F	F	F	F	F	F	F	F	F	F	U	U
17	D	D	F	F	F	F	F	F	F	F	F	F	U	U
18	D	D	D	F	F	F	F	F	F	F	F	F	U	U
19	D	F	F	F	F	F	F	F	F	F	F	F	F	U
20	D	D	F	F	F	F	F	F	F	F	F	F	F	U
21	D	D	D	F	F	F	F	F	F	F	F	F	F	U
22	D	F	F	F	F	F	F	F	F	F	F	F	U	U
23	D	D	F	F	F	F	F	F	F	F	F	F	U	U
24	D	D	D	F	F	F	F	F	F	F	F	F	U	U
25	D	F	F	F	F	F	F	F	F	F	F	U	U	U
26	D	D	F	F	F	F	F	F	F	F	F	U	U	U
27	D	D	D	F	F	F	F	F	F	F	F	U	U	U
⋮														
62-254	Reserved													
255	UE determines the slot format for the slot based on tdd-UL-DL-CofigurationCommon, or tdd-UL-DL-CofigurationDedicated and if, any, on detected DCI formats.													

2.1.4 Physical resources

Physical resources in the context of wireless communication pertain to the allocated time and frequency resources for each BS or UE to transmit or receive signals. These resources are fundamentally organized within an antenna port, which is further linked to a resource grid. This resource grid is, in turn, comprised of Resource Block (RB)s, and these RBs are made up of individual resource elements. In this section, the fundamental concepts of antenna ports, resource grids, RBs, and resource elements are given.

2.1.4.1 Antenna port

According to the standard organization that develops protocols for mobile telecommunications, the 3GPP, an antenna port is defined in a way that enables us to deduce the channel used to convey a symbol on that antenna port from the channel used for another symbol on the same antenna port. In simpler terms, antenna ports are not directly tied to physical antennas; they are abstract entities distinguished by their unique reference signal sequences. What this means is that you can transmit multiple signals associated with different antenna ports from a single transmit antenna, or conversely, you can distribute the signals from a single antenna port across multiple transmit antennas. This concept is particularly valuable for implementing beamforming using multiple physical antennas, all without requiring the receiver (UE/BS) to have awareness of the specific beamforming process carried out at the transmitter (UE/BS) side.

The assignment of these logical antenna ports to the actual transmit antennas in a base station for instance is a flexible arrangement that is at the discretion of the base station itself. It can vary not only between base stations of the same type due to differing operational conditions but also between base stations from different manufacturers. This flexibility allows for adaptation to the unique characteristics and requirements of each base station.

2.1.4.2 Resource grid

A resource grid consists of RBs, which are further subdivided into resource elements. For each specific numerology and carrier configuration, a resource grid is defined with characteristics denoted as $N_{\text{grid},\chi}^{\text{size},\mu} N_{sc}^{\text{RB}}$ subcarriers and $N_{\text{symb}}^{\text{subframe},\mu}$ OFDM symbols. Here, χ represents either the DL or UL, N_{sc}^{RB} represents the number of subcarriers per RB, and $N_{\text{grid},\chi}^{\text{size},\mu}$ pertains to the carrier bandwidth. It is worth noting that there exists one unique resource grid for each antenna port p, per subcarrier spacing configuration μ, and each transmission direction (DL or UL). This organization allows for the precise allocation and management of resources across the network's various elements and configurations.

2.1.4.3 Resource elements

In the frequency domain, the fundamental physical resource in NR is an individual OFDM symbol on a single subcarrier, known as a resource element (RE). In other words, it represents each element in the resource grid for antenna port p and subcarrier spacing μ. It identifies a specific subcarrier-OFDM symbol (k, l) where k is the index in the frequency domain and l refers to the symbol position in the time domain relative to some reference point. A resource element $(k, l)_{p,\mu}$ corresponds to the complex value $\alpha_{k,l}^{(p,\mu)}$. It is the smallest physical RB (see Figure 2.5).

2.1.4.4 Resource blocks

A RB is defined as a group of $N_{\text{symb}}^{\text{subframe},\mu}$ consecutive OFDM symbols in the time domain and $N_{\text{sc}}^{\text{RB}} = 12$ consecutive subcarriers in the frequency domain (as illustrated in Figure 2.5). In essence, a physical RB is composed of $N_{\text{symb}}^{\text{subframe},\mu} N_{\text{sc}}^{\text{RB}}$ resource elements. These resource elements represent the smallest defined units, each consisting of a single OFDM subcarrier during a single OFDM symbol interval. In contrast to LTE, where there was only one subcarrier

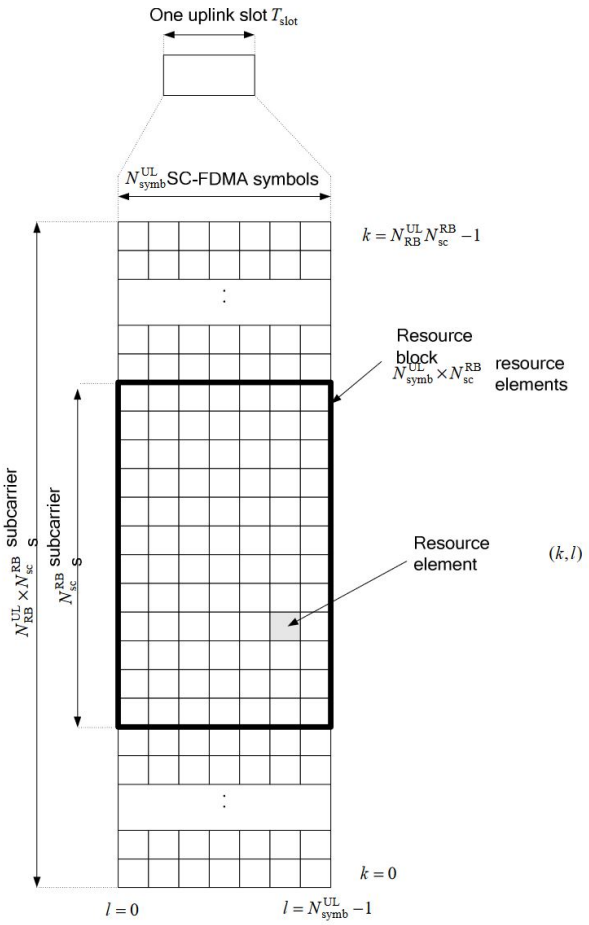


Figure 2.5: Uplink resource grid [24].

spacing, NR offers multiple numerologies, granting flexibility in the duration of transmissions. Therefore, the definition of a RB in NR is primarily provided in the frequency domain. This enhanced flexibility in subcarrier spacing and RB allocation is a distinctive feature of NR, accommodating diverse use cases and applications.

The specification distinguishes four types of RBs: reference RBs, common RBs, physical RBs, and virtual RBs, each of which is detailed in [26]. The differentiation between these blocks becomes significant when mapping physical channels and signals to the resource grid for specific users. Nevertheless, it is important to note that mapping remains achievable even without this differentiation. In other words, physical channels and signals can be effectively mapped by utilizing one or more RBs.

2.1.5 Bandwidth parts

Given the substantial bandwidths in 5G NR, it is impractical for devices to support every available bandwidth. Unlike LTE, where devices primarily worked with a fixed 20 MHz bandwidth, 5G NR allows for component carriers with a maximum bandwidth of 400 MHz. Moreover, 5G NR allows for devices to operate with narrower bandwidths than the configured maximum, which enhances energy efficiency when the full bandwidth is not required. Thus, a key concept introduced in 5G NR is the concept of BandWidth Part (BWP). The primary role of BWPs is to inform a UE about the specific bandwidth it will use to receive data. Each BWP comes with

its subcarrier spacing, which has distinct signal characteristics that enhance spectral and power efficiency.

Figure 2.6 illustrates several benefits and services enabled by this technology. The first use case (up left in the figure) supports reduced energy consumption. By allowing users to use smaller portions of a given carrier, energy consumption per user can be minimized. The second use case (up right in the figure) supports non-contiguous BWPs. Different BWPs within a single carrier can have varying subcarrier spacing. This flexibility enables non-contiguous bandwidth allocation within a carrier. The last use case (down in the figure) supports a non-contiguous spectrum. This feature allows for the insertion of new services in non-contiguous parts of the spectrum.

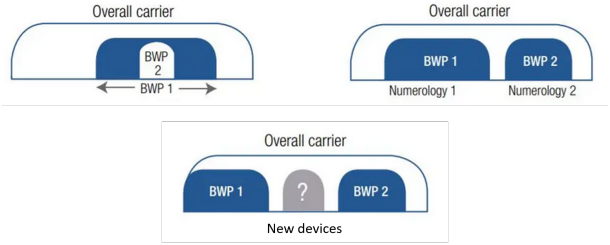


Figure 2.6: 5G NR bandwidth parts.

Each BWP consists of contiguous Common RB within a carrier. It begins at a specified RB. While a device can be configured for up to four different bandwidth parts, only one of them can be active. For the case of UL, a device can transmit on physical channels only within an active BWP. This design ensures efficient and flexible bandwidth utilization in 5G NR.

2.2 5G NR signal model

Many types of reference signals (RS) are used in 5G NR, as explained in section 1.6. As a UL-only signal, the Sounding Reference Signal (SRS) is essential for estimating the channel quality between a UE and a BS. Even though it is not a dedicated signal for positioning like Positioning Reference Signal (PRS) used for DL positioning, in this work we will use the SRS for UL positioning. It plays an important role in NR since the TDD deployment is dominant where gNB can utilize the channel estimation results from SRS not only for UL scheduling but also for DL scheduling based on channel reciprocity in TDD.

The SRS is generated using a low PAPR Zadoff-Chu sequence as outlined in TS 38.211 [24]. This sequence's elements are allocated to specific time and frequency units known with the name Physical Resource Unit (PRU), following a set of configuration rules explained later on.

The configuration of the SRS pattern is defined by a set of parameters defined in signaling messages like the RRC Connection Setup message and RRC Connection Reconfiguration messages:

- $N_{\text{symb}}^{\text{SRS}} \in 1, 2, 4, 8, 12$ known as nrofSymbols and represent consecutive OFDM symbols.
- $l_0 = 8 \sim 13$ represents the starting position in the time domain for the SRS signal given by $l_0 = N\text{symb}^{\text{slot}} - 1 - l_{\text{offset}}$, where $N\text{symb}^{\text{slot}}$ denotes the specific slot within which the SRS signal is transmitted and l_{offset} the offset in question counts symbols backward

from the end of the slot. The latter, $l_{\text{offset}} \geq N\text{symb}^{\text{slot}} - 1$ must be greater than or equal to a reference value $N\text{symb}^{\text{slot}} - 1$. The 3GPP standards reserve the 8th to 13th OFDM symbols within one slot.

- k_0 represents the frequency-domain starting subcarrier index of the SRS signal.
- $K_{\text{TC}} \in 2, 4, 8$ represents the transmission comb number, the subcarrier span between two adjacent Zadoff-Chu sequence entries for the same UE. The SRS is transmitted every K_{TC} subcarriers.
- $M_{\text{SRS}}, C_{\text{SRS}}, B_{\text{SRS}}$ represent bandwidth configuration variables controlling the allocated bandwidth to the SRS. The latter is a parameter that enables or not the frequency hopping. Note that, these parameters collectively impact the selection of the total frequency domain RB number, m_{SRS}, whose values are taken from a predefined table, Table 6.4.1.4.3-1 in [26]. UEs and BSs pre-store this information. Consequently, the BS can extract each UE's SRS signal separately based on the unique allocation pattern.

Upon mapping Zadoff-Chu entries to the appropriate PRUs, a frequency domain SRS OFDM symbol, denoted as X_{SRS}, is formed. According to the configuration rules, SRS signals from different UEs are allocated with orthogonal time and frequency patterns. Moreover, since SRS resources are positioned in a certain interval in the frequency domain, multiple SRS can be interleaved (multiplexed) along the frequency domain occupying the same OFDM symbols.

Finally, the sounding reference signal sequence for an SRS resource (denoted with **a**) is generated according to:

$$\mathbf{a}^{\text{SRS}}_{K_{\text{TC}}k'+k_0,l'+l_0} = \frac{1}{\sqrt{N_{\text{ap}}}}\beta_{\text{SRS}}\mathbf{X}_{\text{SRS}}(k', l'), \tag{2.17}$$

where $k' = 0, 1, \cdots, M^{\text{rs}}_{\text{sc},b} - 1$, $l' = 0, 1, ..., N^{\text{SRS}}_{\text{symb}} - 1$ represents the subcarrier (frequency) index and symbol (time) index of SRS entries. Note that **a** represents the frequency and time domain location of the SRS entry. Additionally, β_{SRS} is a crucial parameter for controlling signal power, and $\sqrt{N_{\text{ap}}}$ corresponds to the logical antenna port number. The subcarrier index, k', varies from 0 to $M^{\text{rs}}_{\text{sc},b}$, where $M^{\text{rs}}_{\text{sc},b}$ is the maximum subcarrier number for the SRS signal, refered to M in this work. This value is determined by $m_{\text{SRS}} \cdot 12/K_{\text{TC}}$. Meanwhile, the symbol index, l', spans from the first SRS symbol to the $(N^{\text{SRS}}_{\text{symb}} - 1)$-th symbol, with a total of $N^{\text{SRS}}_{\text{symb}}$ symbols allocated based on the reference start location, l_0.

For the case of DL, where PRS signal is used, the symbol's location and length are defined by $l^{\text{PRS}}_{\text{start}}$ and L_{PRS}, while the subcarrier index, k', for PRS is selected from Table 7.4.1.7.3-1 in [24] based on the symbol index, l. Note that the PRS subcarrier index varies with the symbol number, in contrast to SRS, where it remains constant.

2.3 System architecture and capabilities

In this section, the overall architecture of the simulator using standard specifications [18], [31] to create simulation environments is presented. The software simulator is based on models and/or experimental measurements to obtain the positioning performance in realistic but generic coverage areas or trajectories. Additionally, it explains how these standard defined environments

are used to simulate 5G positioning by providing 5G ranging and angle observables, position solutions, and power consumption levels for a configured scenario in urban areas together with the main capabilities of the simulator. Finally, the system architecture is composed of four parts: system-level simulation, physical-layer simulation, observable generation, and position computation as depicted in Figure 2.7. The system-level simulation consists of initial network configuration parameters used to determine the link budget, the LoS propagation conditions, and the power consumption levels. The physical-layer simulation is related to the modeled ranging errors using the 3GPP channel models. Note that the computation of angle errors is based on statistical and mathematical principles. The observable generation consists of computation of ranging and angle errors based on the ranging error models and angle error estimations. Lastly, the position computation consists on computing the position solution with the available ranging and angle observables for the 3GPP positioning techniques.

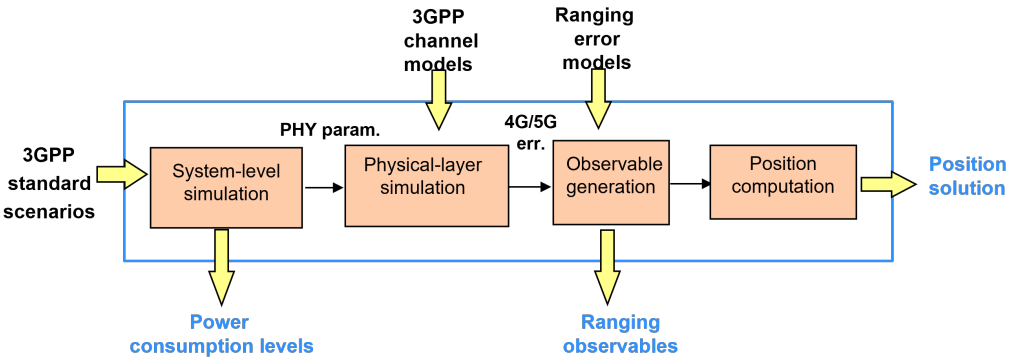


Figure 2.7: General architecture of the simulation tool.

2.3.1 System-level simulation

The system-level simulation tool built upon 3GPP's standard propagation and network models performs various computations, including link budget assessment, propagation conditions analysis, and power consumption evaluation (see Figure 2.8).

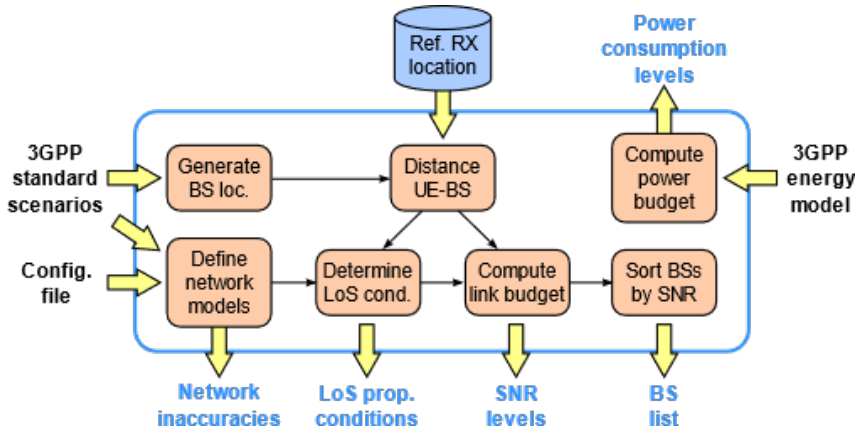


Figure 2.8: Architecture of the system-level simulation tool.

The BS deployment is generated based on the standard hexagonal layout, by following the corresponding network density and Inter-Site Distance (ISD) according to a certain scenario, such as urban, suburban, or rural. The standard ISDs are 1732 m, 500 m, and 200 m for Rural

Macro (RMa), Urban Macro (UMa), and Urban Micro (UMi) cellular deployments respectively. Smaller ISD leads do a denser deployment. The default layout of the 5G network is based in TR 38.855 [18]. This standard hexagonal deployment is used in the BS generator as a regular grid to determine the BS locations. The local coordinates of the cellular grid have an offset of ISD/3 in the x-axis with respect to the local coordinates of the receiver locations, with the scope to set the origin of the receiver's local coordinates in the center of a cell. The process of BS deployment itself involves several steps. Initially, a set of BSs is deployed around each receiver location, following the regular hexagonal grid pattern. The number of BSs initially deployed is determined by a configuration parameter. This parameter is often associated with network tiers, where each tier corresponds to a specific number of BSs. To avoid overlapping BSs in the same location, only one tri-sectorial BS is considered for each cellular grid location. A deployment ratio parameter will define the dominance of the type of scenario: rural deployment ratio r_{rural}, urban deployment ratio r_{urban} and the ratio between UMa and UMi $r_{\text{UMi-UMa}}$, where $r_{\text{UMi-UMa}} = 0$ stands for full UMi deployment and $r_{UMi-UMa} = 1$ stands for full UMa deployment. These ratios are applied by discarding the corresponding number of initially deployed BSs for each scenario. This is done following one of two approaches: discarding BSs based on their distance from receiver locations, with BSs farther from receivers being selected first for removal and the second approach involves randomly discarding the specified number of BSs. The deployment procedure defines the local x and y coordinates of BS and the height is set randomly between an interval defined for each scenario according to the standard [18].

The next step involves determining the conditions of signal propagation between the BS and each UE. It is based on a concept called "UE drops". In this concept, UEs are placed randomly within the coverage area of a predefined deployment scenario. Each drop is an independent single statistical event. A sufficiently high number of drops has therefore to be drawn, usually through Monte-Carlo simulations, in order to obtain a statistical validity of the aggregated results expressed in the form of appropriate metrics. However, this approach is no longer valid in simulations in which mobility is an important factor, e.g. in vehicular environments, or when results have to be obtained in time along a trajectory. Each drop can indeed, in that case, no longer be considered as an independent event, and a more realistic description of the propagation environment is needed. Because the channel parameters do not change rapidly and thus remain relatively constant for several meters, an UE moving along a trajectory or multiple UEs closely separated will experience channel parameters that are correlated. This is typically the case for the LoS conditions, Ricean K-factor, or the shadow fading due to obstruction, e.g. by buildings or trees. A common approach to generate spatially consistent random variables consists in filtering Gaussian-distributed random variables $k(x, y) \sim N(\mu, \sigma^2)$, which is, therefore, a function of the two-dimensional (2D) coordinates of the UE in the horizontal plane. The 2D spatial autocorrelation function of the random process is modeled as an exponential delay function:

$$\rho(d) = e^{-\frac{|d|}{d_{\text{corr}}}}, \tag{2.18}$$

with d being the distance between any two positions and d_{corr} is the decorrelation distance. It is then applied to generate spatially-consistent LoS conditions by correlating the distance-dependent LoS probability models for each BS to later be used to compute the Signal-to-Noise Ratio (SNR) levels from each BS.

This determination is based on the distance between the BS and the UE, and it relies on

specific models that account for the likelihood of LoS connections and path loss as a function of distance. These models are used to assess the quality of the signal link between the BS and each UE. Depending on these propagation conditions (whether LoS or Non Line of Sight (NLoS)), a multipath channel is stochastically generated. The characteristics of this channel, including signal reflections and interference, are generated randomly based on statistical data and parameters (see Table 2.4 where h_{UT} is the antenna height for the User Terminal (UT), $d_{2\mathrm{D}}$ is the 2D distance between BS and UE) provided in reference document [18]. Importantly, this channel modeling is done in a stochastic manner, meaning it incorporates randomness or probability in generating the channel conditions. The LoS propagation generator offers four modes for determining the LoS or NLoS state of the 5G cellular link: LoS only, NLoS only, distance-dependent LoS, and spatially-consistent LoS conditions. Furthermore, the standard

Table 2.4: Propagation conditions based on the type of scenario.

Scenario	LoS probability (distance in meters)
RMa	$Pr_{\mathrm{LoS}} = \begin{cases} 1 & , d_{2\mathrm{D}} \leqslant 10m \\ exp(-\frac{d_{2\mathrm{D}}-10}{1000}) & , 10m < d_{2\mathrm{D}} \end{cases}$
UMa	$Pr_{\mathrm{LoS}} = \begin{cases} 1 & , d_{2\mathrm{D}} \leqslant 18m \\ \left[\frac{18}{d_{2\mathrm{D}}} + exp(-\frac{d_{2\mathrm{D}}}{63})(1-\frac{18}{d_{2\mathrm{D}}})\right](1 + C'(h_{\mathrm{UT}})\frac{5}{4}(\frac{d_{2\mathrm{D}}}{100})^3 exp(-\frac{d_{2\mathrm{D}}}{150})) & , 18m < d_{2\mathrm{D}} \end{cases}$ where $C'(h_{\mathrm{UT}}) == \begin{cases} 0 & , h_{\mathrm{UT}} \leqslant 13m \\ (\frac{h_{\mathrm{UT}}-13}{10})^1.5 & , 13m < h_{\mathrm{UT}} \leqslant 23m \end{cases}$
UMi-Street canyon	$Pr_{\mathrm{LoS}} = \begin{cases} 1 & , d_{2\mathrm{D}} \leqslant 18m \\ \left[\frac{18}{d_{2\mathrm{D}}} + exp(-\frac{d_{2\mathrm{D}}}{36})(1-\frac{18}{d_{2\mathrm{D}}})\right] & , 18m < d_{2\mathrm{D}} \end{cases}$

scenarios play a role in configuring network inaccuracies, such as synchronization offsets between BSs, which is factored into the observable generation tool to be explained later on. The system level tool also computes power consumption budgets, following the methodology defined in TR 45.820 [32] and the link budget denoted by the received power at the BS side defined as:

$$P_{\mathrm{R,[dBm]}} = P_{\mathrm{T,[dBm]}} + G_{\mathrm{T,[dB]}} - (PL_{\mathrm{[dB]}} + SF_{\mathrm{[dB]}} + L_{\mathrm{[dB]}}) + (G_{\mathrm{R,[dB]}} - NF_{\mathrm{[dB]}}), \tag{2.19}$$

with $P_{\mathrm{T,[dBm]}}$ being the transmit power of the UE, $G_{\mathrm{T,[dB]}}$ and $G_{\mathrm{R,[dB]}}$ being the antenna gains of the UE and of the BS, respectively and $NF_{\mathrm{[dB]}}$ corresponding to the BS noise figure expressed as:

$$NF_{\mathrm{[dB]}} = NF_{\mathrm{eq,[dB]}} + 10log_{10}(B), \tag{2.20}$$

where $B = M \cdot \Delta f$ is the bandwidth of the SRS sequence and $NF_{\mathrm{eq,[dB]}} = NF_{0,\mathrm{[dB]}} + 10log_{10}(k \cdot T)$ is the noise figure of the whole reception chain with k is the Boltzmann's constant and $T = 290K$ the standard noise temperature and $NF_{0,\mathrm{[dB]}}$ is the standard noise figure per type of scenario as defined in [26].

2.3.2 Physical-level simulation

The physical-layer simulation tool plays a crucial role in creating 5G ranging error models by simulating physical received signals (available for both DL and UL). This process is referred to as the "physical-layer abstraction of observables" which essentially means modeling observables derived from physical-layer simulations or experimental measurements. It enables easy access to predefined observable models for specific propagation conditions, channel models, system bandwidth, SNR levels, and time-delay estimator without the need for extensive physical-layer simulations or measurements.

The architecture of the physical-layer simulation tool is depicted in Figure 2.9. It follows a specific sequence starting with the simulation of received physical 5G signals (currently available for PRS and SRS signals) to estimate ranging errors across various SNR levels. The simulation is done by convolving one OFDM 5G signal with a multipath channel impulse response (CIR), and by adding Additive White Gaussian Noise (AWGN) for a certain SNR level. Note that a maximum of 4 symbols can be used in one slot according to the standard. However, for this part of the work only one OFDM symbol is considered for both UL and DL to make it compliant with 4G network as well. Then, a conventional threshold-based estimator according to [7] is used to obtain the time-delay measurement τ of the first peak of the correlation between the received signal and the pilots that is above a certain threshold Λ_{thr} which is here defined 6 dB below the maximum peak over a correlation window. The design of threshold is based on [33] and a heuristic approximation of its likelihood is defined as $\Lambda_{\text{thr}} \simeq \frac{1}{4} \cdot \max\{\Lambda_\tau\}$ as denoted in [7]. Finally, the time-delay estimation is computed as:

$$\hat{\tau} = \min_{\tau_{\min} \leqslant \tau < \tau_{\max}} \qquad s.t. \qquad \Lambda(\tau) \geq \Lambda_{\text{th}}. \tag{2.21}$$

In urban scenarios, where the ranging bias is introduced due to the presence of multipath, the threshold-based ranging estimators [33] are considered as widely used techniques for multipath mitigation because of their low complexity. It continues with the computation of the Cumulative Density Function (CDF) of the resulting ranging errors for each SNR level, followed by interpolating this data over the probability and SNR axes. This interpolation process leads to the creation of ranging error models that can be employed to generate 5G ranging observables based on specific SNR levels and probabilities.

The channel models are validated in the tool for Frequency Range 1 (FR1), i.e., 5G cmWave signals. Apart from propagation conditions, the following standard parameters are considered.

- **Pathloss models**. Defined according to the propagation conditions and scenarios in Table 7.4.1-1 of [26]. Note that the distribution of the shadow fading is log-normal, and its standard deviation for each scenario can also be found in Table 7.4.1-1. These models mainly depend on the distance between UT and BS, carrier frequency, street width, and average building height.

- **Shadow fading**. Also known as shadowing, it is defined as the variability in the received power due to signal obstructions, which can be accurately represented as a random Gaussian variable with standard deviation σ_{sf}. A high contribution of shadowing is expected in urban areas, while a reduced standard deviation is expected in flat rural environments.

- **Multipath**. The multipath components can follow random delay distributions or fixed clustered delay line (CDL) models [26]. In the first case, multipath delays are randomly generated following an exponential distribution with a specific delay spread, which is defined in Table 4-5 of [26]. In the second case, the multipath delays are tabulated in [26]. Here, given random or fixed tap delays, time-varying multipath components are used.

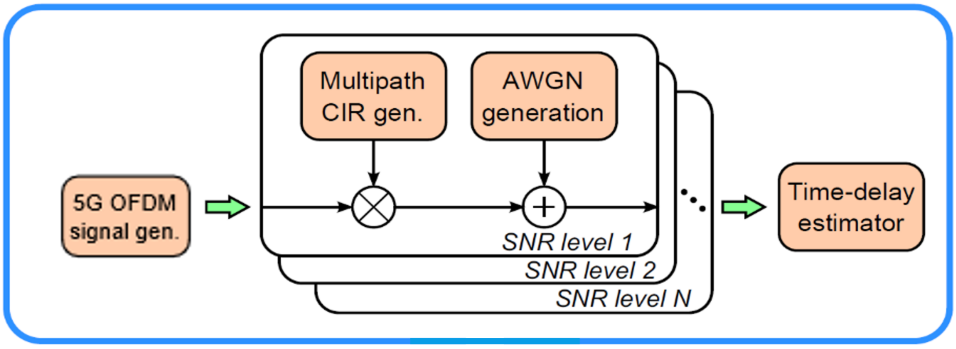


Figure 2.9: Physical-level simulation tool

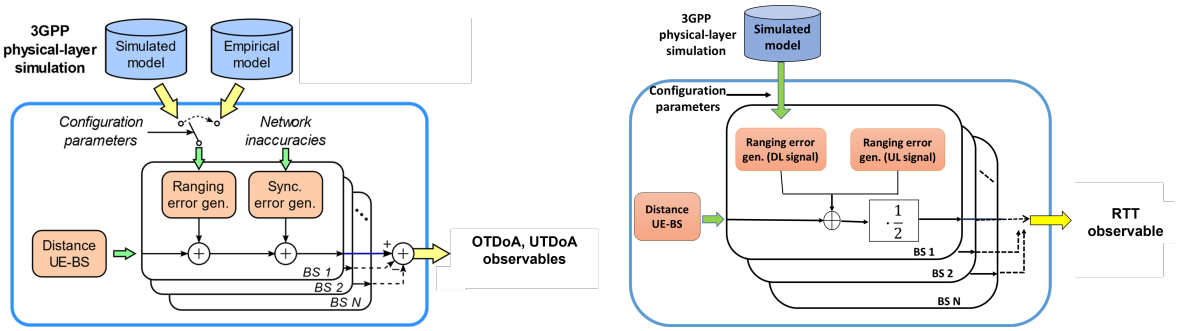
Finally, the general parameters for the computation of SNR values have been agreed on the technical report TR 38.855 [18] and it is summarized in Table 2.5.

Table 2.5: Configuration parameters of the NR positioning support.

Parameter	**Downlink**	**Uplink**
Carrier frequency [GHz]	0.9, 2, 4, 6	
Simulation bandwidth [MHz]	1.4, 5, 10, 20, 50, 100	
Transmit power [dBm]	Below 6GHz: 44	Below 6GHz: 23
	Above 6GHz: 37	Above 6GHz: 21
Tx antenna gain [dBi]	8	0
Rx antenna gain [dBi]	0	8
Rx noise figure [dB]	Below 6GHz: 9	Below 6GHz: 5
	Above 6GHz: 13	Above 6GHz: 7
BS antenna height [m]	35	
UE antenna height [m]	1.5	

2.3.3 Observable generation

The observable generator tool is applied to both UL and DL transmissions for simulated and experimental ranging measurements. Since the computational complexity of the abstraction process also scales with the degrees of freedom, the angle observables, for instance, require an additional dimension for the antenna array orientation with respect to the transmitter, leading to a four-dimensional (4D) interpolator in terms of angle error, antenna array orientation, SNR and probability. Thus, for a simpler process, in this part of the work, angle observables are generated through CRB. Angle estimators are implemented later on in this thesis and integrated into the experimental part, which can be found in Chapter 6.



(a) OTDoA and UTDoA observable generation. (b) RTT observable generation.

Figure 2.10: Architecture of the observable generation tool.

2.3.3.1 Ranging observable

The ranging observable generation (see Figure 2.10) is performed through Monte-Carlo simulations in order to obtain an accurate CDF of the ranging errors. The ranging errors are modeled based on the LoS condition and SNR level as denoted in [26]. Thus, the abstraction procedure is repeated for LoS and NLoS conditions within the set of expected SNR values. In addition, a modification to the TR 38.901 channel model is added in order to consider the NLoS bias as explained in [34]. This is because the 3GPP channel models lack certain representativity or suitability for positioning due to the absence of NLoS bias. As it is discussed in [34], the path delays generated according to [26] are normalized to the first arrival path as:

$$\tau = \text{sort}(\tau' - \min(\tau')) \tag{2.22}$$

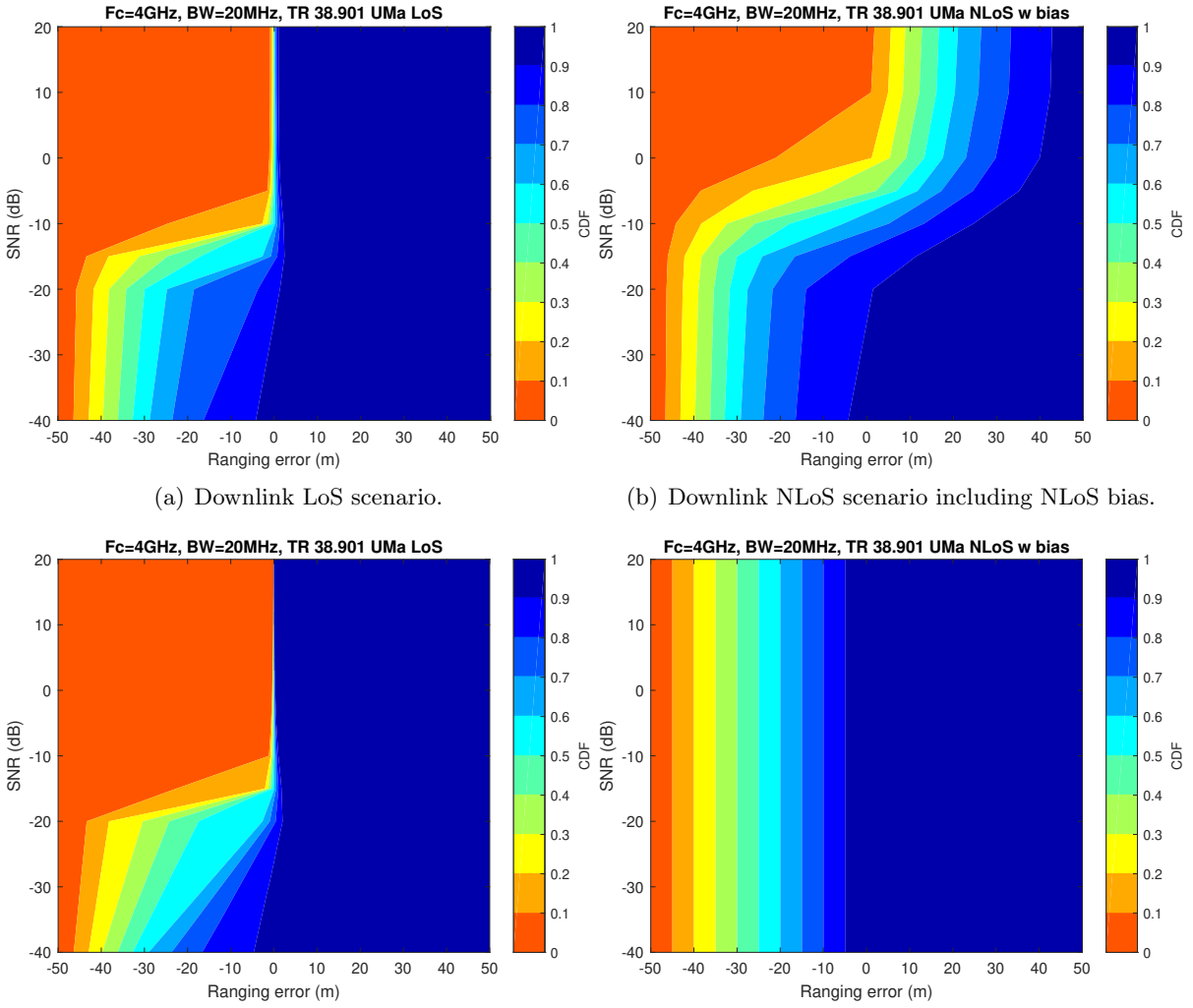
where τ' are the stochastically-generated path delays. This normalization is only valid for LoS conditions. Thus, in order to study the impact of the NLoS bias, the path delay normalization is here removed as:

$$\tau = \text{sort}(\tau'). \tag{2.23}$$

This contribution, which had been done in the group [25], is also considered for the part of UL. However, since this modification is not validated experimentally, it is only used to show the significance of the NLoS bias for positioning evaluations.

Figure 2.11 shows the impact of LoS and NLoS conditions on ranging accuracy. Due to non-regular grid probabilities of ranging errors, a two-dimensional (2D) scattered interpolation is conducted for the set of SNR levels. The example considers the cellular UMa environment with a 5G PRS/SRS system bandwidth of 20 MHz and a carrier frequency of 4 GHz. The resulting interpolation functions/model can be evaluated for a specific SNR level and probability. High ranging accuracy is achievable in LoS conditions. The dominant SNR gain of around 5 dB compared to the spread energy of NLoS channels. It can be said that NLoS bias significantly affects ranging errors, limiting the overall 5G positioning performance. The ranging errors are particularly influenced by multipath in NLoS conditions, especially for SNR levels above -10 dB.

The results show a greater degradation in NLoS scenario for the uplink compared to downlink. This difference is due to worse link budget because of lower transmit power and lower antenna gain in uplink case (refer to the Table 2.5). This will result in larger ranging errors for the uplink part. Moreover, a higher noise figure at the receiver side for the uplink will degrade the



(a) Downlink LoS scenario.

(b) Downlink NLoS scenario including NLoS bias.

(c) Uplink LoS scenario.

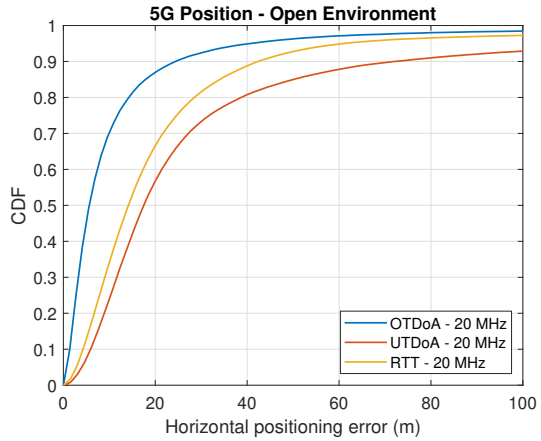
(d) Uplink NLoS scenario including NLoS bias.

Figure 2.11: 2D-interpolated CDF of ranging errors over UMa environments.

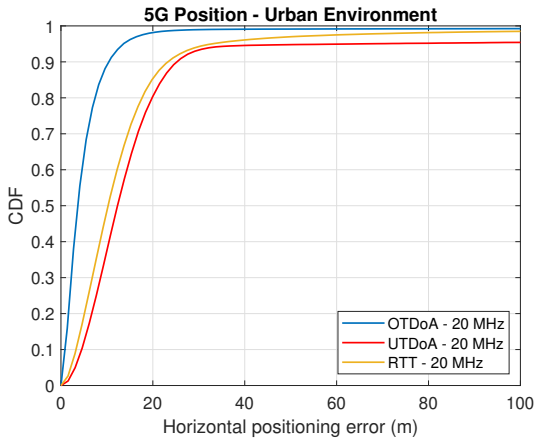
signal to noise ratio, impacting the accuracy of ranging measurements. The path loss has greater variations in NLoS conditions and it tends to increase faster with the increase of distance. The ranging errors for both LoS and NLoS scenarios have been used for estimating the position of UE for the cellular UMa environment.

In order to understand better the effect of NLoS bias in positioning accuracy, for the three main core positioning methods: Observed Time Difference of Arrival (OTDoA), UTDoA and RTT, simulations including or not the NLoS bias are performed. Results depicted in Figure 2.12 show a higher impact in the positioning accuracy for the OTDoA and little degradation for UTDoA and RTT. The small impact of NLoS bias is because of the predominance of LoS links compared to NLoS links in each group of BS considered to estimate each UE position. The increase of NLoS links in a more dense scenario (UMi), keeping the parameter scenarios the same as UMa environment, results in a bigger degradation in the positioning accuracy. The NLoS bias has more impact on RTT than on OTDoA because the signal is transmitted twice over the channel. It can be seen that UTDoA has a significant degradation compared to the other ranging methods due to worse link budget. This phenomenon is seen in both cases: UE location in an open environment with low BS density and UE location in a more dense environment. However,

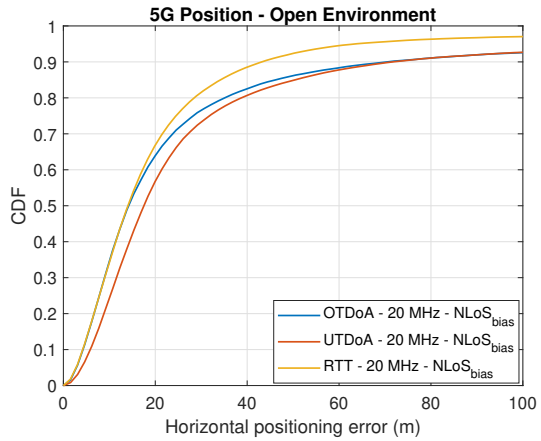
the degradation is higher in open environment than in urban one because of the increasing distance.



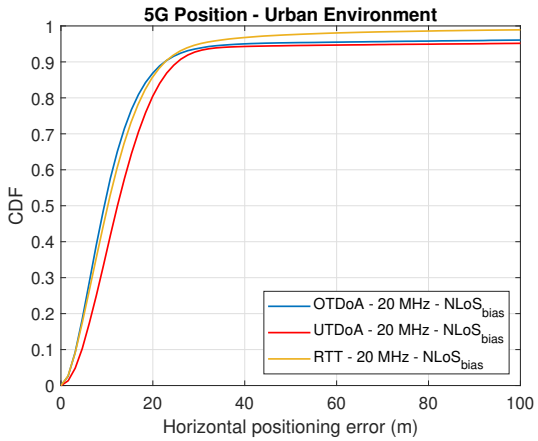
(a) Open environment without NLoS bias.



(b) Urban environment without NLoS bias.

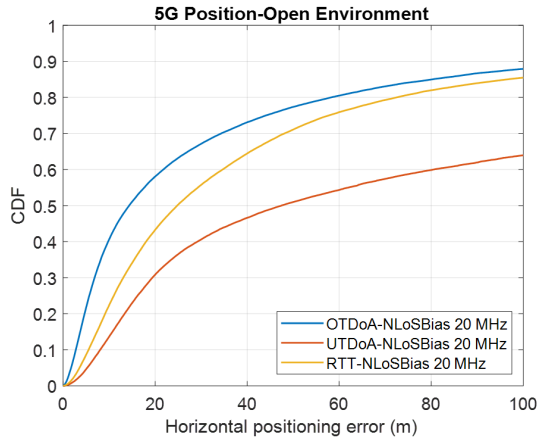


(c) Open environment with NLoS bias.

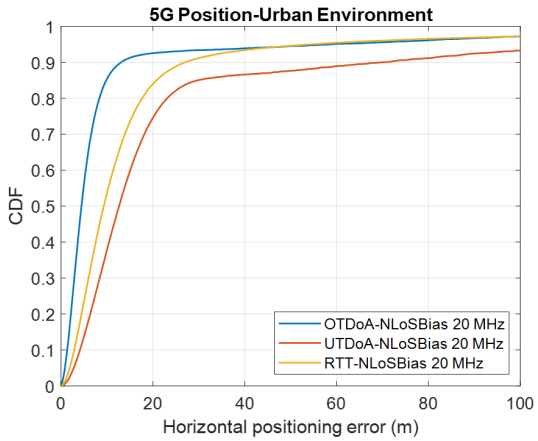


(d) Urban environment with NLoS bias.

Figure 2.12: 5G positioning performance over UMa environments.



(a) Open environment with NLoS bias.



(b) Urban environment with NLoS bias.

Figure 2.13: 5G positioning performance over UMi environments.

The computation of ranging observables is done following the procedure below.

1. Time Difference of Arrival (TDoA) Observable

   The computation process of TDoA observables for both DL and UL is similar. Note that for the calculation of ranging measurements, the pilot signals of PRS are used for the DL part and the pilot signals of SRS for the UL one. The 5G ranging observable from the m-th BS is formulated as

   $$\hat{\rho}_{\text{cell},m} = c\hat{\tau}_{\text{cell},m} = \|\mathbf{x}_{\text{BS},m} - \mathbf{x}_{\text{rx}}\| + c\delta t_{\text{rxcell}} + e_{\text{sync},m} + e_{\text{TDE},m}, \tag{2.24}$$

   where $\hat{\tau}_{\text{cell},m}$ is the time-of-flight of the 5G signal, $\mathbf{x}_{\text{BS},m} = [x_{\text{BS},m}, y_{\text{BS},m}, z_{\text{BS},m}]$ is the m-th BS position, $\mathbf{x}_{\text{rx}} = [x_{\text{rx}}, y_{\text{rx}}, z_{\text{rx}}]$ is the receiver position, δt_{rxcell} is the clock offset of the receiver (referenced to Global Navigation Satellite System (GNSS) time), $e_{\text{sync},m}$ is the BS synchronization error, and $e_{\text{TDE},m}$ is the Time-Delay Estimation (TDE) error. The BS synchronization error $e_{\text{sync},m}$ is modeled following the instructions in TR 38.855 [18]. It is based on a truncated Gaussian distributed random variable with zero mean and standard deviation σ_{sync} within the interval of values $[-2\sigma_{\text{sync}}, 2\sigma_{\text{sync}}]$. For instance, the standard methodology considers a perfect network synchronization with $\sigma_{\text{sync}} = 0$ ns and tight network synchronization with $\sigma_{\text{sync}} = 50$ ns. As already noted, the ranging error models require LoS conditions, the SNR level, and the probability obtained from a uniformly distributed random variable between 0 and 1 for its computation. If the spatial consistency configuration is enabled, this uniformly distributed random probability is also spatially correlated, and the ranging observables generated are also spatially correlated. The m-th TDoA observables are computed as the time difference of ranging observables from the serving and neighbor BSs as

   $$\hat{\rho}_{\text{OTDoA},m} = \hat{\rho}_{\text{cell-DL},1} - \hat{\rho}_{\text{cell-DL},(m+1)}, \tag{2.25}$$

   $$\hat{\rho}_{\text{UTDoA},m} = \hat{\rho}_{\text{cell-UL},1} - \hat{\rho}_{\text{cell-UL},(m+1)}, \tag{2.26}$$

   for $1 \leq m < M_{\text{BS}} - 1$, where $\hat{\rho}_{\text{cell},1}$ is the ranging observable from the serving BS, i.e., the most powerful BS (with the highest SNR) at the receiver position, $\hat{\rho}_{\text{cell},(m+1)}$ is the ranging observable from the $(m+1)$-th neighbor BS, and $M_{\mathbf{BS}}$ is the total number of BSs used for positioning. Thus, the SNR is considered for sorting the list of BSs between serving and neighbor BSs, i.e., from the most to least powerful BS. Note that the subscripts DL and UL are used to distinguish the observables of the downlink from the uplink case.

2. RTT Observable

   Compared to the case of TDoA observable, the computation process of RTT observables takes into account both DL and UL. The m-th 5G RTT observable is formulated as:

   $$\hat{\rho}_{\text{RTT},m} = c\tau_{\text{RTT},m} = \|x_{\text{BS},m} - x_{\text{rx}}\| + e_{\text{RTT},m}, \tag{2.27}$$

   where $\hat{\tau}_{\text{RTT},m}$ is the two-way time-of-flight of the 5G signal, $\mathbf{x}_{\text{BS},m} = [x_{\text{BS},m}, y_{\text{BS},m}, z_{\text{BS},m}]$ is the m-th BS position, $\mathbf{x}_{\text{rx}} = [x_{\text{rx}}, y_{\text{rx}}, z_{\text{rx}}]$ is the receiver position, c is the speed of light, and $e_{\text{RTT},m}$ is the RTT error, which is defined as $e_{\text{RTT},m} \sim \mathcal{N}(0, \sigma^2_{\text{RTT},m})$, where $\sigma^2_{\text{RTT},m}$ is the RTT error variance from the m-th BS. This error variance includes the receiver-transmitter synchronization error, noise errors, and multipath errors. Note that $e_{\text{RTT},m} = \frac{e_{\text{DL_TDE},m} + e_{\text{UL_TDE},m}}{2}$, therefore $\sigma_{\text{RTT},m} = \sqrt{\frac{\sigma^2_{\text{DL_TDE},m} + \sigma^2_{\text{UL_TDE},m}}{4}}$. Thanks to the

two-way transmission between the receiver and transmitter, there is no UE clock offset present in the RTT observables, which relaxes the positioning problem.

2.3.3.2 Angle observable

For the computation of AoA observables, the CRB has been introduced to assess the positioning capabilities in AWGN channel. A Uniform Plannar Array (UPA) antenna (see Figure 2.14) is used to estimate the azimuth and elevation angles.

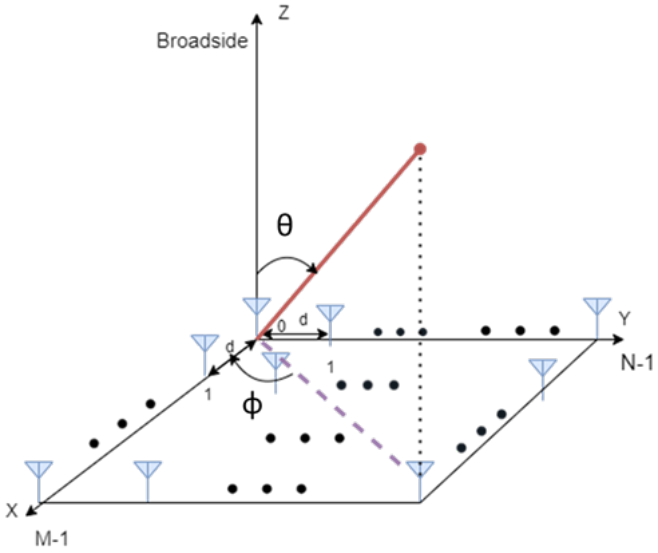


Figure 2.14: UPA structure and AoA representation.

The azimuth angle ϕ is the angle between the x-axis and the orthogonal projection of the vector onto the xy-plane. The elevation angle is the angle between the vector and its orthogonal projection onto the xy-plane. The angle is positive when going toward the positive z-axis from the xy plane. By default, the boresight direction of the array is aligned with the positive z-axis.

To calculate the array direction of BS to UE, which is the angle of incidence at which the signal travels from the TX to the RX, the following steps are used.

- Knowing that the orientation of the BS arrays (β) is set to 3 typical sectors ($0°, 120°, 240°$), the rotation matrix around the x-axis for each of the 3 orientations of BS arrays is computed with the formula:

$$\mathbf{R}_x = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos(\beta) & -\sin(\beta) \\ 0 & \sin(\beta) & \cos(\beta) \end{bmatrix}. \tag{2.28}$$

- The UE-BS vector's position ($\mathbf{P'}_m$) after rotation is computed using the formula:

$$\mathbf{P'}_m = \begin{bmatrix} X' \\ Y' \\ Y' \end{bmatrix} = \mathbf{R}_x \begin{bmatrix} X_{\text{UE}} - X_{\text{BS}} \\ Y_{\text{UE}} - Y_{\text{BS}} \\ Z_{\text{UE}} - Z_{\text{BS}} \end{bmatrix}, \tag{2.29}$$

with $[X_{\text{UE}}, Y_{\text{UE}}, Y_{\text{UE}}]$ and $[X_{\text{BS}}, Y_{\text{BS}}, Y_{\text{BS}}]$ being the position coordinates of UE and BS respectively.

- The angle between vector position $\mathbf{P'}_m$ and the unit vector $\mathbf{v} = [0, 0, 1]^T$ that corresponds to the direction of the array (z-axis) is computed as:

$$\angle\zeta_{m,\beta} = \cos^{-1}\left(\frac{\mathbf{v}^T\mathbf{P'}_m}{\|\mathbf{v}^T\mathbf{P'}_m\|}\right), \tag{2.30}$$

  The array orientation β is chosen as the one that yields the smallest angle ($\angle\zeta$).

- Then, the computation of the azimuth and elevation angles in the local system is done using the following formulas:

$$\varphi_m = \text{atan2}\left(\frac{Y'}{X'}\right), \tag{2.31}$$

$$\theta_m = \text{acos}\left(\frac{Z'}{d}\right), \tag{2.32}$$

  where $d = \sqrt{X'^2 + Y'^2 + Z'^2}$, and β being the array orientation computed in 2.30. Both estimated angles are expressed in radians.

- Finally, the angular estimation is done mathematically through CRB formulas for a channel with only a LoS signal following the process depicted in [35]:

$$\sigma^2_{\theta_m,\text{CRB}} = \frac{6}{C/\sigma^2 MNN_s\left(\frac{w_c d}{c}\right)^2\cos^2\theta_m}\frac{1}{[(N^2-1)\sin^2\varphi_m + (M^2-1)\cos^2\varphi_m]}, \tag{2.33}$$

$$\sigma^2_{\phi_m,\text{CRB}} = \frac{6}{C/\sigma^2 MNN_s\left(\frac{w_c d}{c}\right)^2\sin^2\theta_m}\frac{1}{[(N^2-1)\cos^2\varphi_m + (M^2-1)\sin^2\varphi_m]}, \tag{2.34}$$

  where $w_c = 2\pi f_c$, C/σ^2 is the m-th SNR of the 5G signal at m-th BS and N_s is the number of subcarriers per bandwidth allocated. Note that increasing the number of antenna elements reduces the angle errors. Thus, the m-th 5G AoA observables of elevation and azimuth are computed using the following formulas, respectively:

$$\theta_{obs,m} = \angle\text{A}_{\theta_m} + \sigma_{\theta_m}\cdot\alpha, \quad \alpha \sim N(\mu, \sigma^2), \tag{2.35}$$

$$\phi_{obs,m} = \angle\text{A}_{\phi_m} + \sigma_{\phi_m}\cdot\beta, \quad \beta \sim N(\mu, \sigma^2), \tag{2.36}$$

  where σ_{θ_m} and σ_{ϕ_m} are the angle errors calculated in (2.34) and (2.33), $\angle\text{A}_{\theta_m}$ and $\angle\text{A}_{\phi_m}$ are the azimuth and elevation angles calculated in (2.31) and (2.32), respectively.

The hybrid observables are composed of both the TDoA and AoA observables, whose implementation will be seen more in detail in Chapter 5.

2.3.4 Position computation

The position computation tool estimates the position using the ranging/angle observables computed in 2.3.3. Note that the ranging errors are simulated or empirical ranging error models. The empirical ranging error models are provided from real experimentations. The positioning computation in this work is based on a Weighted Least Squares (WLS) algorithm. Four main positioning techniques from the 5G standard in TS 38.305 [21]: OTDoA (DL), UTDoA (UL),

RTT, AoA and Hyb (joint UTDoA/AoA) are implemented in the simulator as the core positioning method and Cell IDentity (CID) as fallback technology. This means that, when the 3D position solution of the core positioning algorithms does not converge due to bad geometry, outlier measurements, or a lack of measurements, the 3D estimated receiver position is obtained using the CID method. In this case, the position of the most powerful base station (with the highest SNR) is assigned to the estimated receiver position. The position computation of each of the methods is done as follows.

2.3.4.1 TDoA positioning algorithm

Given the known location of the base stations, the unknown 3D receiver position $x = [x, y, z]^T$ is solved using the WLS classical solution of the OTDoA/TDoA positioning problem, utilizing the iterative Gauss-Newton (GN) method. The GN solution at the l-th iteration is defined as

$$\hat{\mathbf{x}}_l = \hat{\mathbf{x}}_{l-1} + \left(\mathbf{G}^T_{\text{TDoA},l-1}\mathbf{W}^{-1}_{\text{TDoA}}\mathbf{G}_{\text{TDoA},l-1}\right)^{-1}\mathbf{G}^T_{\text{TDoA},l-1}\mathbf{W}^{-1}_{\text{TDoA}}\left(\rho(\hat{\mathbf{x}}_{l-1}) - \hat{\rho}\right), \tag{2.37}$$

where $\mathbf{G}_{\text{TDoA}}$ is the $(M_{\text{BS}} - 1) \times 3$ geometry matrix, W is the weighting matrix, $\rho(\hat{\mathbf{x}}_{l-1}) = \left[\rho_1(\hat{\mathbf{x}}_{l-1}), \rho_2(\hat{\mathbf{x}}_{l-1}), \ldots, \rho_{(M_{\text{BS}}-1)}(\hat{\mathbf{x}}_{l-1})\right]^T$ with $\rho_m(\hat{\mathbf{x}}_{l-1}) = \|\mathbf{x}_{(\text{BS},1)} - \hat{\mathbf{x}}\| - \|\mathbf{x}_{(\text{BS},(m+1))} - \hat{\mathbf{x}}\|$ for $1 \leq m < M_{\text{BS}} - 1$, $\hat{\rho} = \left[\hat{\rho}_{\text{TDoA},1}, \hat{\rho}_{\text{TDoA},2}, \ldots, \hat{\rho}_{\text{TDoA},(M_{\text{BS}}-1)}\right]^T$ is the vector of TDoA observables for both DL and UL. The geometry matrix itself is defined as:

$$[\mathbf{G}]_{m,1:3} = \left[\frac{\mathbf{x}_{(\text{BS})} - \hat{\mathbf{x}}}{\|\mathbf{x}_{(\text{BS},1)} - \hat{\mathbf{x}}\|} - \frac{\mathbf{x}_{(\text{BS},(m+1))} - \hat{\mathbf{x}}}{\|\mathbf{x}_{(\text{BS},(m+1))} - \hat{\mathbf{x}}\|}\right] \text{ for } 1 \leq m < M_{\text{BS}} - 1, \tag{2.38}$$

and the weighting matrix is formed by the weighting coefficients of the OTDoA/UTDoA observables as

$$\mathbf{W} = \begin{bmatrix} \sigma^2_{\text{cell},1} + \sigma^2_{\text{cell},2} & \sigma^2_{cell,1} & \cdots & \sigma^2_{cell,1} \\ \sigma^2_{\text{cell},1} & \sigma^2_{\text{cell},1} + \sigma^2_{\text{cell},3} & \cdots & \sigma^2_{\text{cell},1} \\ \vdots & \vdots & \ddots & \vdots \\ \sigma^2_{\text{cell},1} & \sigma^2_{\text{cell},1} & \cdots & \sigma^2_{\text{cell},M_{\text{BS}}} \end{bmatrix}, \tag{2.39}$$

where $\sigma^2_{\text{cell},m}$ is the variance of the m-th BS ranging observable. The simulator allows three different weight configurations to define the variance.

- Identical weights. The variance of the m-th BS ranging observable is set to 1, i.e., $\sigma^2_{\text{cell},m} = 1$, resulting in the Least Squares (LS) algorithm. Note that this is the worst case.
- Known error variance. The variance of the m-th BS ranging observable is determined based on the known TDE error variance $\sigma^2_{\text{TDE},m}$ and the network synchronization error variance σ^2_{sync} as $\sigma^2_{\text{cell},m} = \sigma^2_{\text{TDE},m} + \sigma^2_{\text{sync}}$. Note that this configuration represents more realistic conditions.
- Known errors. The variance of the m-th BS ranging observable is approximated using known TDE and synchronization errors as $\sigma^2_{\text{cell},m} \approx |e_{\text{TDE},m} + e_{\text{sync},m}|^2$. Note that this configuration represents more ideal conditions.

2.3.4.2 RTT positioning algorithm

For the RTT positioning method, similar to the previous methods, the unknown 3D receiver position $\mathbf{x} = [x, y, z]^T$ is determined using the WLS classical solution. The GN solution at the l-th iteration is defined as:

$$\hat{\mathbf{x}}_l = \hat{\mathbf{x}}_{l-1} + \left(\mathbf{G}_{\text{RTT},l-1}^T \mathbf{W}_{\text{RTT}}^{-1} \mathbf{G}_{\text{RTT},l-1}\right)^{-1} \cdot \mathbf{G}_{\text{RTT},l-1}^T \mathbf{W}_{\text{RTT}}^{-1} \left(\boldsymbol{\rho}(\hat{\mathbf{x}}_{l-1}) - \hat{\boldsymbol{\rho}}\right), \tag{2.40}$$

with $\mathbf{G}_{\text{RTT}}$ being the $(M_{\text{BS}} - 1) \times 3$ geometry matrix, $\mathbf{W}_{\text{RTT}}$ the diagonal weighting matrix, $\boldsymbol{\rho}(\hat{\mathbf{x}}_{l-1})$ the vector of RTT observables represented as $[\rho_1(\hat{\mathbf{x}}_{l-1}), \rho_2(\hat{\mathbf{x}}_{l-1}), \ldots, \rho_{M_{\text{BS}}}(\hat{\mathbf{x}}_{l-1})]^T$, where $\rho_m(\hat{\mathbf{x}}_{l-1}) = \|\mathbf{x}_{\text{BS},m} - \hat{\mathbf{x}}\|$ for $1 \leq m < M_{\text{BS}}$ and $\hat{\boldsymbol{\rho}} = [\hat{\rho}_{\text{RTT},1}, \hat{\rho}_{\text{RTT},2}, \ldots, \hat{\rho}_{\text{RTT},M_{\text{BS}}}]$ being the vector of RTT observables. The geometry matrix is defined as:

$$[\mathbf{G}]_{m,1:3} = \frac{\mathbf{x}_{\text{BS},m} - \hat{\mathbf{x}}}{\|\mathbf{x}_{\text{BS},m} - \hat{\mathbf{x}}\|}, \text{ for } 1 \leq m < M_{\text{BS}}. \tag{2.41}$$

The weighting matrix is constructed using the weighting coefficients of the RTT observables as:

$$\mathbf{W} = \begin{bmatrix} \sigma_{\text{RTT},1}^2 & 0 & \ldots & 0 \\ 0 & \sigma_{\text{RTT},2}^2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \sigma_{\text{RTT},M_{\text{BS}}}^2 \end{bmatrix}, \tag{2.42}$$

where $\sigma_{\text{RTT},m}^2$ represents the variance of the m-th BS ranging observable. The weight configuration options to define the variance are similar to the previous case. Note that for the realistic conditions, the variance of the m-th BS ranging observable is determined from the known TDE error variance of the DL $\sigma_{\text{DL_TDE},m}^2$ and the UL signal $\sigma_{\text{UL_TDE},m}^2$ as $\sigma_{\text{RTT},m}^2 = (\sigma_{\text{DL_TDE},m}^2 + \sigma_{\text{UL_TDE},m}^2)/4$, while in ideal conditions it is approximated as $\sigma_{\text{RTT},m}^2 \approx |(e_{\text{DL_TDE},m} + e_{\text{UL_TDE},m})/2|^2$.

2.3.4.3 AoA positioning algorithm

The computation solution of the unknown 3D receiver position with known height using the AoA positioning algorithm is solved based on the classical WLS through the well-known GN method. Similar to the previous methods, the GN solution at the l-th iteration is defined as:

$$\hat{\mathbf{x}}_l = \hat{\mathbf{x}}_{l-1} + \left(\mathbf{G}_{\text{AoA},l-1}^T \mathbf{W}_{\text{AoA}}^{-1} \mathbf{H}_{l-1}\right)^{-1} \mathbf{G}_{\text{AoA},l-1}^T \mathbf{W}_{\text{AoA}}^{-1} \mathbf{b}, \tag{2.43}$$

Where $\mathbf{G}_{\text{AoA}}$ is the geometry matrix calculated as explained in 2.A, $\mathbf{W}_{\text{AoA}}$ is the weighting matrix defined as:

$$\mathbf{W}_{\text{AoA}} = \text{diag}(\sigma_{\phi_m,\text{CRB}}, \sigma_{\theta_m,\text{CRB}}), \tag{2.44}$$

where $\sigma_{\phi_m,\text{CRB}}$ and $\sigma_{\theta_m,\text{CRB}}$ are computed in 2.33 and 2.34 respectively, the $\mathbf{b}$ is the vector of residuals $\mathbf{b} = [b_{\phi_m}; b_{\theta_m}]$, being the difference between angle estimation and AoA observables, where the residuals are wrapped in radians to $[-\pi, \pi]$. Even for the angle-based method, three weight configurations are available whose computation is similar to the previous cases. Note that for the known error variance case, the m-th BS angle observable variance is defined from the inverse of the angular estimation (azimuth and elevation) computed mathematically through

CRB formulas in 2.33 and 2.34. The computation method considered only the LoS signal. The effect of multipath is considered just adding a very small bias to the angle observables. For the case of known errors, it is approximated with known azimuth and elevation angle errors.

Finally, the position computation using the hybrid-based method is solved based on the WLS solution through the GN method similar to the approach followed in the previous methods. Note that for the hybrid case, the geometry matrix $\mathbf{G}_{\text{Hyb}}$ is a M'_{BS}x3 matrix composed by the $[\mathbf{G}_{\text{TDoA}}, \mathbf{G}_{\text{AoA}}]^T$ where $M'_{\text{BS}} = M_{\text{BS}_{\text{TDoA}}} + M_{\text{BS}_{\text{AoA}}}$, $\mathbf{W}_{\text{Hyb}} = \text{blkdiag}(\mathbf{W}_{\text{TDoA}}, \mathbf{W}_{\text{AoA}})$ being the weighting matrix composed by the weighting matrix of TDoA method and AoA method, and the residuals are composed by the vector of residuals of TDoA and AoA method.

2.4 5G parametric elements

2.4.1 Dilution of precision

In a positioning system that relies on either range or angle measurements, the spatial distribution of the base stations plays a critical role in determining the accuracy of the positioning results. This relationship between the distribution of base stations and the resulting accuracy is often quantified using a parameter known as DOP. DOP serves to characterize how measurement errors translate into errors in determining the precise position. This is typically assessed with the Geometric Dilution of Precision (GDOP). A smaller GDOP is inherently more desirable. A low GDOP signifies that minor variations or inaccuracies in measurements will not lead to significant errors in the resulting location estimation. Since we are dealing with terrestrial systems in this work, it is worth noting that the effective planning of the location and quantity of base stations within the desired coverage area plays a pivotal role. Failure to carefully plan these aspects can lead to the predominance of GDOP's influence, significantly constraining the system's performance. When the angular positions of base stations are in close proximity, the GDOP value tends to be elevated, leading to suboptimal positioning performance. To achieve a high degree of positional accuracy, it is important that the base stations are strategically positioned in a manner that envelops the UE with a network of base stations. In a AoA system, as the distance between the base station and the mobile station increases, the AoA measurement error grows. In a TDoA system, the range measurement error typically remains consistent under ideal conditions when the lines connecting the mobile station to the base stations form a right angle. In the context of a combined system utilizing both AoA and TDoA measurements, the GDOP increases as the mobile station moves farther from the base station. This is based on the assumption that a single base station can provide both AoA and TDoA measurements. Moreover, the additional use of AoA observables with the TDoA observables improves the geometry.

Depending on the specific requirements of a positioning system, GDOP can be further dissected into various components such as Horizontal Dilution of Precision (HDOP) and Vertical Dilution of Precision (VDOP) for 3D positioning. Since we are dealing with terrestrial deployment, we are only interested in the horizontal positioning and therefore in the HDOP. This parameter for the joint TDoA-AoA is calculated following the derivations in [36], defined as:

$$\text{HDOP} = \sqrt{\mathbf{P}_{1,1}^{-1} + \mathbf{P}_{2,2}^{-1}}, \tag{2.45}$$

where

$$\mathbf{P} = k_\phi^2 \mathbf{G}_\phi^T \mathbf{G}_\phi + k_\theta^2 \mathbf{G}_\theta^T \mathbf{G}_\theta + \mathbf{G}_{\text{TDoA}}^T \mathbf{G}_{\text{TDoA}}, \tag{2.46}$$

with $\mathbf{G}_\phi$, $\mathbf{G}_\theta$, and $\mathbf{G}_{\text{TDoA}}$ being the geometry matrix of elevation angles, azimuth angles, and time delays, respectively, computed as in (2.61) and (2.38), k_ϕ and k_θ representing the relationship between variance of time delays with variance of angles (elevation and azimuth, respectively), defined as:

$$k_\phi = \frac{\sigma_{\text{TDoA}}}{\sigma_\phi}, k_\theta = \frac{\sigma_{\text{TDoA}}}{\sigma_\theta}. \tag{2.47}$$

These coefficients serve to make the GDOP of AoA dimensionless and comparable to the GDOP of the TDoA. The GDOP value for the angle part can be obtained by extracting the first two terms of the sum in (2.46) and then using the result in (2.45). The same method also works for the calculation of GDOP for the time delay part separately. In this case, only the third term of the sum in (2.46) is needed. Smaller values of GDOP are preferred, meaning that small changes in the measurement will not result in large errors in the location output.

2.4.2 Fisher information and bounds for localization

The CRB for TDoA, AoA, and a combination of Time of Arrival (ToA) and AoA (ToA/AoA) localization provide a lower bound on the achievable positioning accuracy when obtaining time-delay and angle measurements with antenna arrays at different network sites. Note that a Uniform Rectangular Array (URA) antenna is considered for the above computations. The position accuracy is defined by the Root-Mean-Square Error (RMSE) of the position estimate $\hat{\mathbf{x}}$ and it is bounded by the square root of the CRB of the position $\mathbf{x}$ with ranging, angle or joint measurements as:

$$\epsilon_{\mathbf{x},\text{TDoA}} = \sqrt{E[\|\hat{\mathbf{x}} - \mathbf{x}\|]^2} \geq \sqrt{\text{tr}\{\mathbf{CRB}_{\text{TDoA}}(\mathbf{x})\}}, \tag{2.48}$$

$$\epsilon_{\mathbf{x},\text{AoA}} = \sqrt{E[\|\hat{\mathbf{x}} - \mathbf{x}\|]^2} \geq \sqrt{\text{tr}\{\mathbf{CRB}_{\text{AoA}}(\mathbf{x})\}}, \tag{2.49}$$

$$\epsilon_{\mathbf{x},\text{Joint}} = \sqrt{E[\|\hat{\mathbf{x}} - \mathbf{x}\|]^2} \geq \sqrt{\text{tr}\{\mathbf{CRB}_{\text{Joint}}(\mathbf{x})\}}, \tag{2.50}$$

where $E[\cdot]$ is the expectation and $\text{tr}\{\cdot\}$ is the trace operator. The CRB is calculated from the inverse Fisher Information Matrix (FIM) $\mathbf{J}$. Therefore, the Equivalent Fisher Information Matrix (EFIM) for the joint TDoA and AoA positioning is:

$$\mathbf{J}_{\text{Joint}}(\mathbf{x}) = \mathbf{J}_{\text{TDoA}}(\mathbf{x}) + \mathbf{J}_{\text{AoA}}(\mathbf{x}), \tag{2.51}$$

where the joint EFIM is decoupled into the EFIM for TDoA positioning $\mathbf{J}_{\text{TDoA}}(\mathbf{x})$ and the EFIM for AoA positioning $\mathbf{J}_{\text{AoA}}(\mathbf{x})$. The EFIM for TDoA positioning is defined as:

$$\mathbf{J}_{\text{TDoA}}(\mathbf{x}) = \mathbf{G}_{\text{TDoA}}^T \mathbf{C}_{\text{TDoA}}^{-1} \mathbf{G}_{\text{TDoA}}, \tag{2.52}$$

where $\mathbf{G}_{\text{TDoA}}$ is a $M_{\text{BS}} \times 3$ matrix defined as in 2.38 and $\mathbf{C}_{\text{TDoA}}$ is a $M_{\text{BS}} \times M_{\text{BS}}$ square matrix expressed as shown in appendix 2.B:

$$\mathbf{C} = \begin{pmatrix} \sigma^2_{1,\text{ToA}} + \sigma^2_{2,\text{ToA}} & \sigma^2_{1,\text{ToA}} & \cdots & \sigma^2_{1,\text{ToA}} \\ \sigma^2_{1,\text{ToA}} & \sigma^2_{1,\text{ToA}} + \sigma^2_{3,\text{ToA}} & \cdots & \sigma^2_{1,\text{ToA}} \\ \vdots & \vdots & \ddots & \vdots \\ \sigma^2_{1,\text{ToA}} & \sigma^2_{1,\text{ToA}} & \cdots & \sigma^2_{1,\text{ToA}} + \sigma^2_{M_{\text{BS}},\text{ToA}} \end{pmatrix}, \tag{2.53}$$

where $\sigma^2_{m,\text{ToA}}$ is the time estimation done mathematically through the CRB formula for a channel estimation with only a LoS signal following the process depicted in [35]:

$$\sigma^2_{\text{ToA}_m,\text{CRB}} = \frac{6c^2}{C/\sigma^2 MNN_s(N_s^2 - 1)(2\pi\Delta f K_{\text{TC}})}, \tag{2.54}$$

with C/σ^2 being the m-th SNR of the 5G signal at m-th BS. The EFIM for AoA positioning is expressed as:

$$\mathbf{J}_{\text{AoA}}(\mathbf{x}) = \mathbf{G}^T_{\text{AoA}} \mathbf{C}^{-1}_{\text{AoA}} \mathbf{G}_{\text{AoA}}, \tag{2.55}$$

where $\mathbf{G}_{\text{AoA}}$ is a $M'_{\text{BS}} \times 3$ matrix defined as in 2.61 and $\mathbf{C}_{\text{AoA}}$ is a $M'_{\text{BS}} \times M'_{\text{BS}}$ square matrix expressed as:

$$\mathbf{C}_{\text{AoA}} = \text{blkdiag}(\text{diag}(\sigma^2_{1,\text{AoA}}, \sigma^2_{2,\text{AoA}}, \cdots, \sigma^2_{\theta_m,\text{AoA}}), \text{diag}(\sigma^2_{1,\text{AoA}}, \sigma^2_{2,\text{AoA}}, \cdots, \sigma^2_{\phi_m,\text{AoA}})), \tag{2.56}$$

where $\sigma^2_{\theta_m,\text{AoA}}$ and $\sigma^2_{\phi_m,\text{AoA}}$ are the angle estimation (azimuth and elevation respectively) computed mathematically through the CRB formulas in 2.33, 2.34.

Therefore, the CRB for TDoA positioning, i.e., when using only time-delay measurements, is defined as:

$$\mathbf{CRB}_{\text{TDoA}}(\mathbf{x}) = \mathbf{J}^{-1}_{\text{TDoA}}. \tag{2.57}$$

The use of multiple antennas is equivalent to the use of multiple measurements in terms of position accuracy with TDoA localization, which is expressed as:

$$\epsilon_{\mathbf{x},\text{TDoA}} \geq \sqrt{\text{tr}\{\mathbf{CRB}_{\text{TDoA}}(\mathbf{x})\}}. \tag{2.58}$$

In the case of using only angle measurements, the CRB for AoA positioning is defined as:

$$\mathbf{CRB}_{\text{AoA}}(\mathbf{x}) = \mathbf{J}^{-1}_{\text{AoA}}, \tag{2.59}$$

and the position accuracy is:

$$\epsilon_{\mathbf{x},\text{AoA}} \geq \sqrt{\text{tr}\{\mathbf{CRB}_{\text{AoA}}(\mathbf{x})\}}. \tag{2.60}$$

Having a look at $\mathbf{J}_{\text{TDoA}}$ and $\mathbf{J}_{\text{AoA}}$, the distance between UE and BS, and the distance between antenna elements of the array has a higher impact on the EFIM for AoA positioning than on the EFIM for TDoA positioning. Consequently, in the context of joint TDoA/AoA positioning, the CRB is predominantly influenced by the ToA measurements, particularly when dealing with high signal bandwidth scenarios. On the other hand, the AoA measurements assume greater significance in situations characterized by shorter distances between the UE and BS, coupled with a higher number of antenna elements. Moreover, the joint TDoA and AoA approach offers the advantage of determining the UE's location with fewer sites compared to the TDoA approach.

2.4.3 5G signal bandwidth

With the simulator, it is possible to use any bandwidth up to 100 MHz since it operates only in the FR1. The bandwidth of the 5G signal is a pivotal factor influencing the achievable accuracy in range estimation within positioning systems. In the context of AWGN propagation conditions, this accuracy is theoretically defined by the CRB for range estimation, which relies on signal bandwidth and power levels. This will be shown in the following chapter, where simulation results of dedicated deployments will be presented that yield sub-meter accuracy due to high signal levels in AWGN conditions.

However, achieving such precision becomes challenging with bandwidths below 100 MHz or in scenarios with significant multipath effects that will be seen more in depth in Chapter 6. Thus, increasing bandwidth not only enhances the time resolution but can also mitigate the adverse effects of multipath propagation, potentially allowing the utilization of multipath components for positioning. Multipath propagation can severely affect range estimates, even in LoS conditions, especially in low SNR environments. This is due to the interference caused by multiple propagation paths, each contributing to the overall detected channel response at the receiver. To mitigate these ranging errors resulting from multipath interference, larger bandwidths can be employed to enhance time resolution and improve the separation between different paths in time.

The extent of ranging errors attributed to multipath propagation varies based on the specific multipath scenario, including the propagation delays and channel coefficients of each path. Although the use of directional antennas in the transmitter and/or receiver can help filter out NLoS components, the most critical NLoS components often share similar angle characteristics with the LoS path, making them challenging to spatially filter with practical antenna array sizes. The impact on ranging accuracy is big, where a smaller bandwidth leads to significant degradation due to multipath propagation. However, it is noteworthy that the disparity between the multipath and LoS-only scenarios diminishes when larger bandwidths are utilized.

2.4.4 Antenna array elements

Antenna arrays serve as a crucial tool for beamforming, directing radio signals either for transmission or reception toward specific areas of interest. These arrays offer the capability for spatial multiplexing, spatial diversity, and beamforming accuracy, depending on the array configuration and RF transmission chains. Considering the prevalence of 3D scenarios in many 5G NR use cases, the planar array, particularly the URA, has become one of the most popular choices. By adjusting the number of antenna elements in rows and columns, the URA allows fine-tuning of spatial selectivity in elevation and azimuth directions. In this work, a URA is implemented, where any number of antenna elements in rows and columns can be applied. However, it can easily applied to Uniform Linear Array (ULA) considering one of rows and columns to 1.

In the context of positioning, antenna arrays play a crucial role in obtaining angle estimates, namely Angle of Departure (AoD) or AoA estimation. The accuracy of angle estimation is directly related to the number of antenna elements in the array. Understanding the influence of array dimensions on positioning accuracy is valuable. Formulating a CRB, already presented in 2.4.2, for angle estimation provides insights into the smallest possible angle estimation error variance under specific conditions. Moreover, knowing the antenna orientation is crucial for

angle-based positioning. In some UE implementations, such as handheld devices or smartphones, the antenna orientation is typically unknown, introducing another estimation parameter in the positioning problem. However, this constraint can be circumvented in Unmanned Aerial Vehicles (UAV) setups where antennas have fixed mounts within the payload.

When angle estimation contributes to position estimation, the utility of angle information is influenced by the system's geometric configuration. To assess the effect of angle estimation on positioning accuracy, angle measurements must be translated to the position domain. This transformation can be achieved by considering the geometry of the system and the inherent geometry constraints, including angle unambiguity. In the next Chapter 3 we will demonstrate how the accuracy of position estimation changes concerning the UE's distance to the BS, array size, SNR, and system geometry, emphasizing the impact of AoA measurements on positioning error.

Appendix 2.A Derivation of the geometry matrix in AoA positioning method

This section reports the computation of the geometry matrix being used in the position computation when AoA positioning method is used. Note that for the computation, an URA antenna is considered. The geometry matrix ($\mathbf{G}_{\text{AoA}}$) is defined as:

$$[\mathbf{G}]_{\text{AoA},2m} = \begin{bmatrix} \frac{\partial \phi_m}{\partial x} & \frac{\partial \phi_m}{\partial y} & \frac{\partial \phi_m}{\partial z} \\ \frac{\partial \theta_m}{\partial x} & \frac{\partial \theta_m}{\partial y} & \frac{\partial \theta_m}{\partial z} \end{bmatrix} \tag{2.61}$$

Considering the BS position coordinates as $\mathbf{P}_{\text{BS}} = [X_{\text{BS},m}, Y_{\text{BS},m}, Z_{\text{BS},m}]$, where $1 \leq m < M_{\text{BS}}$. Note that, in the software, a maximum of 6 BS per UE is considered for the position computation. The UE position coordinates are set as $\mathbf{P}_{\text{UE}} = [X_{\text{UE}}, Y_{\text{UE}}, Z_{\text{UE}}]$. The equation in 2.29 can be written as:

$$\mathbf{P}' = \mathbf{R}_{\mathbf{x}}(\mathbf{P}_{\text{UE}} - \mathbf{P}_{\text{BS}}), \tag{2.62}$$

and considering the spatial dimension for $3D$ positioning, the azimuth and elevation angles are computed as:

$$\theta = \cos^{-1}\left(\frac{\mathbf{v}^T \mathbf{R}_x(\mathbf{P}_{\text{UE}} - \mathbf{P}_{\text{BS}})}{\|(\mathbf{P}_{\text{UE}} - \mathbf{P}_{\text{BS}})\|}\right), \tag{2.63}$$

$$\phi = \text{atan2}\left([\mathbf{R}_x(\mathbf{P}_{\text{UE}} - \mathbf{P}_{\text{BS}})]_y, [\mathbf{R}_x(\mathbf{P}_{\text{UE}} - \mathbf{P}_{\text{BS}})]_x\right). \tag{2.64}$$

Note that $\mathbf{v}$ is the unit vector of the z-axis that corresponds to the direction of the array. Therefore, the geometry matrix $\mathbf{G}_{\text{AoA},2m}$ defined as in 2.61, its elements are computed as following:

$$\frac{\partial \theta_m}{\partial x} = -\frac{1}{\sqrt{1-\left(\frac{Z'}{d}\right)^2}} \quad \frac{\partial}{\partial x}\left(\frac{Z'}{d}\right) = -\frac{1}{\sqrt{1-\left(\frac{Z'}{d}\right)^2}} \frac{\partial \mathbf{P}'}{\partial x} \nabla_{\mathbf{P}'}\left[\frac{Z'}{d}\right], \tag{2.65}$$

$$\frac{\partial \theta_m}{\partial y} = -\frac{1}{\sqrt{1-\left(\frac{Z'}{d}\right)^2}} \quad \frac{\partial}{\partial y}\left(\frac{Z'}{d}\right) = -\frac{1}{\sqrt{1-\left(\frac{Z'}{d}\right)^2}} \frac{\partial \mathbf{P}'}{\partial y} \nabla_{\mathbf{P}'}\left[\frac{Z'}{d}\right], \tag{2.66}$$

$$\frac{\partial \theta_m}{\partial z} = -\frac{1}{\sqrt{1-\left(\frac{Z'}{d}\right)^2}} \quad \frac{\partial}{\partial z}\left(\frac{Z'}{d}\right) = -\frac{1}{\sqrt{1-\left(\frac{Z'}{d}\right)^2}} \frac{\partial \mathbf{P}'}{\partial z} \nabla_{\mathbf{P}'}\left[\frac{Z'}{d}\right], \tag{2.67}$$

where

$$\nabla_{\mathbf{P}'}\left[\frac{Z'}{d}\right] = \begin{bmatrix} \frac{-Z'X'}{d^3} \\ \frac{-Z'Y'}{d^3} \\ \frac{d^2 - Z'^2}{d^3} \end{bmatrix},$$

and

$$\frac{\partial \mathbf{P}'}{\partial x} = (\mathbf{R}_x(:,1))^H, \quad \frac{\partial \mathbf{P}'}{\partial y} = (\mathbf{R}_x(:,2))^H, \quad \frac{\partial \mathbf{P}'}{\partial z} = (\mathbf{R}_x(:,3))^H.$$

with $\mathbf{R}_x$ being the rotation matrix around x axis.

$$\frac{\partial \phi_m}{\partial x} = \frac{X'^2}{X'^2 + Y'^2} \quad \frac{\partial}{\partial x}\left(\frac{Y'}{X'}\right) = \frac{X'^2}{X'^2 + Y'^2} \quad \frac{\partial \mathbf{P'}}{\partial x} \quad \nabla_{\mathbf{P'}}\left[\frac{Y'}{X'}\right], \tag{2.68}$$

$$\frac{\partial \phi_m}{\partial y} = \frac{X'^2}{X'^2 + Y'^2} \quad \frac{\partial}{\partial y}\left(\frac{Y'}{X'}\right) = \frac{X'^2}{X'^2 + Y'^2} \quad \frac{\partial \mathbf{P'}}{\partial y} \quad \nabla_{\mathbf{P'}}\left[\frac{Y'}{X'}\right], \tag{2.69}$$

$$\frac{\partial \phi_k}{\partial z} = \frac{X'^2}{X'^2 + Y'^2} \quad \frac{\partial}{\partial z}\left(\frac{Y'}{X'}\right) = \frac{X'^2}{X'^2 + Y'^2} \quad \frac{\partial \mathbf{P'}}{\partial z} \quad \nabla_{\mathbf{P'}}\left[\frac{Y'}{X'}\right], \tag{2.70}$$

where

$$\nabla_{\mathbf{P'}}\left[\frac{Y'}{X'}\right] = \nabla_{\mathbf{P'}}\begin{bmatrix} \frac{\partial}{\partial X'}\left(\frac{Y'}{X'}\right) \\ \frac{\partial}{\partial Y'}\left(\frac{Y'}{X'}\right) \\ \frac{\partial}{\partial Y'}\left(\frac{Y'}{X'}\right) \end{bmatrix} = \begin{bmatrix} -\frac{Y'}{X'^2} \\ \frac{X'}{X'^2} \\ 0 \end{bmatrix}, \tag{2.71}$$

and

$$\frac{\partial \mathbf{P'}}{\partial x} = (\mathbf{R}_x(:,1))^H, \quad \frac{\partial \mathbf{P'}}{\partial y} = (\mathbf{R}_x(:,2))^H, \quad \frac{\partial\ \mathbf{P'}}{\partial z} = (\mathbf{R}_x(:,3))^H. \tag{2.72}$$

Appendix 2.B Derivation of the covariance matrix in CRB TDoA positioning.

This section reports the computation of the covariance matrix [37] being used in the position computation when TDoA positioning method is used, for both DL and UL. According to [38], where TDoA acquisition is investigated, the diagonal terms of the FIM_τ of gaining measurements, that depend only on the receiver signals at the BS pair, are:

$$\mathrm{FIM}_{12} = (\frac{\partial \mathbf{y}}{\partial \tau_{12}})^H (\frac{\partial \mathbf{y}}{\partial \tau_{12}}) \tag{2.73}$$

$$\mathrm{FIM}_{13} = (\frac{\partial \mathbf{y}}{\partial \tau_{13}})^H (\frac{\partial \mathbf{y}}{\partial \tau_{13}}) \tag{2.74}$$

$$\vdots$$

$$\mathrm{FIM}_{1M} = (\frac{\partial \mathbf{y}}{\partial \tau_{1M}})^H (\frac{\partial \mathbf{y}}{\partial \tau_{1M}}) \tag{2.75}$$

The cross term between pair $1i$ and pair $1j$ $(i \neq j)$ can be evaluated as:

$$\mathrm{CF}_{1i,1j} = (\frac{\partial \mathbf{y}}{\partial \tau_{1i}})^H (\frac{\partial \mathbf{y}}{\partial \tau_{1j}}) \tag{2.76}$$

Through the Jacobian matrices transformation with the $M-1$ TDoA measurements:

$$\hat{\tau}_{1M} = \tau_{1M} + v_{1M}, \tag{2.77}$$

where $\tau_{ij} = \tau_i - \tau_j$ and v_{ij} is the measurement noise, yields:

$$\frac{\partial \mathbf{y}}{\partial \tau_{12}} = \begin{bmatrix} \frac{\partial \mathbf{y_1}}{\partial \tau_{12}} \\ \frac{\partial \mathbf{y_2}}{\partial \tau_{12}} \\ \frac{\partial \mathbf{y_3}}{\partial \tau_{12}} \\ \vdots \\ \frac{\partial \mathbf{y_M}}{\partial \tau_{12}} \end{bmatrix} = \begin{bmatrix} \frac{\partial \mathbf{y_1}}{\partial \tau_1}\frac{\partial \tau_1}{\partial \tau_{12}} \\ \frac{\partial \mathbf{y_2}}{\partial \tau_2}\frac{\partial \tau_2}{\partial \tau_{12}} \\ 0 \\ \vdots \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{\partial \mathbf{y_1}}{\partial \tau_1} \\ -\frac{\partial \mathbf{y_2}}{\partial \tau_2} \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \tag{2.78}$$

$$\frac{\partial \mathbf{y}}{\partial \tau_{13}} = \begin{bmatrix} \frac{\partial \mathbf{y_1}}{\partial \tau_{13}} \\ \frac{\partial \mathbf{y_2}}{\partial \tau_{13}} \\ \frac{\partial \mathbf{y_3}}{\partial \tau_{13}} \\ \vdots \\ \frac{\partial \mathbf{y_M}}{\partial \tau_{13}} \end{bmatrix} = \begin{bmatrix} \frac{\partial \mathbf{y_1}}{\partial \tau_1}\frac{\partial \tau_1}{\partial \tau_{13}} \\ 0 \\ \frac{\partial \mathbf{y_3}}{\partial \tau_3}\frac{\partial \tau_3}{\partial \tau_{13}} \\ \vdots \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{\partial \mathbf{y_1}}{\partial \tau_1} \\ 0 \\ -\frac{\partial \mathbf{y_3}}{\partial \tau_3} \\ \vdots \\ 0 \end{bmatrix}, \tag{2.79}$$

and the last term is:

$$\frac{\partial \mathbf{y}}{\partial \tau_{1M}} = \begin{bmatrix} \frac{\partial \mathbf{y_1}}{\partial \tau_{1M}} \\ \frac{\partial \mathbf{y_2}}{\partial \tau_{1M}} \\ \frac{\partial \mathbf{y_3}}{\partial \tau_{1M}} \\ \vdots \\ \frac{\partial \mathbf{y_M}}{\partial \tau_{1M}} \end{bmatrix} = \begin{bmatrix} \frac{\partial \mathbf{y_1}}{\partial \tau_1}\frac{\partial \tau_1}{\partial \tau_{1M}} \\ 0 \\ 0 \\ \vdots \\ \frac{\partial \mathbf{y_3}}{\partial \tau_3}\frac{\partial \tau_M}{\partial \tau_{1M}} \end{bmatrix} = \begin{bmatrix} \frac{\partial \mathbf{y_1}}{\partial \tau_1} \\ 0 \\ 0 \\ \vdots \\ -\frac{\partial \mathbf{y_M}}{\partial \tau_M} \end{bmatrix}, \tag{2.80}$$

Substituting 2.78 to 2.80 in 2.73 to 2.76 we have:

$$\mathrm{FIM}_{12} = (\frac{\partial \mathbf{y_1}}{\partial \tau_1})^H(\frac{\partial \mathbf{y_1}}{\partial \tau_1}) + (\frac{\partial \mathbf{y_2}}{\partial \tau_2})^H(\frac{\partial \mathbf{y_2}}{\partial \tau_2}), \tag{2.81}$$

$$\mathrm{FIM}_{13} = (\frac{\partial \mathbf{y_1}}{\partial \tau_1})^H(\frac{\partial \mathbf{y_1}}{\partial \tau_1}) + (\frac{\partial \mathbf{y_3}}{\partial \tau_3})^H(\frac{\partial \mathbf{y_3}}{\partial \tau_3}), \tag{2.82}$$

$$\vdots$$

$$\mathrm{FIM}_{1M} = (\frac{\partial \mathbf{y_1}}{\partial \tau_1})^H(\frac{\partial \mathbf{y_1}}{\partial \tau_1}) + (\frac{\partial \mathbf{y_M}}{\partial \tau_M})^H(\frac{\partial \mathbf{y_M}}{\partial \tau_M}), \tag{2.83}$$

$$\mathrm{CF}_{1i,1j} = CF_{1j,1i} = (\frac{\partial \mathbf{y_1}}{\partial \tau_1})^H(\frac{\partial \mathbf{y_1}}{\partial \tau_1}). \tag{2.84}$$

Therefore, the FIM cross-term between pairs is just the FIM of the shared BS itself. Denoting the FIM of the m-th BS as $\mathbf{F}$ for $m_1, \cdots, M$:

$$\mathrm{F}_m = (\frac{\partial \mathbf{y_m}}{\partial \tau_m})^H(\frac{\partial \mathbf{y_m}}{\partial \tau_m}), \tag{2.85}$$

yields the FIM of the measurement set $\tau = [\tau_{12}, \tau_{13}, \cdots, \tau_{1M}]$ to:

$$\mathbf{FIM}_{\tau} = \begin{bmatrix} \mathrm{FIM}_{12} & \mathrm{CF}_{12,13} & \cdots & \mathrm{CF}_{12,1M} \\ \mathrm{CF}_{13,12} & \mathrm{FIM}_{13} & \cdots & \mathrm{CF}_{13,1M} \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{CF}_{1M,12} & & & \mathrm{FIM}_{1M} \end{bmatrix} = \begin{bmatrix} \mathrm{F}_1 + \mathrm{F}_2 & \mathrm{F}_1 & \cdots & \mathrm{F}_1 \\ \mathrm{F}_1 & \mathrm{F}_1 + \mathrm{F}_3 & \cdots & \mathrm{F}_1 \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{F}_1 & & & \mathrm{F}_1 + \mathrm{F}_M \end{bmatrix}. \tag{2.86}$$

Therefore, the covariance matrix will have the structure shown in (2.39).

Chapter 3

Assessment of positioning techniques using the 5G NR simulator

The 5G New Radio (NR) simulator presented in Chapter 2, which provides network solutions, will be now used for implementing, simulating and testing the 3rd Generation Partnership Project (3GPP) stack in order to analyze the following candidate techniques: Cell IDentity (CID), Time Difference of Arrival (TDoA) for both downlink and uplink, Round Trip Time (RTT), and Angle of Arrival (AoA). The target use cases chosen are two of the ones presented in Chapter 1, i.e. low-energy Internet of Things (IoT) and high-accuracy autonomous cars. This part, which constitutes the core of the chapter, is outlined in Section 3.2. The trade-offs presented in the technology's analysis done in Chapter 1 are taken into account. Understanding such properties will help to characterize the positioning methods and conditions for precise cellular positioning.

Additional numerical results, aimed to benchmark the 5G localization performance of several techniques will be presented in Section 3.1. The implementation is done in compliance with the latest 5G positioning 3GPP standards. These results are compared with simulations conducted by various 3GPP contributors, taking into account different metrics. Given the variations in simulation outcomes from different institutions, the benchmark for these metrics is established by comparing the mean value of the results presented.

Moreover, the positioning performance of a real experiment is compared with a simulation reproducing the same scenario (Section 3.3). In particular, the same base station locations of the experiment are used for the simulation and the configuration parameters of the simulation are chosen to be as similar as possible to the real scenario. This approach ensures a reliable basis for evaluating the performance of 5G localization.

The forthcoming numerical results provide insights into the accuracy attainable through 5G localization, leveraging a combination of time-based multi-link measurements and a thorough exploration of potential localization algorithms. Results show interesting insights in terms of research and development, making them valuable tools for advancing the field of 5G positioning and localization. Our contribution in this chapter will give valuable help to understand how to perform 5G localization, providing an effective methodology to deploy an experimental test-bed to be seen in Chapter 6. In this way it will enable the examination and validation of algorithms and provide research results using measurements of 5G localization signals transmitted by high-

end platforms. For this, standardized localization procedures and real operating conditions should be taken into account. The conclusions and discusions about this part of the work are outlined in Section 3.4.

Part of the simulation studies presented in this chapter have been done in the framework of "GNSS Integration into 5G Wireless Networks" project (GINTO5G) funded by the European Space Agency (ESA), being the UAB part of the consortium, where the PoPeCoT simulation platform described in Chapter 2 has been implemented.

3.1 A reliable benchmark for 5G localization performance

The significance of the analysis presented in this section lies in the evaluation of the performance of 3GPP scenarios under various options and configurations. It consists on the verification through a comparison with results from various companies, aligning with target accuracy standards. The requirements set as minimum performance for NR positioning are the following:

- Horizontal positioning error $\leq$ 50 m for 80% of User Equipment (UE).
- Vertical positioning error $<$ 5 m for 80% of UEs.
- End-to-end latency and Time to first fix (TTFF) $<$ 30 seconds.

Additional targets are based on the need for commercial use cases for indoor and outdoor scenarios:

- Horizontal positioning error $<$ 3 m for 80% of UEs in indoor deployment scenarios.
- Vertical positioning error $<$ 3 m for 80% of UEs in indoor deployment scenarios.
- Horizontal positioning error $<$ 10 m for 80% of UEs in outdoor deployments scenarios.
- Vertical positioning error $<$ 3 m for 80% of UEs in outdoor deployment scenarios.
- End to end latency $<$ 1 s.

The selected scenarios corresponding to the 5G cmWave network operate at frequency bands below 6 GHz [39]. Due to the limited available spectrum, there is a reduced system bandwidth of up to 100 MHz. Two types of scenarios are considered based on the Inter-Site Distance (ISD) between Base Station (BS) according to [26], where in urban areas, the ISD of the macro cells is equal to 500 m (considered in Scenario 2), and hotspots are covered with small cells or micro sites of ISD equal to 200 m (considered in Scenario 1). Each network topology, i.e., urban micro, urban macro, is simulated with a hexagonal cell layout of three-sectorial sites and the corresponding ISD. Note that for the case of the 5G NR simulator, these topologies are achieved following the network deployments explained in 2.3.1. The network density is then achieved by selecting the 6 closest BS to each receiver position. This means that BSs are discarded according to the distance between BS and receiver locations, i.e., BS far from receiver locations are prioritized to be discarded. Furthermore, an average height of buildings is defined for each of these environments according to [26]. For instance, suburban areas with a low building height have a low density of BSs, while a high density of BSs is considered in populated urban areas with

a high-building profile. However, since we are dealing with terrestrial use cases, the evaluation is concentrated on the horizontal dimension.

The observables based on TDoA, RTT, and AoA measurements are computed following the process explained in Chapter 2. In the analysis, 5G downlink Positioning Reference Signal (PRS) and uplink Sounding Reference Signal (SRS) Orthogonal Frequency Division Multiplexing (OFDM) cmWave signals are used. A predefined carrier frequency with a signal bandwidth up to 100 MHz formed by M contiguous pilot subcarriers based on the bandwidth value and subcarrier spacing of 15 or 30 kHz are considered. The evaluation parameters, including Root-Mean-Square Error (RMSE), Cumulative Density Function (CDF) of the UE position errors are compared with the corresponding results given by selected companies [40, 41, 42]. The CDF of the horizontal positioning accuracy is here used as the metric to assess the positioning performance. All the simulated scenarios are based on standardization bodies that define reproducible scenarios in order to evaluate candidate specifications.

3.1.1 Downlink evaluation: OTDoA

The stand-alone 5G Downlink (DL)-TDoA (Observed Time Difference of Arrival (OTDoA)) cmWave positioning method is performed for Urban Micro (UMi) and Urban Macro (UMa) environment including conditions with perfect synchronization and with a synchronization error of 50 ns standard deviation. The positioning algorithm is then evaluated with prior information on the ranging errors. That is, a Weighted Least Squares (WLS) positioning algorithm approach, i.e., using the absolute ranging errors within the weighting matrix. Different choices for subcarrier spacing are explored. Ideal muting is used to avoid interference. The PRS start with no frequency offset in the system bandwidth and it is configured with a bandwidth ranging from 24 to 276 physical resource blocks (PRBs) in steps of 4 PRBs. Full bandwidth is considered for both scenarios. The configuration parameters for each scenario are explained in detail below.

3.1.1.1 Scenario 1: UMi

The evaluation considers a UMi cellular deployment with ISD of 200 m and wrap-around of BSs. Three configuration parameters are considered based on system bandwidth and subcarrier spacing as depicted in 3.1. The 5G system is assumed to operate a dedicated PRS transmission from the highest bandwidth value for Frequency Range 1 (FR1) (100 MHz) to the lowest (5 MHz) with ideal PRS muting at a carrier frequency of 4 GHz. One PRS symbol per slot and both perfect and 50 ns network synchronization error are considered. The urban micro topology is simulated with a hexagonal cell layout of 19 three-sectorial sites. The 5G DL-TDoA observables are simulated using the procedure explained in Chapter 2, where the Line of Sight (LoS) conditions of the 5G ranging observables are obtained based on the distance-dependent LoS probability for UMi environments and the Signal-to-Noise Ratio (SNR) level of each observable is computed with a 3GPP-like link budget as in Chapter 2, by using the UMi scenario parameters defined in [18]. Note that the ranging observables are limited to the six most powerful BSs (BS near the receiver locations) for each UE dropped position. Recall that the ranging observables are generated following the physical-layer abstraction explained in Chapter 2 using as input the LoS conditions, the SNR levels, and the probabilities obtained from uniformly distributed random variables between 0 and 1. Figure 3.1 displays the performance obtained

from the simulations in comparison with the one presented by Qualcomm company [40]. These results are summarized in Tables 3.2 and 3.3.

Table 3.1: Parameters details for FR1 with perfect and realistic synchronization using OTDoA method [40]

Parameter	**Case1 FR1, 100 MHz**	**Case2 FR1, 50 MHz**	**Case3 FR1, 5 MHz**	**Case1 FR1, 100 MHz**	**Case2 FR1, 50 MHz**	**Case3 FR1, 5 MHz**
Channel model (baseline, otherwise state any modifications)	Baseline Channel Model based on common assumptions defined related to the channel models of 3GPP TRs 38.901 / 38.802 / 37.857.			Baseline Channel Model based on common assumptions defined related to the channel models of 3GPP TRs 38.901		
Carrier frequency	4 GHz					
Subcarrier spacing	30 kHz	15 kHz			15 kHz	
Reference Signal Transmission Bandwidth	100 MHz	50MHz		5 MHz		
Reference Signal Physical Structure and Resource Allocation (RE pattern)	1-symbol PRS					
Number of sites	19 (3-sector)					
Number of symbols used per occasion	1					
Interference modelling (ideal muting, or other)	Ideal muting					
Description of positioning technique / applied positioning algorithm (e.g. Least square, Taylor series, etc)	For DL-TDoA Pick the best between Taylor series, and Chan's Algorithm. Chan's Algorithm according to: Y. T. Chan, K. C. Ho, " A Simple and Efficient Estimator for Hyperbolic Location", IEEE Transactions on Signal Processing, vol. 42, pp. 1905-1915, Aug. 1994. Taylor Series Algorithm: W. H. Foy, " Position-Location Solutions by Taylor-Series Estimation", IEEE Transactions on Aerospace and Electronic Systems, vol. AES-12, pp. 187-194, March 1976. Equal weight is used in the ToA covariance matrix.		RTT, Gauss-Newton algorithm			
Network synchronization assumptions	Perfect Sync and Realistic Sync with T1 = 50 nsec					
Simulations by	Qualcomm		5G NR simulator			

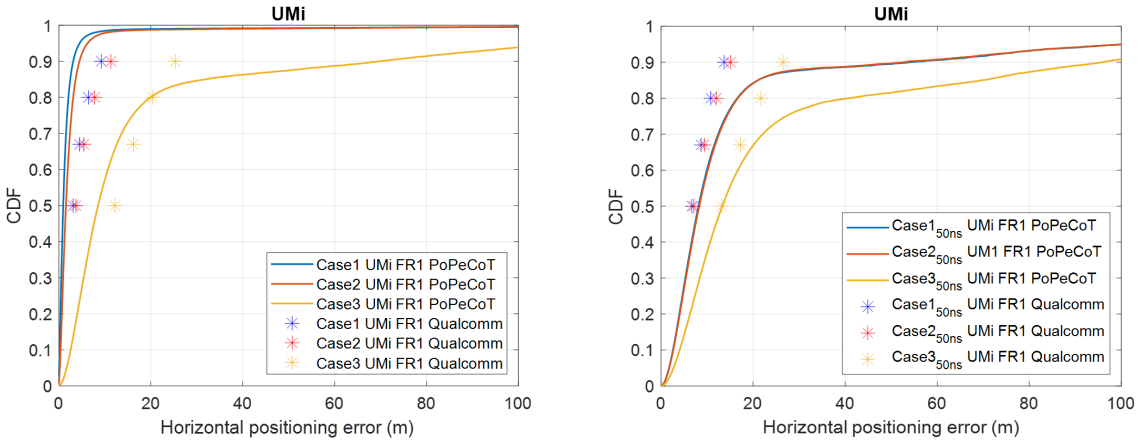
Table 3.2: Summary of evaluation results in UMi scenario with perfect synchronization: OTDoA at FR1

Conditions Techno.	**Results by**	**Source**	**Network sync.**	**Horizontal accuracy (m)**			
				50%	67%	80%	90%
OTDoA	Qualcomm	Case 1 UMi FR1	Perfect sync.	3.1	4.5	6.4	9.2
		Case 2 UMi FR1	Perfect sync.	3.7	5.4	7.8	11.3
		Case 3 UMi FR1	Perfect sync.	12.2	16.2	20.4	25.3
	5G NR simulator	Case 1 UMi FR1	Perfect sync.	0.95	1.47	2.15	3.02
		Case 2 UMi FR1	Perfect sync.	1.51	2.26	3.16	4.5
		Case 3 UMi FR1	Perfect sync.	8.72	12.78	19.89	30.74

Table 3.3: Summary of evaluation results in UMi scenario with 50-ns synchronization error: OTDoA at FR1

Conditions Techno.	**Results by**	**Source**	**Network sync.**	**Horizontal accuracy (m)**			
				50%	67%	80%	90%
OTDoA	Qualcomm	Case 1 UMi FR1	50-ns sync. err.	6.7	8.7	10.8	13.7
		Case 2 UMi FR1	50-ns sync. err.	7.1	9.4	12	15.1
		Case 3 UMi FR1	50-ns sync. err.	13.2	17.2	21.7	26.5
	5G NR simulator	Case 1 UMi FR1	50-ns sync. err.	8.53	12.12	16.89	30.66
		Case 2 UMi FR1	50-ns sync. err.	8.3	17.82	17.83	30.55
		Case 3 UMi FR1	50-ns sync. err.	13.95	20.89	30.83	30.92

Simulations conducted with perfect network synchronization and wide bandwidths yield optimistic results, meeting the performance target. 5G signal bandwidth has a key impact on the achievable ranging accuracy within the positioning system and this is reflected in the cases of bandwidth 100 MHz and 50 MHz where the OTDoA horizontal positioning error is less than 10 meters for 80% of UEs. A degradation is noted with a narrow bandwidth when, even in conditions of no synchronization error, the position error is twice higher. The delay error variance decreases in the order of the square of the bandwidth as the bandwidth increases and this is reflected in the results. However, when a 50 ns RMSE for synchronization is introduced, the OTDoA performance falls short of meeting the positioning requirements. It only satisfies the minimal criterion of having a horizontal positioning error less than or equal to 50 meters for 80% of UEs. Even in conditions of error synchronization, the effect of narrow bandwidth in the degradation of the estimation accuracy is noted.



(a) Perfect synchronization.

(b) 50 ns synchronization error.

Figure 3.1: Results of OTDoA for UMi deployment for FR1.

Comparing the results obtained from the 5G NR simulator and those provided by Qualcomm, our results demonstrate superior performance overall. Nevertheless, in the presence of synchronization errors, Qualcomm's results are marginally better. We believe that this discrepancy could be attributed to factors such as LoS conditions where a poor positioning performance is mainly due to the predominance of Non Line of Sight (NLoS) ranging bias, the effect of bad geometry of the BSs, base station density, etc. Note that further details on their implementation are not published.

3.1.1.2 Scenario 2: UMa

In the second scenario, the evaluation focuses on the estimation of UE's position in a UMa cellular deployment, characterized by an ISD of 500 meters. Like in the first scenario, the study considers three configuration parameters based on system bandwidth and subcarrier spacing, as outlined in Tables 3.4 and 3.5. Narrow bandwidth, i.e. 5 MHz, and wide bandwidths, i.e., 50 and 100 MHz for FR1 with a 0 ns and 50 ns RMSE for the network synchronization are taken into account. The PRS transmission occurs at a carrier frequency of 4 GHz and 2 GHz, with the inclusion of one PRS symbol per slot for the case of 5G NR simulator and 8 symbols for the case of Huawei company simulations [41], that are used as a comparison in this case. The simulation replicates an urban macro topology using a hexagonal cell layout with 19 three-sectorial sites. Again, the 5G OTDoA observables are generated using the methodology outlined in Chapter 2 and the UMa scenario parameters defined in [18]. Note that, the ranging observables are constrained to the six most powerful BSs, i.e. those closest to the UE drop positions. Figure 3.2 visually presents the performance results obtained from the simulations, offering a comparative analysis with the data presented by Huawei. These findings are briefly summarized in Tables 3.6 and 3.7.

The simulation results affirm the anticipated outcome: wideband signals facilitate precise positioning, meeting high-accuracy standards, while the narrowband configuration merely satisfies regulatory requirements. The ambitious performance target of achieving less than 10 meters positioning error for 80% of UEs is realized only under conditions of perfect synchronization and with a wide bandwidth. Another effect on the accuracy of position estimation is the subcar-

Table 3.4: Parameters details for FR1 with no synchronization error[41]

Parameter	Case 1 UMa, FR1	Case 1 UMa, FR1	Case 2 UMa, FR1	Case 2 UMa, FR1	Case 3 UMa, FR1	Case 3 UMa, FR1	Case 4 UMa, FR1	Case 4 UMa, FR1
Channel model (baseline, otherwise state any modifications)	38.901	38.901	38.901	38.901	38.901	38.901	38.901	38.901
Carrier frequency	4GHz	4GHz	4GHz	4GHz	2GHz	2GHz	2GHz	2GHz
Subcarrier spacing	30kHz	30kHz	15kHz	15kHz	15kHz	15kHz	15kHz	15kHz
Reference Signal Transmission Bandwidth	100MHz	100MHz	50MHz	50MHz	50MHz	50MHz	5MHz	5MHz
Reference signal (type of sequence, number of ports, ...)	PRS: Gold, 1-port	PRS	PRS: Gold, 1-port	PRS	PRS: Gold, 1-port	PRS	PRS: Gold, 1-port	PRS
Number of sites	19	19	19	19	19	19	19	19
Number of symbols used per occasion	8	1	8	1	8	1	8	1
Description of positioning technique / applied positioning algorithm (e.g. Least square, Taylor series, etc)	DL-TDoA, Gauss-Newton algorithm	DL-TDoA, Gauss-Newton algorithm	DL-TDoA, Gauss-Newton algorithm	DL-TDoA, Gauss-Newton algorithm	DL-TDoA, Gauss-Newton algorithm	DL-TDoA, Gauss-Newton algorithm	DL-TDoA, Gauss-Newton algorithm	DL-TDoA, Gauss-Newton algorithm
Network synchronization assumptions	No sync error	No sync error	No sync error	No sync error	No sync error	No sync error	No sync error	No sync error
Beam-related assumption (beam sweeping / alignment assumptions at the tx and rx sides)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Simulations by	Huawei	5G NR simulator	Huawei	5G NR simulator	Huawei	5G NR simulator	Huawei	5G NR simulator

Table 3.5: Parameters details for FR1 with 50 ns synchronization error [41]

Parameter	Case 9 UMa, FR1	Case 9 UMa, FR1	Case 10 UMa, FR1	Case 10 UMa, FR1	Case 11 UMa, FR1	Case 11 UMa, FR1	Case 12 UMa, FR1	Case 12 UMa, FR1
Channel model (baseline, otherwise state any modifications)	38.901	38.901	38.901	38.901	38.901	38.901	38.901	38.901
Carrier frequency	4GHz	4GHz	4GHz	4GHz	2GHz	2GHz	2GHz	2GHz
Subcarrier spacing	30kHz	30kHz	15kHz	15kHz	15kHz	15kHz	15kHz	15kHz
Reference Signal Transmission Bandwidth	100MHz	100MHz	50MHz	50MHz	50MHz	50MHz	5MHz	5MHz
Reference signal (type of sequence, number of ports, ...)	PRS: Gold, 1-port	PRS	PRS: Gold, 1-port	PRS	PRS: Gold, 1-port	PRS	PRS: Gold, 1-port	PRS
Number of sites	19	19	19	19	19	19	19	19
Number of symbols used per occasion	8	1	8	1	8	1	8	1
Description of positioning technique / applied positioning algorithm (e.g. Least square, Taylor series, etc)	DL-TDoA, Gauss-Newton algorithm	DL-TDoA, Gauss-Newton algorithm	DL-TDoA, Gauss-Newton algorithm	DL-TDoA, Gauss-Newton algorithm	DL-TDoA, Gauss-Newton algorithm	DL-TDoA, Gauss-Newton algorithm	DL-TDoA, Gauss-Newton algorithm	DL-TDoA, Gauss-Newton algorithm
Network synchronization assumptions	Sync error 50ns	Sync error 50ns	Sync error 50ns	Sync error 50ns	Sync error 50ns	Sync error 50ns	Sync error 50ns	Sync error 50ns
Beam-related assumption (beam sweeping / alignment assumptions at the tx and rx sides)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Simulations by	Huawei	5G NR simulator	Huawei	5G NR simulator	Huawei	5G NR simulator	Huawei	5G NR simulator

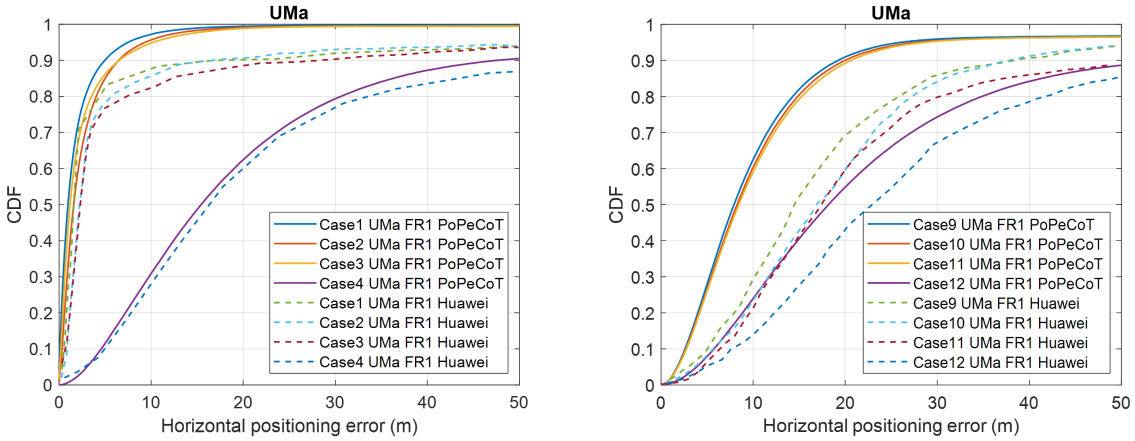
Table 3.6: Summary of evaluation results in UMa scenario with perfect synchronization: OTDoA at FR1

Conditions Techno.	Results by	Source	Network sync.	Horizontal accuracy (m)			
				50%	67%	80%	90%
OTDoA	Huawei	Case 1 UMa FR1	Perfect sync.	1.1	1.5	3.5	62.4
		Case 2 UMa FR1	Perfect sync.	1.9	2.5	5.7	16.5
		Case 3 UMa FR1	Perfect sync.	2.2	2.8	7.9	32.1
		Case 4 UMa FR1	Perfect sync.	16.3	22.9	34.0	68.4
	5G NR simulator	Case 1 UMa FR1	Perfect sync.	0.93	2.75	2.75	5.01
		Case 2 UMa FR1	Perfect sync.	1.6	2.11	4.04	6.27
		Case 3 UMa FR1	Perfect sync.	1.23	2.11	3.41	6.94
		Case 4 UMa FR1	Perfect sync.	15.78	23.48	30.82	30.91

Table 3.7: Summary of evaluation results in UMa scenario with perfect synchronization: OTDoA at FR1

Conditions Techno.	Results by	Source	Network sync.	Horizontal accuracy (m)			
				50%	67%	80%	90%
OTDoA	Huawei	Case 9 UMa FR1	50-ns sync. err.	15	20	27	42
		Case 10 UMa FR1	50-ns sync. err.	16	23	28	40
		Case 11 UMa FR1	50-ns sync. err.	17	23	31	55
		Case 12 UMa FR1	50-ns sync. err.	23	30	42	62
	5G NR simulator	Case 9 UMa FR1	50-ns sync. err.	7.91	10.72	14.11	19.64
		Case 10 UMa FR1	50-ns sync. err.	8.29	15.37	15.37	20.28
		Case 11 UMa FR1	50-ns sync. err.	7.99	10.91	10.91	14.65
		Case 12 UMa FR1	50-ns sync. err.	18.67	25.95	30.84	30.92

rier spacing. This effect is a bit peculiar since it gives a linear decrease to the delay variance. This linear relationship between subcarrier spacing and delay variance implies that as subcarrier spacing decreases, the accuracy of timing measurements improves proportionally. Consequently, this can contribute to more accurate localization results in positioning applications, benefiting overall system performance and reliability. However, in the results obtained, this impact is not dominant thanks to the high system bandwidth. Moreover, shorter distances thanks to higher



(a) No synchronization error.

(b) 50 ns synchronization error.

Figure 3.2: Results of OTDoA for UMa deployment for FR1.

carrier frequency allow better frequency reuse within a dense network coverage area. This is the reason why with 4 GHz is slightly more accurate. However, this impact is not high in this case since the difference between frequencies is not big.

On the other hand, the performance of OTDoA experiences a considerable decline in the absence of perfect synchronization. Under these conditions, the achievement of the 10 m target is achieved with a probability of approximately 50%. This underlines the sensitivity of the OTDoA performance to synchronization accuracy. Finally, the comparative analysis between the 5G NR simulator and Huawei's results shows that our results outperform Huawei in these scenarios. This performance advantage is particularly evident when assessing the reliability of positioning results in less-than-ideal conditions since not every detail in their implementation is published. Note that when using more than one PRS symbol, the accuracy is expected to improve since we are dealing with more data.

3.1.2 Uplink evaluation: UTDoA

The stand-alone 5G TDoA is evaluated also for the uplink, known as Uplink Time Difference of Arrival (UTDoA). Like in the downlink case, also in uplink, the cmWave positioning method is executed in both UMi and UMa environments with scenarios having a perfect synchronization network. A WLS positioning algorithm is employed, utilizing the absolute ranging errors within the weighting matrix. Various combinations of subcarrier spacing are explored. The SRS signal is transmitted at a carrier frequency of 4 GHz. In the time domain, the SRS resources for positioning span 1 consecutive OFDM symbols which provide enough coverage to reach all BSs involved in the positioning procedures. The SRS for positioning is using Zadoff-Chu sequences as a base signal, to ensure low Peak-to-Average Power Ratio (PAPR) transmission from the UE. Full bandwidth is considered for both UMi and UMa scenarios. The specific configuration parameters for each scenario are detailed below. They will be compared with the one provided by the Nokia company [42].

3.1.2.1 Scenario 1: UMi

The evaluation in a UMi cellular deployment with an ISD of 200 meters considers two configuration parameters: a wide bandwidth of 100 MHz with a subcarrier spacing of 30 kHz and a narrow bandwidth of 5 MHz with a subcarrier spacing of 15 kHz as outlined in Table 3.8. The SRS transmission at a carrier frequency of 4 GHz includes one SRS symbol per slot. The simulation replicates an urban micro topology using a hexagonal cell layout with 21 three-sectorial sites. The 5G UTDoA observables are generated using the methodology outlined in Chapter 2 based on the channel model depicted in [26] and following the UMi scenario parameters defined in [18]. Also here, the ranging observables are constrained to the six most powerful BSs that are those closest to the UE drop positions. Figure 3.3 presents the performance results obtained from the simulations, offering a comparative analysis with the data presented by Nokia and summarized in Table 3.9.

Table 3.8: Parameters details for FR1 with perfect synchronization: UTDoA at FR1 [42].

Parameter	**Case 1, Case 2 FR1**	**Case 1, Case 2 FR1**
Channel model (baseline, otherwise state any modifications)	Baseline	38.901
Carrier frequency	4 GHz	4 GHz
Subcarrier spacing	15 kHz, 30 kHz	15 kHz, 30 kHz
Reference Signal Transmission Bandwidth	5 MHz, 100 MHz	5 MHz, 100 MHz
Reference Signal Physical Structure and Resource Allocation (RE pattern)	NR SRS Comb-2	SRS
Number of sites	21	21
Number of symbols used per occasion	2	1
Interference modelling (ideal muting, or other)	Perfect muting	Perfect muting
Network synchronization assumptions	Perfect synchronization	Perfect synchronization
Beam-related assumption (beam sweeping / alignment assumptions at the tx and rx sides)	N/A	N/A
Precoding assumptions (codebook, nr of antenna elements used, etc)	N/A	N/A
Simulations by	Nokia	5G NR simulator

Table 3.9: Summary of evaluation results in UMi scenario: UTDoA at FR1.

Conditions Techno.	**Results by**	**Source**	**Network sync.**	**Horizontal accuracy (m)**			
				50%	67%	80%	90%
UTDoA	Nokia	Case 1 UMi FR1	Perfect sync.	17.52	27.1	39.73	59.19
		Case 2 UMi FR1	Perfect sync.	12.98	22.8	36.94	52.79
	5G NR simulator	Case 1 UMi FR1	Perfect sync.	35.87	54.13	83.95	100.87
		Case 2 UMi FR1	Perfect sync.	14.04	19.25	27.64	79.04

The obtained results show that the performance of UTDoA is inferior to that obtained through OTDoA, primarily due to a worse link budget. Under conditions of perfect synchronization and a wide bandwidth SRS signal (100 MHz), the position accuracy is higher compared to scenarios with narrow bandwidth. Nevertheless, a significant degradation in UTDoA accuracy becomes visible, particularly beyond the 90th percentile, even when operating at maximum bandwidth. The results provided by Nokia demonstrate a twofold improvement over the 5G NR

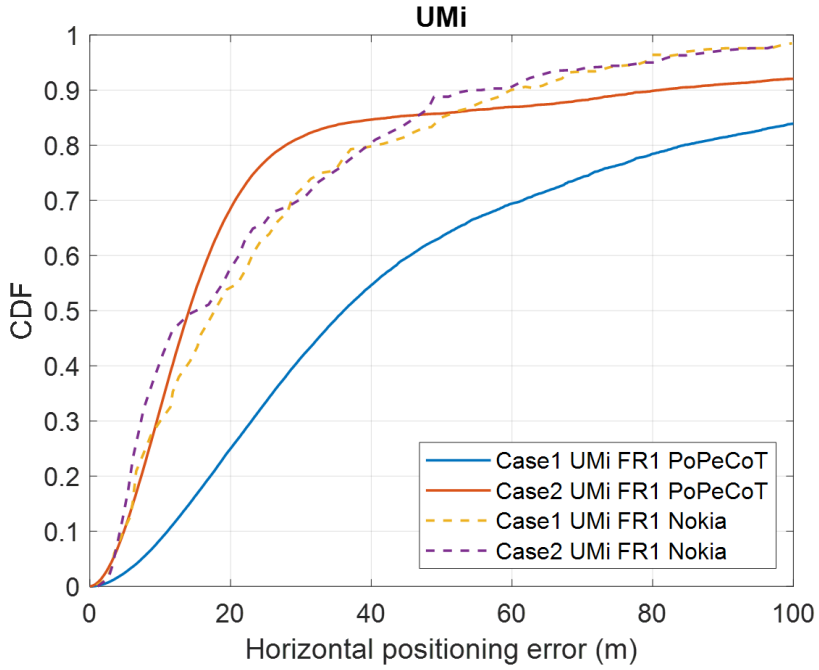


Figure 3.3: Results of UTDoA for UMi deployments for FR1 with perfect synchronization.

simulator in the case of narrow bandwidth. This difference may be attributed to the utilization of a distance-dependent LoS model in our simulations explained in Chapter 2, which can influence pseudo-range error and, consequently, impact positioning accuracy. The utilization of an additional SRS OFDM symbol also affects the improvement of the estimation accuracy.

3.1.2.2 Scenario 2: UMa

The simulations are repeated for a UMa environment. The configuration parameters are maintained the same with a change in the urban macro topology using a hexagonal cell layout with 12 three-sectorial sites. Figure 3.4 presents the performance results obtained from the simulations, offering a comparative analysis with the data presented by Nokia and summarized in Table 3.11.

In the context of network deployment, UMa layouts focuse on providing broad coverage for larger areas. This may lead to a lower level of precision in position estimation due to the larger cell size and potential challenges associated with signal propagation in urban macro environments. This is reflected in the results obtained. They show that the accuracy of position estimation in UMi deployment is higher compared to UMa deployment thanks to the fact that UMi cells are designed to cover smaller geographical areas, have lower interference levels and more favorable signal propagation characteristics, further contributing to enhanced positioning accuracy. Moreover, the results indicate that the UMa layout, characterized as a conventional deployment, only meets regulatory requirements, achieving horizontal accuracy of ≤ 50 m for 80% of UEs. A decline in UTDoA accuracy becomes evident, particularly beyond the 90th percentile, even under conditions of perfect synchronization. All in all, 5G NR simulator results outperform Nokia in terms of achieved performance.

Table 3.10: Parameters details for FR1 with perfect synchronization: UTDoA at FR1 [42].

Parameter	**Case 1, Case 2 FR1**	**Case 1, Case 2 FR1**
Channel model (baseline, otherwise state any modifications)	38.901	38.901
Carrier frequency	4GHz	4GHz
Subcarrier spacing	15kHz, 30kHz	15kHz, 30kHz
Reference Signal Transmission Bandwidth	5MHz, 100MHz	5MHz, 100MHz
Reference Signal Physical Structure and Resource Allocation (RE pattern)	NR SRS Comb-2	SRS
Number of sites	12	12
Number of symbols used per occasion	2	1
Interference modelling (ideal muting, or other)	Perfect muting	Perfect muting
Network synchronization assumptions	Perfect synchronization	Perfect synchronization
Beam-related assumption (beam sweeping / alignment assumptions at the tx and rx sides)	N/A	N/A
Precoding assumptions (codebook, nr of antenna elements used, etc)	N/A	N/A
Simulations by	Nokia	5G NR simulator

Table 3.11: Summary of evaluation results in UMa scenario: UTDoA at FR1.

Conditions Techno.	**Results by**	**Source**	**Network sync.**	**Horizontal accuracy (m)**			
				50%	67%	80%	90%
UTDoA	Nokia	Case 1 UMa FR1	Perfect sync.	28.22	32.11	51.31	81.28
		Case 2 UMa FR1	Perfect sync.	3.88	29.25	48.96	78.83
	5G NR simulator	Case 1 UMa FR1	Perfect sync.	24.71	32.23	40.65	56.04
		Case 2 UMa FR1	Perfect sync.	11.83	15.27	18.89	23.62

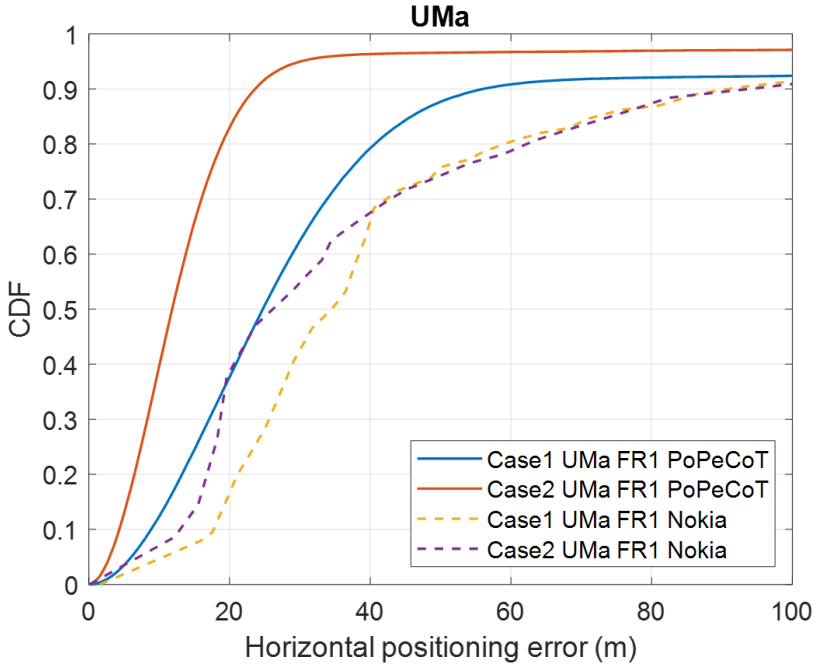


Figure 3.4: Results of UTDoA for UMa deployments for FR1 with perfect synchronization.

3.1.3 Round trip time evaluation

RTT-based positioning, including multi-RTT, offers a solution that mitigates the necessity for synchronization inherent in TDoA-based positioning. This approach leverages two-way ranging, measuring the RTT by transmitting and receiving signals between the BS and the UE. Un-

like TDoA, RTT-based methods do not require precise synchronization. Here we will see the performance of the standalone method by comparing it with the results given by Qualcomm company [40].

3.1.3.1 Scenario 1: UMi

Like in the downlink evaluation, also here, the study considers three configuration parameters based on system bandwidth and subcarrier spacing, starting from a wide bandwidth of 100 MHz with 30 kHz subcarrier spacing to a narrow bandwidth of 5 MHz with 15 kHz subcarrier spacing, as outlined in Table 3.12. The reference signals are transmitted at carrier frequencies of 4 and 2 GHz, with the inclusion of one PRS/SRS symbol per slot. The simulation replicates an urban micro topology using a hexagonal cell layout with 19 three-sectorial sites. Figure 3.5 presents the performance results obtained from the simulations with a comparative representation of the data presented by Qualcomm. These results are summarized in Tables 3.13.

Table 3.12: Parameters details for FR1 of UMi deployment [40].

Parameter	**Case1 FR1, 100 MHz**	**Case2 FR1, 50 MHz**	**Case3 FR1, 5 MHz**	**Case1 FR1, 100 MHz**	**Case2 FR1, 50 MHz**	**Case3 FR1, 5 MHz**
Channel model (baseline, otherwise state any modifications)	Baseline Channel Model based on common assumptions defined related to the channel models of 3GPP TRs 38.901 / 38.802 / 37.857.			Baseline Channel Model based on common assumptions defined related to the channel models of 3GPP TRs 38.901		
Carrier frequency	4 GHz					
Subcarrier spacing	30 kHz	15 kHz			15 kHz	
Reference Signal Transmission Bandwidth	100 MHz	50MHz		5 MHz		
Reference Signal Physical Structure and Resource Allocation (RE pattern)	Comb-1 with 1-symbol PRS resource			DL:PRS UL: SRS		
Number of sites	19					
Number of symbols used per occasion	1					
Interference modelling (ideal muting, or other)	Ideal muting					
Description of positioning technique / applied positioning algorithm (e.g. Least square, Taylor series, etc)	For multi-RTT, the algebraic solution proposed in -Norrdine, Abdelmoumen. (2015). An Algebraic Solution to the Multilateration Problem. 10.13140/RG.2.1.1681.3602. Equal weight is used in the ToA covariance matrix.		RTT, Gauss-Newton algorithm			
Network synchronization assumptions	Perfect Sync and Realistic Sync with T1 = 50 nsec					
Simulations by	Qualcomm		5G NR simulator			

Table 3.13: Summary of evaluation results in UMi scenario: RTT at FR1.

Conditions Techno.	**Results by**	**Source**	**Network sync.**	**Horizontal accuracy (m)**			
				50%	67%	80%	90%
RTT	Qualcomm	Case 1 UMi FR1	Perfect & Realistic Sync	2.8	4.6	8	16.6
		Case 2 UMi FR1	Perfect & Realistic Sync	4.4	6.4	9.5	15.8
		Case 3 UMi FR1	Perfect & Realistic Sync	17.9	23.3	29.8	38.1
	5G NR simulator	Case 1 UMi FR1	Perfect & Realistic Sync	10.63	14..62	19.34	28.17
		Case 2 UMi FR1	Perfect & Realistic Sync	10.59	14.57	19.28	27.47
		Case 3 UMi FR1	Perfect & Realistic Sync	21.26	30.29	43.96	99

Compared to the previous standalone methods: OTDoA and UTDoA, RTT is less sensitive to synchronization error. This is because it is a two-way ranging technique, where both the transmission and reception of signals contribute to the measurement. The bidirectional nature of RTT inherently helps in compensating for synchronization errors as they affect both the transmission and reception phases. These errors in both directions tend to cancel each other out, resulting in a more robust estimation of the round-trip time. This fact makes that RTT outperforms UTDoA and OTDoA when network synchronization errors are present with a significant reduction on the position error 4 times for the case of company results and a few meters for the results obtained by the 5G NR simulator. In general, both results show that when utilizing narrow bandwidth, the RTT performance falls short of meeting the target positioning requirements. Instead, it only complies with regulatory standards, achieving a horizontal positioning

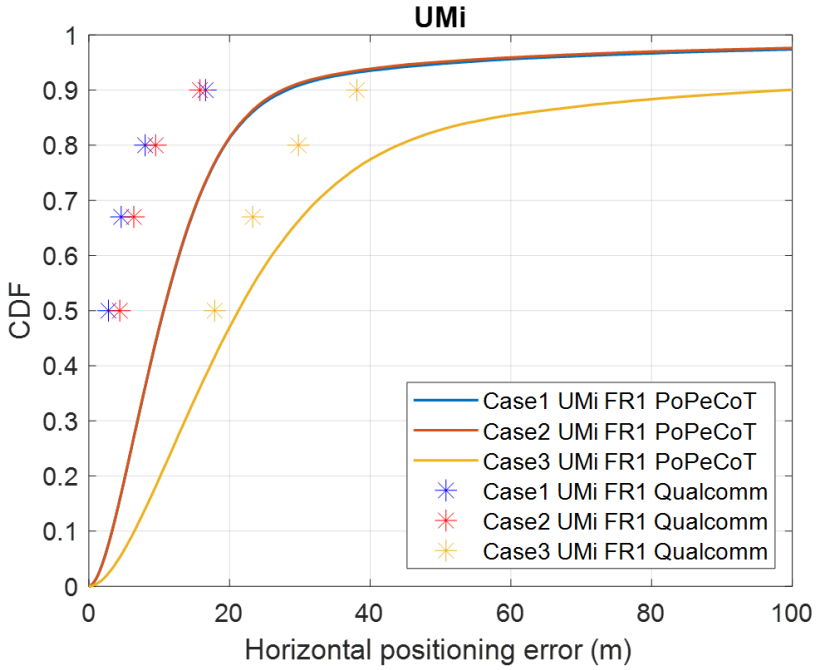


Figure 3.5: Results of RTT for UMi deployments for FR1.

error of $\leq$ 50 m for 80% of UEs. However, when Qualcomm employs a wide bandwidth, the RTT performance successfully meets the target positioning requirements with an estimation accuracy of less than 10 m 80% of the time. For the case of 5G NR simulator, this is almost achieved 50% of the time.

3.1.3.2 Scenario 2: UMa

The results are repeated for the case of UMa network deployment. This study considers two configuration parameters as outlined in Table 3.14. Figure 3.6 presents the performance results obtained from the simulations with a comparative representation of the data presented by Qualcomm. These results are summarized in Tables 3.15.

Table 3.14: Parameters details for FR1 with no synchronization error: RTT [40].

Parameter	**Case1 FR1, 100 MHz**	**Case2 FR1, 50 MHz**	**Case1 FR1, 100 MHz**	**Case2 FR1, 50 MHz**
Channel model (baseline, otherwise state any modifications)	Baseline Channel Model based on common assumptions defined related to the channel models of 3GPP TRs 38.901 / 38.802 / 37.857.		Baseline Channel Model based on common assumptions defined related to the channel models of 3GPP TRs 38.901	
Carrier frequency	4 GHz			
Subcarrier spacing	30 kHz		15 kHz	
Reference Signal Transmission Bandwidth	100 MHz		50 MHz	
Reference Signal Physical Structure and Resource Allocation (RE pattern)	1-port, QPSK sequence		DL:PRS UL: SRS	
Number of sites	19			
Number of symbols used per occasion	10		1	
Interference modelling (ideal muting, or other)	Ideal muting			
Description of positioning technique / applied positioning algorithm (e.g. Least square, Taylor series, etc)	For multi-RTT, the algebraic solution proposed in -Norrdine, Abdelmoumen. (2015). An Algebraic Solution to the Multilateration Problem. 10.13140/RG.2.1.1681.3602. Equal weight is used in the ToA covariance matrix.		RTT, Gauss-Newton algorithm	
Network synchronization assumptions	Perfect Sync and Realistic Sync with T1 = 50 nsec			
Simulations by	Qualcomm		5G NR simulator	

In the scenarios involving a narrower bandwidth, the achieved RTT performance does not

Table 3.15: Summary of evaluation results in UMa scenario: RTT at FR1.

Conditions Techno.	Results by	Source	Network sync.	Horizontal accuracy (m)			
				50%	67%	80%	90%
RTT	Qualcomm	Case 1 UMa FR1	Perfect & Realistic Sync	14.2	28.2	44.4	70.7
		Case 2 UMa FR1	Perfect & Realistic Sync	12.6	25.9	45.7	74.4
	5G NR simulator	Case 1 UMa FR1	Perfect & Realistic Sync	10.005	13.6	17.68	24.46
		Case 2 UMa FR1	Perfect & Realistic Sync	9.91	13.54	17.62	24.22

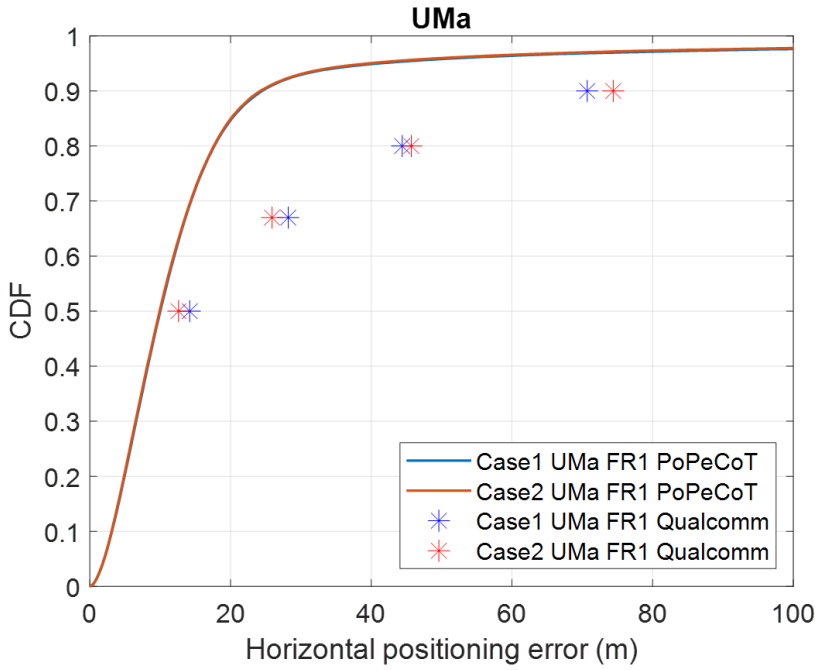


Figure 3.6: Results of RTT for UMa deployments for FR1.

meet the target positioning requirements. Like the case of UMi topology, it only aligns with regulatory standards, achieving a horizontal positioning error lower than 50 m. However, the results obtained from 5G NR simulator for both cases show a position estimation accuracy two times lower than the one provided by Qualcomm. Because in an UMa deployment the environment is less dense than the UMi topology, the resulting RTT performance degrades significantly and this is better seen for the case of company results. Moreover, the comparative results highlight that RTT positioning lies between UTDoA and OTDoA when there are no network synchronization errors. Significantly, RTT outperforms UTDoA and OTDoA when network synchronization errors are present. This underscores the performance of RTT-based positioning in the presence of synchronization challenges.

3.1.4 Uplink evaluation: AoA

Apart from time-based positioning methods, also angle based methods such as AoA have been tested by comparing their performance with the results provided by Huawei [41] for two types of topologies: UMi and UMa having a perfect synchronization network. Different choices for system bandwidth, carrier frequency, subcarrier spacing, and different antenna patterns (in terms of rows and columns spacing in the antenna array) are explored. In the time domain, the SRS resources for positioning span 1 consecutive OFDM symbols which provide enough coverage to reach all BSs involved in the positioning procedures, while the company simulations

use 4 OFDM symbols. Full bandwidth is considered for both UMi and UMa scenarios. The UE position estimation is done following the classical Gauss-Newton (GN) solution as explained in Chapter 2. Note that the computation of angle observables for the case of 5G NR simulator is done using statistical models through Cramér-Rao Bound (CRB) formulas [35] as outlined in Chapter 2. The specific configuration parameters for each scenario are detailed below based on the parameters outlined in [18].

3.1.4.1 Scenario 1: UMi

The scenario examined follows the simulation methodology outlined in the 5G positioning study within 3GPP Release 16 [43], specifically tailored for outdoor environments. The deployment features a hexagonal grid consisting of 19 macro sites, each with three sectors and an ISD of 200 m. Propagation conditions are determined based on the distance between BS and UE, employing distance-dependent LoS probability and path-loss models as already explained in Chapter 2. Angle observables are determined using mathematical models that account for system bandwidth, SNR levels, and antenna elements. The study considers SRS signal with a bandwidth of 100 MHz operating at a carrier frequency of 4 GHz and subcarrier spacing of 30 kHz, and a bandwidth of 50 MHz and 5 MHz, operating at a carrier frequency of 4 and 2 and subcarrier spacing of 15 kHz. Antenna arrays with M = N = 2 elements are employed. The network is assumed to have perfect synchronization among BSs. Table 3.16 provides a summary of the simulation parameters utilized and Figure 3.7 together with Table 3.17 constitutes the results obtained.

Table 3.16: Parameters details for FR1 with no synchronization error:AoA [41].

Parameter	**Case 13 UMi, FR1**	**Case 13 UMi, FR1**	**Case 14 UMi, FR1**	**Case 14 UMi, FR1**	**Case 15 UMi, FR1**	**Case 15 UMi, FR1**	**Case 16 UMi, FR1**	**Case 16 UMi, FR1**
Channel model (baseline, otherwise state any modifications)	38.901	38.901	38.901	38.901	38.901	38.901	38.901	38.901
Carrier frequency	4 GHz	4 GHz	4 GHz	4 GHz	2 GHz	2 GHz	2 GHz	2 GHz
Subcarrier spacing	30 kHz	30 kHz	15 kHz	15 kHz	15 kHz	15 kHz	15 kHz	15 kHz
Reference Signal Transmission Bandwidth	100 MHz	100 MHz	50 MHz	50 MHz	50 MHz	50 MHz	5 MHz	5 MHz
Reference signal (type of sequence, number of ports, ...)	SRS: ZC, 1-port	SRS	SRS: ZC, 1-port	SRS	SRS: ZC, 1-port	SRS	SRS: ZC, 1-port	SRS
Number of sites	19	19	19	19	19	19	19	19
Number of symbols used per occasion	4	1	4	1	4	1	4	1
Description of positioning technique / applied positioning algorithm (e.g. Least square, Taylor series, etc)	UAoA, PSO algorithm	UAoA, Gauss-Newton algorithm	UAoA, PSO algorithm	UAoA, Gauss-Newton algorithm	UAoA, PSO algorithm	UAoA, Gauss-Newton algorithm	UAoA, PSO algorithm	UAoA, Gauss-Newton algorithm
Network synchronization assumptions	No sync error	No sync error	No sync error	No sync error	No sync error	No sync error	No sync error	No sync error
Number of antenna elements	N/A	M=N=2	N/A	M=N=2	N/A	M=N=2	N/A	M=N=2
Simulations by	Huawei	5G NR simulator	Huawei	5G NR simulator	Huawei	5G NR simulator	Huawei	5G NR simulator

Table 3.17: Summary of evaluation results in UMi scenario: UAoA at FR1 [41].

Conditions Techno.	**Results by**	**Source**	**Network sync.**	**Horizontal accuracy (m)**			
				50%	67%	80%	90%
UAoA	Huawei	Case 13 UMi FR1	Perfect sync.	15.7	26.6	41.8	63.8
		Case 14 UMi FR1	Perfect sync.	15.3	24.8	36.6	60.5
		Case 15 UMi FR1	Perfect sync.	16.9	26.6	41.7	61.6
		Case 16 UMi FR1	Perfect sync.	19.6	31.3	47.5	65.3
	5G NR simulator	Case 13 UMi FR1	Perfect sync.	14.4	21.6	31.7	50.97
		Case 14 UMi FR1	Perfect sync.	10.1	15.32	22.67	35.5
		Case 15 UMi FR1	Perfect sync.	6.9	10.34	15.1	23.6
		Case 16 UMi FR1	Perfect sync.	6.68	9.73	14.4	23.01

The simulation results indicate that the 5G NR simulator outperforms Huawei in terms of performance. However, it is essential to note that the configurations, utilizing a minimal number of antenna elements (4 in total), have only met regulatory requirements for 80% of UEs. Examining the graph, it is evident that for Case 13, both simulator and company results exhibit

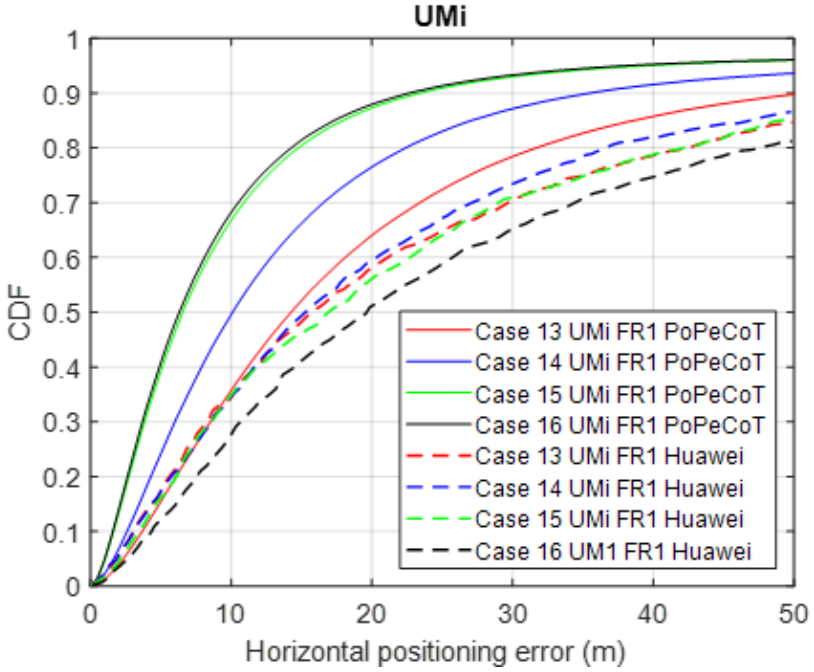


Figure 3.7: Results of AoA for UMi deployments for FR1.

similar positioning accuracy performance, whereas, for the remaining three cases, a significant disparity is observed. The robust performance, particularly noticeable in Case 13, is attributed to the presence of LoS conditions. The dominance of LoS conditions contributes to lower angle errors, resulting in minimal horizontal positioning errors.

3.1.4.2 Scenario 2: UMa

The simulations are repeated for the UMa environment. The configuration parameters are maintained the same. Figure 3.8 presents the performance results obtained from the simulations, offering a comparative analysis with the data presented by Huawei and summarized in Table 3.19.

Table 3.18: Parameters details for FR1 with no synchronization error: UAoA [41].

Parameter	Case 13 UMa, FR1	Case 13 UMa, FR1	Case 14 UMa, FR1	Case 14 UMa, FR1	Case 15 UMa, FR1	Case 15 UMa, FR1	Case 16 UMa, FR1	Case 16 UMa, FR1
Channel model (baseline, otherwise state any modifications)	38.901	38.901	38.901	38.901	38.901	38.901	38.901	38.901
Carrier frequency	4 GHz	4 GHz	4 GHz	4 GHz	2 GHz	2 GHz	2 GHz	2 GHz
Subcarrier spacing	30 kHz	30 kHz	15 kHz	15 kHz	15 kHz	15 kHz	15 kHz	15 kHz
Reference Signal Transmission Bandwidth	100 MHz	100 MHz	50 MHz	50 MHz	50 MHz	50 MHz	5 MHz	5 MHz
Reference signal (type of sequence, number of ports, ...)	SRS: ZC, 1-port	SRS	SRS: ZC, 1-port	SRS	SRS: ZC, 1-port	SRS	SRS: ZC, 1-port	SRS
Number of sites	19	19	19	19	19	19	19	19
Number of symbols used per occasion	4	1	4	1	4	1	4	1
Description of positioning technique / applied positioning algorithm (e.g. Least square, Taylor series, etc)	UAoA, PSO algorithm	UAoA, Gauss-Newton algorithm	UAoA, PSO algorithm	UAoA, Gauss-Newton algorithm	UAoA, PSO algorithm	UAoA, Gauss-Newton algorithm	UAoA, PSO algorithm	UAoA, Gauss-Newton algorithm
Network synchronization assumptions	No sync error	No sync error	No sync error	No sync error	No sync error	No sync error	No sync error	No sync error
Number of antenna elements	N/A	M=N=2	N/A	M=N=2	N/A	M=N=2	N/A	M=N=2
Simulations by	Huawei	5G NR simulator	Huawei	5G NR simulator	Huawei	5G NR simulator	Huawei	5G NR simulator

The results presented show that UMa layout, characterized as a conventional deployment, attains regulatory requirements with horizontal accuracy limited to ≤ 50 m for 80% of the time, particularly in the last two cases. However, it is noteworthy that even in the case of perfect synchronization, a considerable degradation of the AoA accuracy is observed compared to the previous scenario. This is because the enhanced BS density in the UMi layout contributes to superior accuracy. Additionally, several factors have influenced the variance of angle estimates

Table 3.19: Summary of evaluation results in UMa scenario: UAoA at FR1 [41].

Conditions Techno.	Results by	Source	Network sync.	Horizontal accuracy (m)			
				50%	67%	80%	90%
UAoA	Huawei	Case 13 UMa FR1	Perfect sync.	53.8	92.3	147.2	210.4
		Case 14 UMa FR1	Perfect sync.	56.8	91.2	133.9	211.7
		Case 15 UMa FR1	Perfect sync.	49.0	76.8	123.3	164.6
		Case 16 UMa FR1	Perfect sync.	58.8	94.5	144.3	198.1
	5G NR simulator	Case 13 UMa FR1	Perfect sync.	69.5	102	140.8	208.7
		Case 14 UMa FR1	Perfect sync.	51.6	74.3	102.7	152.9
		Case 15 UMa FR1	Perfect sync.	28.7	41.7	58.13	85.02
		Case 16 UMa FR1	Perfect sync.	19.4	42.2	56.8	76.8

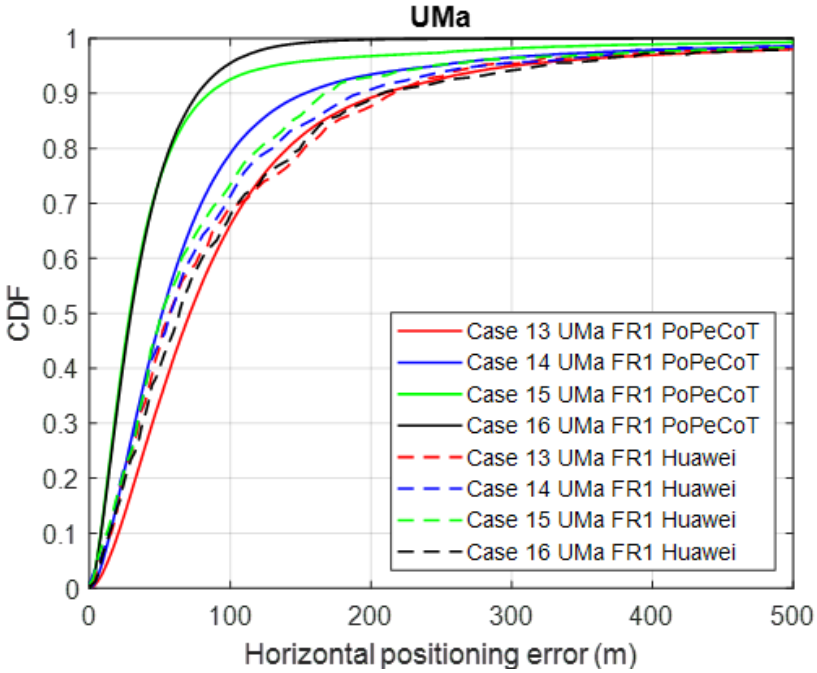


Figure 3.8: Results of AoA for UMa deployments for FR1.

such as subcarrier spacing and antenna array configuration. The subcarrier spacing linearly increases the angle variances. This effect is attributed to the linear increase in noise variance with subcarrier spacing. Therefore the cases with lower subcarrier spacing have a better performance. Moreover, the total number of antenna elements in the array is also a crucial factor. Here, for the case of angle estimates, the variance is proportional to the inverse square of antenna spacing. The number of rows and columns in the array contributes to a cubic decrease in angle estimate variances. This explains the degradation in positioning accuracy obtained. A larger number of antennas is needed to enhance the angle estimation performance. On the other hand, the angle variance remains independent of bandwidth changes different for the time-based methods where the bandwidth had a great impact on the accuracy of the position estimation. In general, the 5G NR simulator demonstrates superior performance compared to Huawei, with closer results observed in the first two cases.

3.2 5G positioning performance in crucial use cases

The need for an accurate, reliable and secure cellular positioning has emerged in a number of 5G and beyond application verticals discussed in Chapter 1. Therefore, in this section, we bring the analysis of the 5G performance of the chosen scenarios for two disruptive technologies: IoT and automated driving. The positioning capabilities of these scenarios are crucial for the following use cases: IoT and autonomous car respectively. Understanding such properties is fundamental to characterize the positioning methods and conditions for precise cellular positioning. With the help of the 5G NR simulator, we not only investigate the cellular positioning performance but also the impact of synchronization, system bandwidth and BS density in the 5G urban network deployed. The standalone time-based positioning methods OTDoA, UTDoA and RTT together with the fallback technology, CID, have been analyzed. The simulation scenarios for both use cases use dedicated positioning signals: PRS for downlink and SRS for uplink, both spanning 1 OFDM symbol. These scenarios are based on an urban deployment map, which comes with an experimental data file of the user's position of the Tres Cantos (Madrid) map [44].

3.2.1 Low-energy use case: IoT

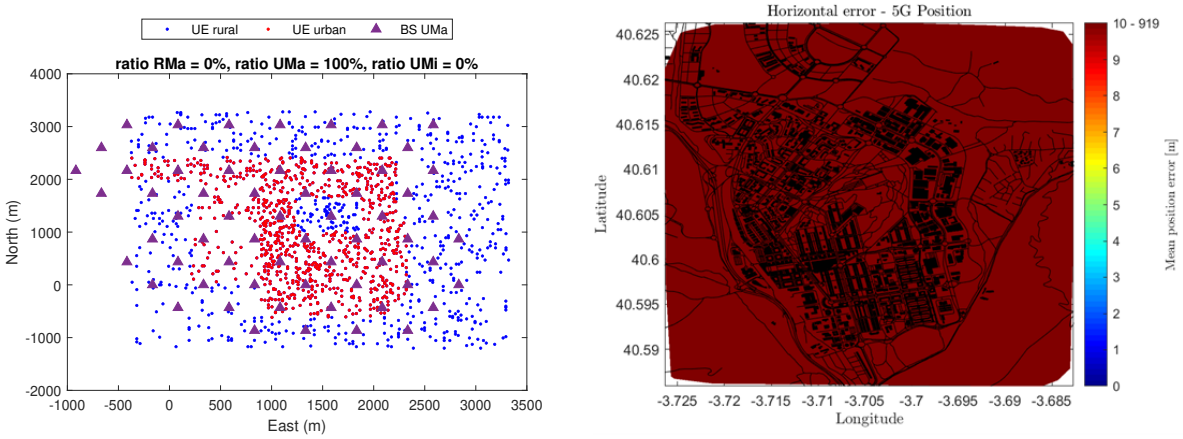
The scenario examined in this use case follows the simulation methodology outlined in the 5G positioning study within 3GPP Release 16 [43], in concrete for outdoor environments. It is based on a predefined network scenario, encompassing an UMa deployment, utilizing a deep urban deployment map. The BSs are strategically placed above building rooftops, with BS heights ranging from 20 to 40 meters. The deployment features a hexagonal grid consisting of seven macro sites, each with three sectors and an ISD varying between 1732 meters in rural areas and 500 meters in urban areas. The UEs are randomly distributed within the coverage area of this predefined deployment scenario, as depicted in Figure 3.9. The urban area constitutes 100% of the positions. Propagation conditions are determined based on the distance between BS and UE, employing distance-dependent LoS probability and path-loss models following the procedure explained in Chapter 2. The multipath channel is stochastically generated in accordance with the tabulated channel parameters in the 3GPP standard [26]. Each receiver position undergoes performance evaluation over 96 Monte Carlo iterations.

The ranging observables for all core methods are computed considering specific propagation conditions, channel models, system bandwidth, SNR levels, and time-delay estimators through the formulas depicted in Chapter 2. The study considers a narrowband network with a bandwidth of 180 kHz operating at a carrier frequency of 2 GHz within the cmWave FR1 of 5G NR. Two cases are considered: a network with no synchronization error among BSs and a network with 50 ns synchronization error. For the estimation of each UE position, 6 most powerful BS (those close to receiver locations with highest SNR) are considered.

Due to the fact that the map used for analysis has a mix of urban and open points, the results have been represented separately for open environment and urban environment. Figures 3.10 represent the CDF of horizontal position errors of both environments. The presence of a narrowband signal and the extended coverage areas that lead to a lower network density result in heavy effects in a bad UE positioning estimation, where the horizontal positioning errors are above 30 m for most of the position points. This can be seen in the heat map depicted in Figure 3.9, where the color bar is limited to a maximum of 10 m that corresponds to the

target accuracy of the standard. The horizontal error for urban points depends on both, the height of the buildings and the proximity between them. A higher number of buildings and a shorter distance between them entails a greater horizontal error. Moreover, this degradation comes also from the predominance of NLoS BS (93.7% of all the deployed BSs) that is difficult to be mitigated due to the narrow bandwidth available. The presence of synchronization errors constrains the performance of cellular positioning. This is reflected by the low percentage of times that the CID is used as a fallback solution. Note that when the 3D position solution does not converge due to bad geometry, outlier measurements, or lack of measurements, the CID method is used, i.e., the position of the most powerful BS (with larger SNR) is assigned to the estimated receiver position.

Overall, results show a better accuracy in an urban environment compared to an open one where the density of the network is lower. Even in conditions of no synchronization errors, the accuracy has a small change compared to the degradation because of synchronization issues due to the dominance of NLoS BS. OTDoA and UTDoA give similar performance, but UTDoA are favoured for low-energy IoT applications since they do not entail extra operation within the UE and therefore they perform minimal power consumption. Among the core methods used, RTT improves accuracy (two times smaller the position error), but comes at the cost of complexity and additional UE power consumption. The results are summarized in Table 3.20 where are considered the mix of urban and open areas together. This means that the simulation results entail a mix of the effects of both environments.



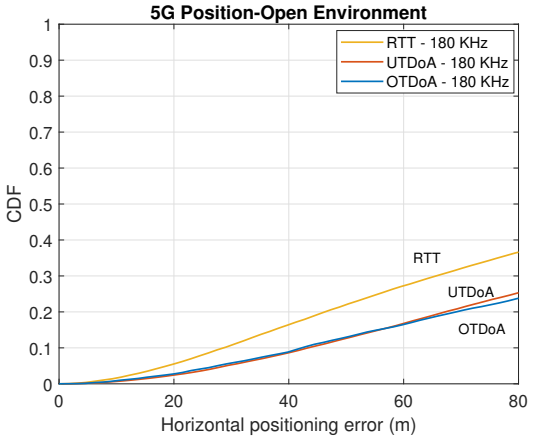
(a) BS distribution for a UMa deployment.

(b) 5G position error heat map. The areas with horizontal positioning error > 10 m is represented with red color. The maximum error achieved for the given scenario is 999 m.

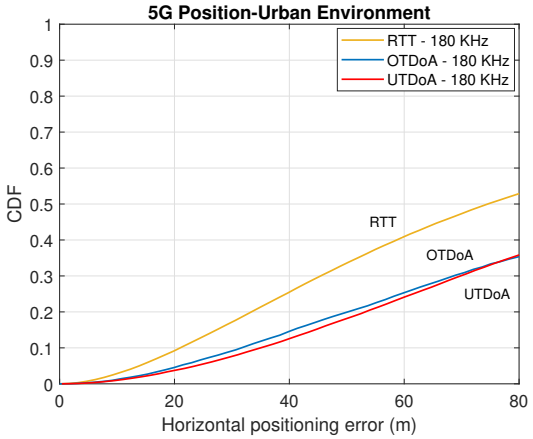
Figure 3.9: IoT use case environment implementation.

Table 3.20: Positioning accuracy of IoT use case for a UMa deployment.

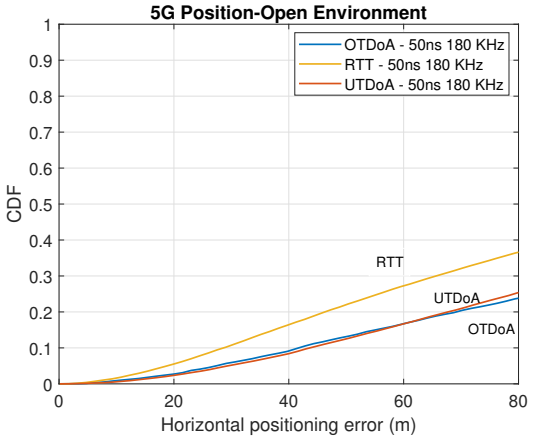
Prob. position fix (%)	**OTDoA - Perf. sync.**		**OTDoA - 50ns sync. err.**		**UTDoA - Perf. sync.**		**UTDoA - 50ns sync. err.**		**RTT**	
	OTDoA	Cell ID	OTDoA	Cell ID	UTDoA	Cell ID	UTDoA	Cell ID	RTT	Cell ID
0 m <hor. pos. acc. ≤ 1 m	0.14	-	0.01	-	0.04	-	0.05	-	0.02	-
1 m <hor. pos. acc. ≤ 10 m	0.89	-	0.89	-	0.82	0.1	0.74	0.02	2.3	0.01
10 m <hor. pos. acc. ≤ 3 m	5.8	0.8	6	0.9	5.6	0.1	5.71	0.1	11.98	0.05
hor. pos. acc. >30 m	45.07	47.3	43.6	48.6	57.14	36.2	58.1	35.28	62.8	22.84
Total (%)	51.9	48.1	50.5	49.5	63.6	36.4	64.6	35.4	77.1	22.9



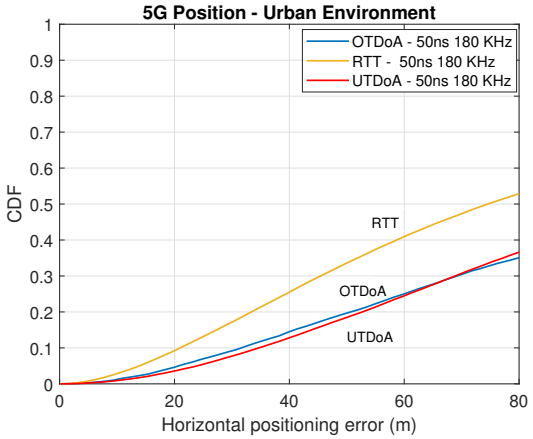
(a) No synchronization error: rural environment.



(b) No synchronization error: urban environment.



(c) With synchronization error: rural environment.



(d) With synchronization error: urban environment.

Figure 3.10: IoT use case 5G horizontal positioning error.

3.2.2 High-accuracy use case: Autonomous car

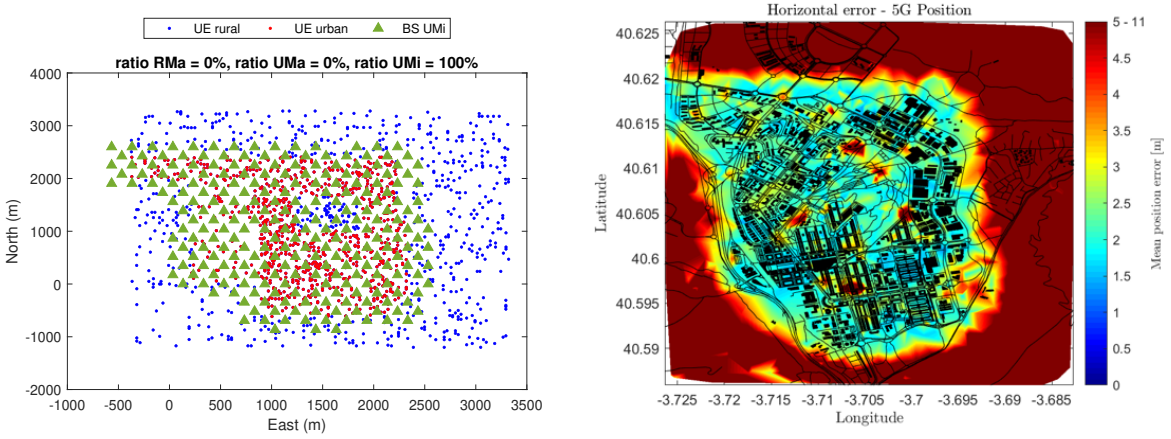
The exploration of 5G positioning impact, particularly when autonomous vehicles operate in challenging environments, such as urban canyons is based on a predefined network scenario, encompassing an UMi deployment. It utilizes a deep urban deployment map, which comes with an experimental data file of the user's position. The deployment consists of a hexagonal grid with seven macro sites, where each has three sectors with an ISD varying between 1732 meters in rural areas and 200 m in dense urban areas. Like in the previous use case, also here the simulation methodology outlined in the 3GPP standard [43] for outdoor environments is followed. The BSs deployment and the propagation conditions follow the same approach as in the IoT use case. The UEs are randomly distributed within the coverage area of the predefined deployment scenario characterized by a deep urban area with 100% of the positions as depicted in Figure 3.11. Also for the autonomous car use case, for each receiver position, 96 Monte Carlo iterations are carried out to undergo the performance evaluation.

The ranging observables for all core methods are computed considering specific propagation conditions, channel models, system bandwidth, SNR levels, and time-delay estimators through the formulas depicted in Chapter 2. The study considers a wide bandwidth (maximum system bandwidth of 100 MHz) operating at a carrier frequency of 4 GHz within the cmWave FR1 of 5G

NR. In the high-density network, two cases are considered: a network with no synchronization error among BSs and a more realistic deployment with 50 ns synchronization error. For the estimation of each UE position, 6 most powerful BS (those close to receiver locations with highest SNR). The results obtained from the analysis of urban and open points have been represented separately for the open environment and the urban environment.

Figures 3.12 represent the CDF of horizontal position errors of both environments. There is a significant improvement in accuracy compared to the IoT scenario thanks to the presence of a wide bandwidth signal and the deep network density. This can be seen in the heat map depicted in Figure 3.11 with color-bar limited to 5 m horizontal positioning error. The heat map represents the horizontal errors in urban areas. The horizontal error is smaller in areas with a denser network than in the zones where the base stations are placed at a bigger distance between them. Indeed, this is reflected visually with the CDF plots where a better performance in position estimation for urban environments compared to open environments can be clearly seen. In conditions of perfect synchronization, OTDoA outperforms the rest of the methods (UTDoA and RTT), and RTT is in between UTDoA and OTDoA. When synchronization error is considered, the position estimation error increases. Since RTT performance does not depend on precise network synchronization, it outperforms the rest of the methods. All in all, UTDoA have a poor performance compared to the OTDoA due to several reasons. Firstly, the low transmit power affects signal strength and, consequently, the accuracy of time-of-arrival measurements. Secondly, the low antenna gain degrades the effective isotropic radiated power (EIRP), leading to weaker signals and potentially worse positioning accuracy.

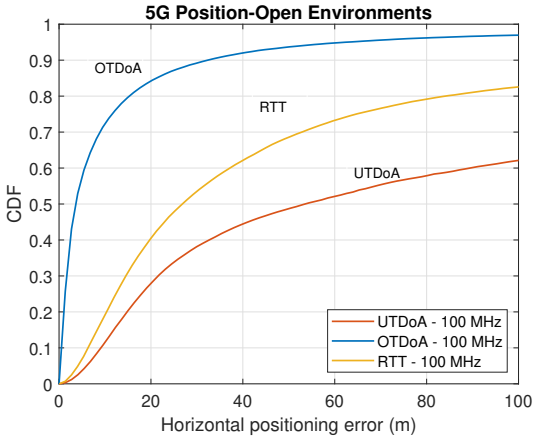
Finally, Table 3.21 summarizes the probability of position fix of all three core methods and the fallback method used in this analysis. These results clearly reflect more accurate and reliable position estimation since the percentage of the usage of CID method is lower than the IoT use case starting from half the value.



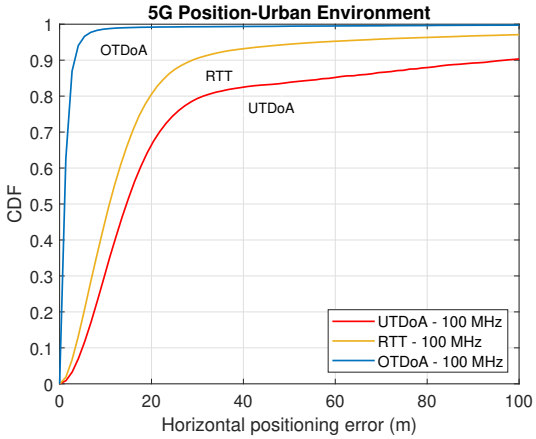
(a) BS distribution for a UMi deployment.

(b) 5G position error heat map.

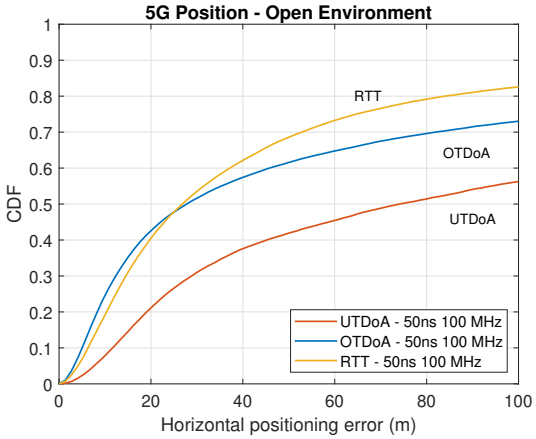
Figure 3.11: Autonomous cars use case environment implementation.



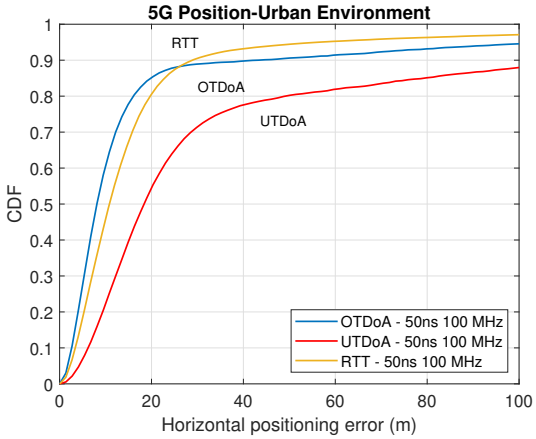
(a) No synchronization error: rural environment.



(b) No synchronization error: urban environment.



(c) With synchronization error: rural environment.



(d) With synchronization error: urban environment.

Figure 3.12: Autonomous cars use case 5G horizontal positioning error.

Table 3.21: Positioning accuracy of Autonomous cars use case for a UMi deployment.

Prob. position fix (%)	**OTDoA - Perf. sync.**		**OTDoA - 50ns sync. err.**		**UTDoA - Perf. sync.**		**UTDoA - 50ns sync. err.**		**RTT**	
	OTDoA	Cell ID	OTDoA	Cell ID	UTDoA	Cell ID	UTDoA	Cell ID	RTT	Cell ID
0 m <hor. pos. acc. $\leq$ 1 m	36	-	1.2	-	13	0.11	0.2	-	0.9	-
1 m <hor. pos. acc. $\leq$ 10 m	50.9	-	43.4	0.06	38.4	0.03	15.5	0.1	33.1	0.07
10 m <hor. pos. acc. $\leq$ 3 m	8.8	0.04	27.4	0.26	22	0.26	37.3	0.3	40	0.03
hor. pos. acc. >30 m	4.3	0.86	13.6	14.08	17.3	21.6	21	25.6	21.2	4.7
Total (%)	99.1	0.9	85.6	14.4	78	22	74	26	95.2	4.8

3.3 Bridging simulation and real-world experimentation for high-accuracy 5G positioning solutions

Like we stated since the beginning of this chapter, the contribution with the development of the 5G NR simulator aimed at enhancing positioning solutions for 5G applications by taking a comprehensive approach through a combination of simulations and theoretical assessments. With a focus on achieving high-accuracy positioning estimation, particularly for applications like autonomous driving and industrial automation, we provided valuable insights into the behavior of 5G technology in these two environments. By randomly deployed transmitting points, the obtained results revealed a diverse range of 2D positioning errors, ranging from sub-meter to several hundred meters. However, when it comes to real implementations, a gap between theoretical expectations and real-case scenarios can be faced. This motivated us to compare

the performance of the positioning approach with a real experiment performed by the Fraunhofer Institute for Integrated Circuits IIS (FIIS) [44] in the environment of an industrial 5G campus network in the mark of the GINTO5G project founded by ESA, in order to amplify the positioning accuracy.

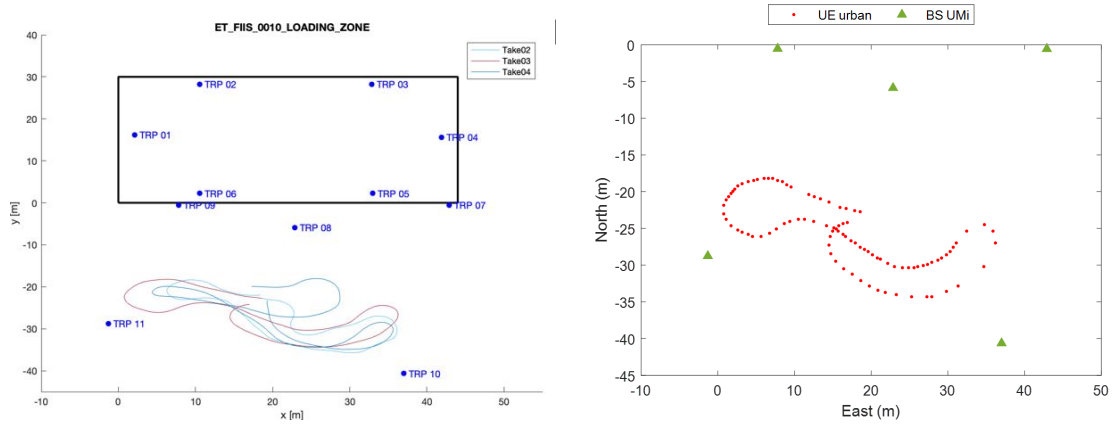
3.3.1 Scenario definition and implementation

The scenario to be evaluated consists in a FIIS 0010 Loading Zone (see the left side of Figure 3.13), representing an UMi scenario for outdoor UEs. The evaluation is based on the OTDoA positioning method.

On the 5G NR simulator side, the analysis utilizes the channel model defined in technical report (TR) 38.901 [26] for FR1 downlink positioning, using a PRS signal with a 100 MHz bandwidth and 4 GHz carrier frequency. A RMSE of the estimated position, CDF of the position error, and the probability of position fix are employed as performance metrics.

On the FIIS side, the anchors Transmitting Reference Point (TRP) are predominantly in LoS, with potential multipath signals at the edges. A LoS model is considered, ensuring LoS probability between BSs and UE for three TRPs, while LoS/NLoS link states are defined for TRPs at the edges using distance-dependent LoS probability models from 3GPP TR 38.901 [26]. Results are presented with perfect synchronization.

The performance evaluation involves five transmitters and a UE trajectory distribution meaning that the input receiver locations follow a trajectory. TRPs 7-11 are used for positioning, and the chosen UE trajectory is the red line as depicted on the right side of Figure 3.13.



(a) FIIS implementation [44].

(b) 5G NR software simulation.

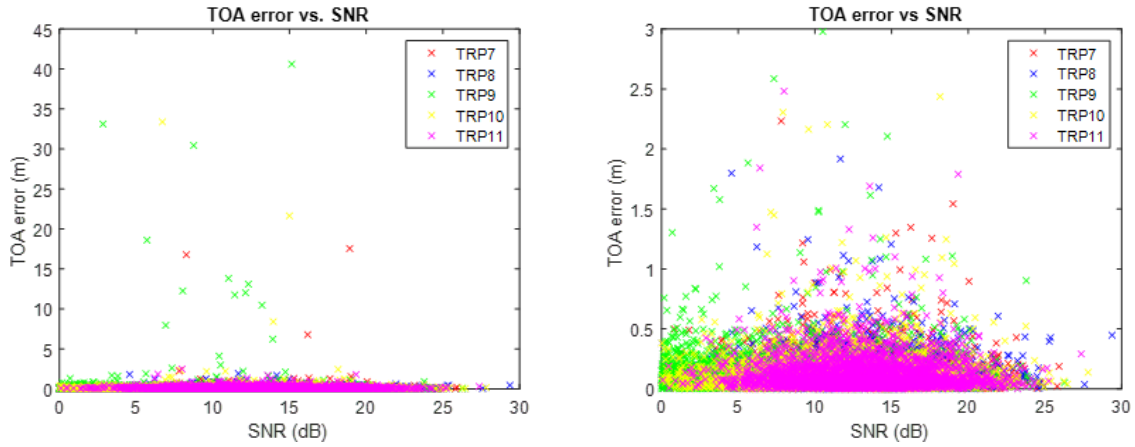
Figure 3.13: Loading Zone environment experimentation.

A comparison between the ranging models of FIIS FR1 campaign and 5G NR simulator is conducted. 5G NR simulator simulates the received downlink signal, estimating ranging error for different SNR levels, utilizing LoS probabilities calculated as in 3GPP TR 38.901 [26]. The CDF of ranging errors per SNR level is then computed and interpolated. For FIIS measurements, TDoA error determination relies on measuring relative to a reference Time of Arrival (ToA), chosen as ToA error "zero" for the corresponding TRP (TRP8). In 5G NR simulator, the simulator uses the first BS with the highest SNR as the reference for each UE. To align with

FIIS configurations, TRPs 7 and 9 are set to be distance-dependent, transitioning between LoS and NLoS conditions. TRPs 8, 10, and 11 are consistently set in LoS. However, discrepancies arise due to height and distance conditions, impacting the results.

3.3.2 Experimentation evaluation and analysis.

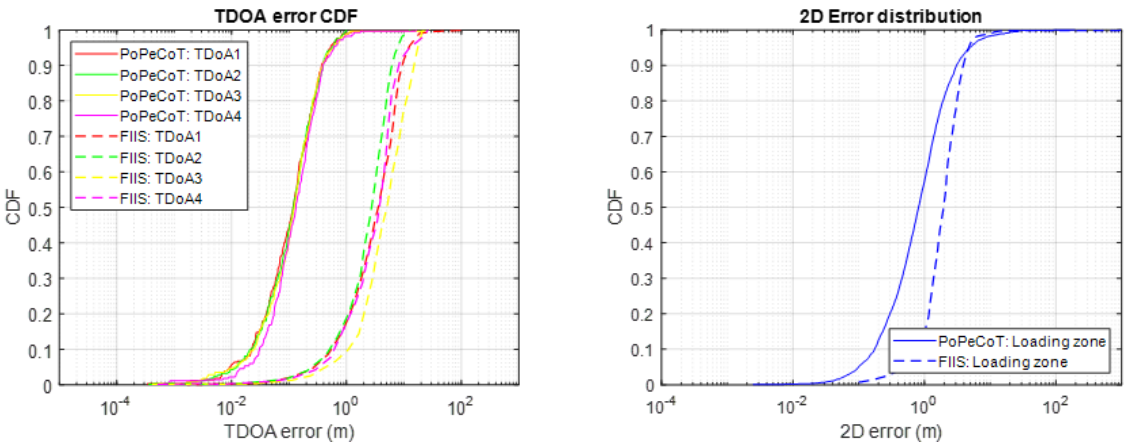
The accuracy of position estimation when using time-based positioning methods is closely related to ranging errors. In a direct comparison of ToA errors relative to SNR values for the outdoor experimentation as depicted in Figure 3.14, 5G NR simulator results exhibit a noteworthy observation: significant ToA error does not necessarily align with low SNR. This divergence can be attributed to SNR behavior concerning multipath signals. In scenarios with multiple reflected multipath transmissions, self-interference can reduce SNR, even if the LoS signal is detectable with low error.



(a) 5G NR software results.

(b) 5G NR software results for ToA error < 3 m.

Figure 3.14: ToA error relative to SNR.



(a) TDoA Error distribution.

(b) 2D error positioning.

Figure 3.15: Experimental results.

The distribution of TDoA error computation for the outdoor experiment where TRPs 8 is chosen as reference is depicted in Figure 3.15. It can be seen that the estimated theoretical

ranging errors are lower compared to the ones in the real experiment. These optimistic results are due to the perfect network synchronization considered in simulations and the conditions of wide bandwidth. Additionally, to the channel model, which is based on the 3GPP standard TR38.901, are assigned the configuration parameters defined by FIIS.

The distribution of TDoA error computation for the outdoor experiment, where TRPs 8 is chosen as reference, is depicted in Figure 3.15. It can be seen that the estimated theoretical ranging errors are lower compared to the ones by the real experiment. These optimistic results are as a result of assuming perfect network synchronization and in conditions of wide bandwidth. Additionally, the predominance of perfect LoS conditions almost all the time simulated by the channel model based on the 3GPP standard TR38.901 [26] further contributes to the observed results. However, even though the real experiments are carried out in LoS conditions, the one provided by the simulator does not fully align with real-world scenarios where real hardware impairments (HIs) of the 5G transceivers such as Carrier Frequency Offset (CFO), Antenna Phase Offset (APO), in-phase-and-quadrature (IQ) imbalance are common and have a huge impact in the degradation of the estimation. Therefore, it is essential to interpret the obtained results within the context of these simulated conditions, acknowledging the potential deviation from real-world scenarios with diverse and dynamic channel environments. Tables 3.22 and 3.23 present the mean and median ToA error for the loading zone test case.

Area	TRP7	TRP8	TRP9	TRP10	TRP11
Loading Zone - FIIS	0.57	0	0.34	0.84	0.61
Loading Zone - 5G NR simulator	0.1796	0	0.252	0.1942	0.1707

Table 3.22: Mean TDoA Error in meters.

Area	TRP7	TRP8	TRP9	TRP10	TRP11
Loading Zone - FIIS	0.40	0	0.26	0.49	0.44
Loading Zone - 5G NR simulator	0.1137	0	0.1221	0.121	0.1186

Table 3.23: Median TDoA Error in meters.

The estimated ranging errors are then used to estimate the position of each receiver. Positioning accuracy is evaluated for both 2D and 3D scenarios, with Key Performance Indicators (KPI) presented in Table 3.24 for both FIIS and 5G NR simulator. These results are visually presented in Figure 3.15 that showcases the 2D distribution, emphasizing Circular Error Probable (CEP) and Spherical Error Probable (SEP) as more suitable KPIs. 5G NR simulator, with lower ToA errors, outperforms FIIS in positioning accuracy. CEP95 and SEP95 values indicate a 2D accuracy below 3 meters for FIIS and below 2 meters for the 5G simulator in the Loading Zone. These results reaffirm the gap between theoretical expectations and real-case scenarios.

Table 3.24: Positioning accuracy KPIs for the 5G FR1 downlink measurements. All KPIs are expressed in meters.

Test	**Iteration**	**Mean 2D**	**Mean 3D**	**CEP50**	**CEP95**	**SEP50**	**SEP95**	**TRPs used for positioning**
Loading Zone - FIIS	1	1.27	4.21	1.01	1.97	3.27	8.76	7-11
	2	40.84	55.94	1.15	2.84	4.52	8.42	7-11
	3	1.38	3.93	0.97	2.60	3.12	9.85	7-11
	all			1.05	2.57	3.58	9.09	
Loading Zone - 5G NR simulator	all	1.65	1.77	0.8148	4.89	0.8415	5.0913	7-11

3.4 Conclusions

In this chapter, the performance of 5G positioning in different types of environments under various options and configurations is presented. The results are compared with other contributions from different companies in order to assess the reliability of the simulator.

Moreover, analysis to assess and enhance the positioning capabilities in scenarios crucial for two challenging use cases (IoT and autonomous cars) are performed. The aim was to offer valuable insights that can drive advancements in connected technologies. In IoT scenarios, where narrowband cellular technologies are prevalent, extended coverage areas lead to lower network density. This, in turn, results in NLoS scenarios, introducing multipath effects that are challenging to mitigate due to the narrow bandwidth available. The effects of NLoS and the improvements of accuracy after mitigation will be presented in Chapters 4 and 5. Additionally, the geometrical distribution of base stations in extended coverage deployments tends to be suboptimal, further hampering positioning accuracy. Trilateration-based techniques are also hindered by the requirement for tight network synchronization, which is often not a standard feature in cellular IoT setups. Consequently, the performance of cellular IoT positioning methods is primarily constrained by low network density, narrow bandwidth, and synchronization issues. For low-energy IoT applications, the most efficient positioning techniques are those that do not entail extra transmission or operation within the UE. The standard techniques like CID and UTDoA are favored due to their minimal power consumption. CID, while power-efficient, offers lower accuracy primarily dependent on the coverage area of the connected base station. RTT techniques improve accuracy, but come at the cost of additional UE power consumption. On the other hand, the use of 5G positioning in autonomous vehicles, offers a promising avenue to improve the accuracy of vehicle localization. The advanced physical features of 5G networks, such as optimized waveforms, wide bandwidth, cmWave technology, and high-density networks, make them well-suited for positioning purposes. However, it is important to note that the network density may vary depending on the area, potentially reducing the availability of 5G localization.

Finally, the combination of simulation and real-world experiments serves not only to assess performance but also to gauge the practical impact, bridging a better understanding of the behaviors of today's equipment, potentially influencing future standardization efforts. The results from the comparison of simulations with a real experiment show that the positioning performance achieved from simulations is very optimistic compared to what is achieved in reality. Therefore, several external conditions such as hadware imparments, propagation conditons: multipath and interference should be taken into account during analysis. For this reason, experimental evaluations with actual 5G signals will be presented in Chapter 6.

Chapter 4

Measurement characterization, outlier detection and exclusion for 5G positioning

Results presented in Chapter 3 addressed a significant challenge in cellular network positioning: achieving accurate positioning in demanding environments, such as urban canyons. This has been a concern of utmost importance for both carrier operators and network users caused by Non Line of Sight (NLoS) propagation. The results reafirmed the fact that NLoS hampers the accurate positioning information. The NLoS conditions are often caused by obstacles in urban settings. Most of the existing contributions to cellular positioning tend to overlook the presence of these propagation obstacles, often assuming an "achievable" positioning performance [6]. Some consider multipath and NLoS, but fail to differentiate between Line of Sight (LoS) and NLoS scenarios [45].

This chapter's primary objective is to introduce the implementation of a mechanism for detecting NLoS conditions in cellular positioning, drawing inspiration from the Receiver Autonomous Integrity Monitoring (RAIM) technique used in Global Navigation Satellite System (GNSS) [46]. The proposed technique ensures the integrity of the position solution by identifying and excluding erroneous measurements. Beyond NLoS detection, this approach offers a more accurate evaluation of actual cellular positioning compared to the traditional assumptions of ideal propagation or mixing LoS and NLoS observations.

The core concept behind this technique lies in assessing the redundancy of range measurements acquired from multiple Base Station (BS) to identify potential faulty transmitters [47]. The technique integrates both Fault Detection (FD) and Fault Detection and Exclusion (FDE) capabilities. In cases where there are more BSs than unknowns, the position is calculated using the minimum required BS ranges, while ranges from remaining BSs are cross-checked for consistency. A substantial difference between a BS's range and the expected value indicates a faulty bias. With a sufficient number of BSs, the algorithm can detect the BS responsible for degradation and exclude it from the calculation. Each positioning solution is defined by a 2-D or 3-D range "tolerance limit" that filters out measurements affected by faulty bias. By addressing the crucial issue of NLoS conditions in cellular positioning, this chapter contributes to enhancing accuracy and reliability, enabling more effective utilization of cellular networks for

location-based services and applications.

This chapter is organized as below. It begins with a discussion of variations of the continuity and integrity requirement and their influence on the achieved protection level described in Section 4.1. The intent is to support the future development of integrity algorithms by providing insights into critical parameters for achieving tighter protection levels using 5G signals. It continues with the presentation of the main integrity monitoring approaches [48] and analyses the limitations of the proposed method (see Sections 4.2 and 4.3). Furthermore, Section 4.4 provides a detailed description of the scenario used to test the feasibility of the method and analyses the results.

4.1 Integrity

Location estimation in wireless systems has been the subject of extensive study over the past few decades. Despite this, there are still unresolved issues, particularly in scenarios where many obstacles between transmitter (TX) and receiver (RX) are present (i.e. with limited direct LoS). These scenarios are common in both indoor environments (like homes, offices, and shopping malls) and outdoor settings (like cities and urban areas). In such situations, maintaining the accuracy and efficiency of location estimation becomes a challenge. Errors cannot be tolerated as readily, and having a consistent and reliable solution for determining location becomes crucial. This brings to the concept of integrity monitoring. Integrity monitoring is defined as the system's ability to detect anomalies and warn users when it is not safe to rely on the system's outputs. For accurate navigation using cellular networks, this means that the system must be able to identify incorrect measurements and provide a measure of how confident it is in its performance. This led to the exploration of methods for determining when the system is safe to use, thus reducing the impact of inaccuracies. Interestingly, although a lot of research has been done in this area for GNSS, to our knowledge, so far, in 5G there has not been any work focused on identifying faulty measurements from base stations due to obstructed signal paths (NLoS), not even using techniques similar to those used in GNSS.

Integrity assurance in positioning relies on two key factors: understanding the nature of measurement errors and the likelihood that these errors might deviate from the norm. This requires a deep comprehension of the sources of errors affecting measurements. If errors in the range of 5G signals are not accurately understood and modeled, the effectiveness of integrity monitoring is hampered. Moreover, the number and arrangement of measurements also affect how well integrity monitoring performs.

The core idea of the integrity monitoring approach researched in this chapter involves using redundant information to autonomously spot faults. It is designed to identify individual faults one at a time. In this scheme, there is a threshold called the Alarm Limit (AL), representing the maximum allowable error. The integrity risk P_{risk} indicates the chance that the actual position exceeds this limit without warning the user within a specific time period [49]. Another key concept is the Protection Level (PL) [48], which sets a statistical limit on the position error, ensuring the integrity risk stays within acceptable levels.

Mathematically, the integrity risk limited by the protection level can be expressed as follows:

$$P\left(|\hat{x} - x| > AL \& PL < AL\right) \leq P_{risk}. \tag{4.1}$$

The possible ways that cellular signals might go wrong are not fully explored yet and no guarantees are yet provided by service providers regarding the performance of these systems.

4.2 Outlier characterization

When obstacles obstruct the LoS signal, the receiver loop produces an unpredictable 'fault' deviation that cannot be effectively characterized. In this context, 'fault' encompasses all abnormal observations that result in unforeseen errors. This section provides a comprehensive description of both the process of generating observations and the FDE method.

4.2.1 5G signal pseudorange measurements

Observed Time Difference of Arrival (OTDoA) is adopted in 5G for the down-link synchronization of Positioning Reference Signal (PRS) signals [21], similar to what was already done in previous releases for 4G/Long Term Evolution (LTE) downlink positioning. To calculate a user's position, the distance between the user's receiver and multiple BSs with known locations must be measured. While the position computation is done by the network, the User Equipment (UE) is in charge of measuring the time delays on the synchronization signals it receives from neighboring BSs, which actually provide the Euclidean distance between UE and BS. In practice, however, these measurements are affected by an unknown clock offset and noise thus leading to a so-called pseudo-distance or pseudo-range.

Let us denote by $\delta t_{5\mathrm{G}}$ the clock offset of UE with respect to reference 5G time, the m-th BS synchronization error by $e_{\mathrm{sync},m}$ and the Time-Delay Estimation (TDE) error in meters by $e_{\mathrm{TDE},m}$. Then let $\mathbf{x} \doteq [x, y, z]^T$ be the unknown UE position and $\mathbf{x}_{\mathrm{BS,m}} = [x_{\mathrm{BS,m}}, y_{\mathrm{BS,m}}, z_{\mathrm{BS,m}}]$ is the known m-th BS position among M_{BS} available BSs, which are closer in distance with UE, relative to a reference coordinate. The ranging errors, which are added to the Euclidean BS-UE distance, are calculated here by taking into account the LoS conditions, the Signal-to-Noise Ratio (SNR) levels and a random probability variable drawn from a uniform distribution between 0 and 1 following the physical-layer abstraction of 5G observables proposed in [50]. As a result, the pseudo-range from the UE to the m-th BS is expressed with the formula:

$$\hat{\rho}_m = c \cdot \hat{\tau}_m = \parallel \mathbf{x}_{\mathrm{BS},m} - \mathbf{x} \parallel + c \cdot \delta t_{5\mathrm{G}} + e_{\mathrm{sync},m} + e_{\mathrm{TDE},m}, \tag{4.2}$$

Calculating the differences of Time of Arrival (ToA) observables eliminates δt_{5G} and yields the OTDoA measurement in the time domain. In this work, it is also assumed a perfectly synchronized network among BSs, so $e_{\mathrm{sync},m}$ is not considered. Thus, the m-th Time Difference of Arrival (TDoA) observable is computed as the time difference of ranging observables from the serving and neighbor BSs as

$$\hat{\rho}_{\mathrm{TDoA},m} = \hat{\rho}_1 - \hat{\rho}_{m+1}, \tag{4.3}$$

for $1 \leq m < M_{\mathrm{BS}} - 1$, where $\hat{\rho}_1$ is the ranging observable from the serving BS, i.e., the most powerful BS (with highest SNR) at the receiver position, $\hat{\rho}_{m+1}$ is the ranging observable from the (m + 1)-th neighbor BS and M_{BS} is the total number of BSs used for positioning. The SNR levels are considered for sorting the ascending list of BSs.

4.2.2 Position computation

Given the known location $\mathbf{x}_{\mathrm{BS},m}$ of the m-th position among M_{BS} available BSs, the unknown 3D receiver position $\mathbf{x}$ is solved based on the Weighted Least Squares (WLS) classical solution of the OTDoA positioning problem by using the well-known iterative Gauss-Newton (GN) method. The BSs used for positioning are the ones closer in distance with the UE, relative to a reference coordinate.

It is worth noting that $\hat{\rho}_m$ in (4.2) is a non-linear function of the user's position. However, it can be linearized using its Taylor series around a user's tentative position $\hat{\mathbf{x}} = [\hat{x}, \hat{y}, \hat{z}]^T$. Using the tentative position, we calculate the approximate pseudo-range $\hat{\rho}_{\mathrm{TDoA},m}$ in (4.3), for $1 \leq m < M_{\mathrm{BS}} - 1$. With $M_{\mathrm{BS}} \geq 4$ BSs, it is possible to provide a single solution. The GN solution at the l-th iteration is:

$$\hat{\mathbf{x}}_l = \hat{\mathbf{x}}_{l-1} + (\mathbf{G}^T_{\mathrm{TDoA},l-1}\mathbf{W}^{-1}_{\mathrm{TDoA}}\mathbf{G}_{\mathrm{TDoA},l-1})^{-1}\mathbf{G}^T_{\mathrm{TDoA},l-1}\mathbf{W}^{-1}_{\mathrm{TDoA}}(\boldsymbol{\rho}(\hat{\mathbf{x}}_{l-1}) - \hat{\boldsymbol{\rho}}), \tag{4.4}$$

where

$$\begin{aligned} \hat{\boldsymbol{\rho}}(\hat{\mathbf{x}}_{l-1}) &= [\hat{\rho}_1(\hat{\mathbf{x}}_{l-1}), \hat{\rho}_2(\hat{\mathbf{x}}_{l-1}), \ldots, \hat{\rho}_{M_{\mathrm{BS}-1}}(\hat{\mathbf{x}}_{l-1})]^T, \\ \rho_m(\hat{\mathbf{x}}_{l-1}) &= \| \mathbf{x}_{BS,1} - \hat{\mathbf{x}} \| - \| \mathbf{x}_{\mathrm{BS},(m+1)} - \hat{\mathbf{x}} \|, for\ 1 \leq m < M_{\mathrm{BS}-1}, \end{aligned} \tag{4.5}$$

is the vector of measured pseudo-ranges corresponding to the linearization reference position $\hat{\mathbf{x}}$,

$$\hat{\boldsymbol{\rho}} = [\rho_{\mathrm{TDoA},1}, \ldots, \rho_{\mathrm{TDoA},\mathrm{M_{BS}-1}}]^T, \tag{4.6}$$

is the vector of predicted pseudo-ranges corresponding to the real receiver position $\mathbf{x}$, $\mathbf{W}_{\mathrm{TDoA}}$ is the weighting matrix formed by the weighting coefficients of the TDoA observables as:

$$\mathbf{W}_{\mathrm{TDoA}} = \begin{bmatrix} \sigma_1^2 + \sigma_2^2 & \sigma_1^2 & \cdots & \sigma_1^2 \\ \sigma_1^2 & \sigma_1^2 + \sigma_3^2 & \cdots & \sigma_1^2 \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1^2 & \sigma_1^2 & \cdots & \sigma_1^2 + \sigma_{M_{\mathrm{BS}}}^2 \end{bmatrix} \tag{4.7}$$

where σ_m^2 is the variance of the m-th ranging errors and $\mathbf{G}_{\mathrm{TDoA}}$ is the geometry matrix defined as:

$$\mathbf{G}_{\mathrm{TDoA},(n,1:3)} = \left[\frac{\mathbf{x}_{\mathrm{BS},1} - \hat{\mathbf{x}}}{\|\mathbf{x}_{\mathrm{BS},1} - \hat{\mathbf{x}}\|} - \frac{\mathbf{x}_{\mathrm{BS},(m+1)} - \hat{\mathbf{x}}}{\|\mathbf{x}_{\mathrm{BS},(m+1)} - \hat{\mathbf{x}}\|} \right]. \tag{4.8}$$

We ensure full rank of $\mathbf{G}_{\mathrm{TDoA}}$, which guarantees the invertibility of $\mathbf{G}^T_{\mathrm{TDoA}}\mathbf{W}_{\mathrm{TDoA}}\mathbf{G}_{\mathrm{TDoA}}$.

The GN method often converges quickly, especially when the iteration begins with a reference position close enough to the true position. However, if the iteration begins far from the target position, convergence may be slow or may not be achieved at all. To avoid this problem, a tolerance level (10^{-4}m) is set to ensure that the range residual parameters (i.e. the difference between the predicted range and pseudo-range measurements) do not exceed the level set by the user. The tolerance level has been set based on Monte Carlo simulation results.

4.2.3 Computation of test statistic

The method for calculating the test statistic and its theoretical statistical distribution is presented in this subsection. The network provides a WLS estimate of the position based on TDoA measurements. This is done using the linearized measurement equation in (4.4). The estimated user position $\hat{\mathbf{x}}$ and the pseudo-range residual errors $\Delta\boldsymbol{\rho} = \rho(\hat{\mathbf{x}}_{l-1}) - \hat{\boldsymbol{\rho}}$ obtained from the WLS will later contribute in the computation of the test statistic. The vector of pseudo-range residual errors, $\Delta\boldsymbol{\rho}$, is the difference between the predicted and the measured pseudo-ranges.

Given the known location $\mathbf{x}_{BS,m}$ of the m-th position among $M_{\mathrm{BS_{TDoA}}}$, available BSs and the estimated user position in (4.4), it is possible to compute the geometry matrix $\mathbf{G}$ as defined in (4.8). The geometry matrix is decomposed into the signal matrix ($\mathbf{U}_{\mathrm{S}}$) and noise matrix ($\mathbf{U}_{\mathrm{N}}$) through QR factorization [51]. The dimension of the noise subspace is ($M_{\mathrm{BS_{TDoA}}} - 4$). In the absence of any fault, the noise subspace should only contain the noisy contribution of the WLS residuals and thus it could be modeled as a subspace of zero-mean Gaussian random vectors [52]. However, when a bias is present, the noise subspace will be distorted by the faulty bias and the noise-only condition will not be clear-cut. The QR factorization is preferable instead of performing conventional orthogonal matrix projection because it requires less computation and allows to easily distinguish the noise from the signal by visualizing the presence of any degradation. These constitute the building blocks for the detection method.

The residuals on which the detection is implemented are obtained as follows:

$$\varepsilon_i = \mathbf{U}_{\mathrm{N}_i}^T \, \Delta\boldsymbol{\rho}_i, \tag{4.9}$$

where $\mathbf{U}_{\mathrm{N}}^T$ is a $(M_{\mathrm{BS_{TDoA}}} - 4) \times (M_{\mathrm{BS_{TDoA}}} - 1)$ matrix, whose rows are mutually orthogonal. To normalize the range residuals and remove the correlation between data, the whitening process is performed. First, the covariance matrix's dimensions of the range residuals are made independent by performing principal component analysis. The covariance matrix is calculated as:

$$\mathbf{Cov}_{\mathrm{res}_i} = \mathbf{U}_{\mathrm{N}_i} \, \mathbf{Cov}_i \, \mathbf{U}_{\mathrm{N}_i}^T, \tag{4.10}$$

where $\mathbf{Cov}$ is the covariance matrix of the pseudo-range errors under the conditions of perfect synchronization error and no bias in the measurements. Then, an eigen decomposition is performed:

$$\mathbf{Cov}_{\mathrm{res}_i} = \mathbf{V}_i \, \mathbf{D}_i \, \mathbf{V}_i^T, \tag{4.11}$$

where $\mathbf{V}$ is an orthogonal rotation matrix composed of eigenvectors of $\mathbf{Cov}_{\mathrm{res}}$, and $\mathbf{D}$ is a diagonal matrix with eigenvalues on the diagonal. $\mathbf{V}^T$ gives a rotation needed to de-correlate the data. So, we have:

$$\hat{\epsilon}_i = (\mathbf{V}_i \sqrt{\mathbf{D}_i})^{-1} \epsilon_i. \tag{4.12}$$

Finally, the test statistic is formed from the Sum of Squared Residuals (SSR):

$$\mathrm{SSR_i} = \hat{\epsilon}_i^T \hat{\epsilon}_i, \tag{4.13}$$

where the i-th test statistic for $i = 1, 2, \ldots\ldots, M_{\mathrm{BS_{TDoA}}} - 1$ subsets is given by:

$$T_i = \sqrt{\mathrm{SSR_i}/(M_{\mathrm{BS_{TDoA}}} - 4)}. \tag{4.14}$$

If the measurement errors are normally distributed with zero mean, $\mathrm{SSR}_{\mathrm{i}}^2$ has χ^2 distribution with $M_{\mathrm{BS_{TDoA}}} - 4$ degrees of freedom. The distribution is modified to a non-central χ^2 with the same degree of freedom if any measurement error is biased. In this case, the distribution is affected more strongly by geometry through the noncentrality parameter. The decision variable T_i is tested against a threshold γ (see next sub-section 4.2.4). Thus, the detection is based on a hypothesis testing where:

$T_i \leq \gamma$: H_0 is accepted (no biased measurement error),

$T_i > \gamma$: H_1 is accepted (biased measurement error).

4.2.4 Selection of threshold parameter

The selection of the threshold is done experimentally based on the requirements for false alarm [51]. For a Cumulative Density Function (CDF) of test statistic values, the quantile α defines the probability of detecting bias-free BSs subsets. Denoting the threshold γ as that providing a specific probability of false alarm ($\mathrm{P_{fa}}$), the following relationship holds:

$$\mathrm{P_{fa}}(\gamma) = 1 - \alpha(\gamma) = 1 - \int_0^{\gamma} f_{\chi^2}(T)dT. \tag{4.15}$$

The pseudo-range measurements should be uncorrelated and have a unit variance to follow a desirable normalized χ^2 distribution.

4.3 Outlier detection and exclusion

This subsection formulates the autonomous outlier detection and exclusion approach. Before the outlier exclusion starts, it is assumed that the UE position was already estimated by the WLS as stated in Sect. 4.2.2, so that a reasonable starting position could be used to ensure the convergence of the GN method. The method monitors the residuals resulting from the WLS positioning solution. The fundamental concept behind the proposed technique is to check the redundancy of range measurements obtained from all available BSs in order to detect one faulty transmitter at a time [47]. The technique includes both a FD [53] and a FDE functionality (see Algorithm 1).

In conditions of synchronization error among BSs and in the presence of NLoS signals, the proposed method aims to detect large biases induced into the measurements. The workflow diagram of measurement's monitoring depicted in Figure 4.1 shows the process of its functionality as follows.

1. Calculate the pseudo-range residuals using all BSs in the scenario. Large residuals indicate that a measurement error (bias) might be present. Generally, to perform a fault detection, there must be at least one redundant observation available. Since we are working with TDoA measurements, a minimum of four BSs are needed to compute a 3D position, five BSs to detect a failure and six BSs to detect and exclude the faulty BS.

2. In order to distinguish between bias-free measurements and those subject to abnormal measurements, a measurable scalar parameter is defined to provide information about pseudo-

range measurement errors. This parameter, named test statistic, is related to pseudo-range observations, and it is calculated as the normalized root sum square of the pseudo-range measurement residuals.

3. The test statistic is then compared with a detection threshold T. If the test statistic exceeds the given threshold, a bias might be present in the measurements and the faulty BS identification is performed. Otherwise, the solution with all the BSs is used in the scenario.

4. If a failure is detected, we create subsets of BSs by setting one BS as serving for the TDoA measurements and removing one BS from the rest of BSs at a time, so that there will be $(M_{\mathrm{BS_{TDoA}}} - 1)$ subsets, each having $(M_{\mathrm{BS_{TDoA}}} - 1)$ BSs. The detection of the failure is achieved by performing a consistency check through the test statistic parameter for each of the subsets. The subset with the minimum test statistic that does not exceed the given threshold is chosen to perform the location computation.

5. If the presence of degraded measurement errors is detected, but the faulty BS cannot be identified, the set of BSs that is used for the computation is selected to be the one whose test statistic is the smallest. The candidates' BSs set (on which the test statistic is calculated) include the $(M_{\mathrm{BS_{TDoA}}} - 1)$ subsets and also the original set with all the available BS in the scenario. In any case, in such situation when the faulty BS cannot be identified, we recognize that the positioning accuracy remains degraded and does not improve as expected.

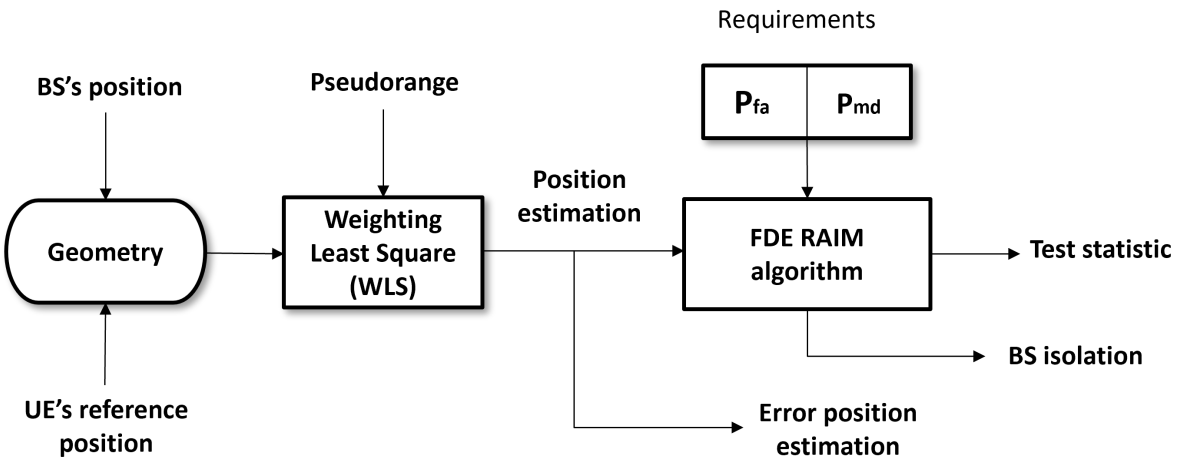


Figure 4.1: NLoS BS exclusion mechanism.

4.4 Simulation results

To check the feasibility of the method, a predefined Urban Macro (UMa) network scenario based on a deep urban deployment map is considered with seven BSs surrounded by high buildings and UE located outdoors at street level. NLoS propagation is common in urban environments, as considered in [50, 26]. Simulations are done for the use case of high-accuracy autonomous cars. The coordinates used are in ENU (East, North, Up) relative to a near reference location.

As explained in Sect. 4.3, the minimum number of BSs to perform detection and exclusion of the faulty BS is six, the reason being that we are using OTDoA, which gives one measurement

Algorithm 1 NLoS BS detection and exclusion. Procedure from 1 to 20 performs the algorithm with all the available BS, while procedure from 22 to 27 performs the algorithm excluding one BS at a time when the computed test statistic with all the available BS exceeds the given threshold

Input: $\mathbf{x}_{\mathrm{BS},m}$, $\hat{\mathbf{x}}$, **Cov**, γ, $\mathbf{W}_{\mathrm{TDoA}}$, $\hat{\boldsymbol{\rho}}$, **where** $m = 1, 2, \ldots, M_{\mathrm{BS_{TDoA}}}$
Output: $\hat{\mathbf{x}}_l$

1: Set NrIter = 10 to perform GN solution
2: $\hat{\mathbf{x}}_l = \hat{\mathbf{x}}$
3: Set $l = 0$
4: **while** $l \leq$ NrIter **do**
5: $l = l + 1$
6: Compute $\mathbf{G}_{\mathrm{TDoA},(m,1:3)} = \left[\frac{\mathbf{x}_{\mathrm{BS},1} - \hat{\mathbf{x}}_l}{\|\mathbf{x}_{\mathrm{BS},1} - \hat{\mathbf{x}}_l\|} - \frac{\mathbf{x}_{\mathrm{BS},(m+1)} - \hat{\mathbf{x}}_l}{\|\mathbf{x}_{\mathrm{BS},(m+1)} - \hat{\mathbf{x}}_l\|} \right]$
7: Compute the pseudo-range error $\boldsymbol{\rho}(\hat{\mathbf{x}}_{l-1})$.
8: Compute the UE estimated location $\hat{\mathbf{x}}_l$:
9: $\hat{\mathbf{x}}_l = \hat{\mathbf{x}}_{l-1} + (\mathbf{G}^T_{\mathrm{TDoA},l-1} \mathbf{W}^{-1}_{\mathrm{TDoA}} \mathbf{G}_{\mathrm{TDoA},l-1})^{-1} \mathbf{G}^T_{\mathrm{TDoA},l-1} \mathbf{W}^{-1}_{\mathrm{TDoA}} (\boldsymbol{\rho}(\hat{\mathbf{x}}_{l-1}) - \hat{\boldsymbol{\rho}})$
10: **end while**
11: Compute $\mathbf{G}_{\mathrm{TDoA}}$ as in 6, where $\hat{\mathbf{x}}_l$ is from 9
12: Decompose $\mathbf{G}_{\mathrm{TDoA}}$ into $\mathbf{U}_{\mathrm{S}}$ and $\mathbf{U}_{\mathrm{N}}$ through QR factorization
13: Compute the residuals $\varepsilon = \mathbf{U}^T_{\mathrm{N}} \Delta\boldsymbol{\rho}$, where $\Delta\boldsymbol{\rho} = (\boldsymbol{\rho}(\hat{\mathbf{x}}_{l-1}) - \hat{\boldsymbol{\rho}})$ from 9
14: Compute the covariance matrix of the range residual vector $\mathbf{Cov}_{\mathrm{res}} = \mathbf{U}_{\mathrm{N}}\, \mathbf{Cov}\, \mathbf{U}^T_{\mathrm{N}}$
15: Perform eigen decomposition of $\mathbf{Cov}_{\mathrm{res}} = \mathbf{V}\, \mathbf{D}\, \mathbf{V}^T$
16: Whiten the range residual vector as $\hat{\epsilon} = (\mathbf{V}\sqrt{\mathbf{D}})^{-1}\epsilon$
17: Compute the sum of squared residuals: SSR $= \hat{\epsilon}^T \hat{\epsilon}$
18: Compute $T = \sqrt{\mathrm{SSR}/(M_{\mathrm{BS_{TDoA}}} - 4)}$
19: **if** $T \leq \gamma$ **then**
20: Use the solution $\hat{\mathbf{x}}_l$ in 9
21: **else**
22: A bias might be present
23: Create subsets of BS by setting the 1st BS as serving and remove one BS from the rest of BS at a time, $\{\mathbf{x}_{\mathrm{BS},m'}\}_i$, where $i \in \{1, 2, \ldots, M_{\mathrm{BS_{TDoA}}} - 1\}$ and $m' \in m - \{i + 1\}$
24: For each of the subsets compute T_i following the procedure from 1 to 18
25: Choose $\{\mathbf{x}_{\mathrm{BS},m'}\}_i$ with minimum T_i that does not exceeds γ
26: **if** T_i found **then**
27: Use solution $\hat{\mathbf{x}}_l$ computed by the corresponding $\{\mathbf{x}_{\mathrm{BS},m'}\}_i$
28: **else**
29: Choose the minimum T_i among test statistics computed in 18 and 24
30: Use solution $\hat{\mathbf{x}}_l$ computed by the corresponding group of BSs
31: **end if**
32: **end if**

less than the conventional ToA usually used in RAIM. The FDE is performed at any subset of $(M_{\mathrm{BS}} - 1)$ BSs. The subsets are created by keeping the first BS as reference for OTDoA measurements and by removing one BS at a time from the rest of serving BSs. Since the accuracy of the estimated position depends upon the BS and UE geometry [54], we ensure that the geometry of our scenario has a Horizontal Dilution of Precision (HDOP) smaller than 2. As we are dealing with a terrestrial deployment with BSs at similar heights, vertical accuracy tends to be rather poor, however, we are only interested in the horizontal positioning.

The simulation is done based on the UMa channel model defined in [26]. The distance between BS and UE is used to determine the propagation conditions based on distance-dependent LoS probability and path loss models tabulated in [26]. These conditions are compared in

terms of LoS/NLoS conditions and SNR levels (limited between −30dB and 30dB) for an UMa environment. The ranging observables are calculated for specific propagation conditions, channel model, system Bandwidth (BW), SNR levels, and time-delay estimator.

A 5G PRS signal with a BW of 20 MHz and 100 MHz at a carrier frequency of 2 GHz, within the cmWave Frequency Range 1 (FR1) of 5G New Radio (NR) has been considered. For simplicity, the network is supposed to be perfectly synchronized among BSs. The TDE error is obtained as the time-delay measurement of the first correlation peak above a threshold through the threshold-based estimator presented in [50]. The UE is initially in "cold start" and has no previous information about its position. Firstly, the position is estimated assuming ideal conditions (LoS scenario and no multipath) and trilaterating the distances between all BS. Then the Least Squares (LS) positioning method is run with 300 Monte Carlo iterations for each UE position.

To check the capability of the method to identify the anomalous measurements, a bias ranging from 5 to 100 meters is added to the ranging error of the second BS of our scenario in the Monte Carlo simulations. The probability of false alarm is set to $P_{\text{fa}} = 0.2$, resulting in a threshold of $\gamma = 1$ m calculated as explained in Sect. 4.15. The presence of a fault measurement (faulty bias) is distinguished between bias-free measurements through the test statistic, a parameter that gives information about pseudo-range measurement errors. After the ith test statistic T_i is computed for each subset of BSs, it is compared against the given threshold. If the test statistic exceeds the given threshold value, a bias might be present. In the subset where the test statistic is smaller than the given threshold, the missing BS is assumed to be faulty and hence excluded. Thus, the estimate of the user's position is performed without this BS. In the figures presented herein, the CDFs of T_i of each subset are given, where the part of the curve with the colored area underneath gives the T_i that is smaller than the given threshold.

4.4.1 Results when BW=20 MHz

Fig. 4.2 and Fig. 4.3 present the CDFs of each T_i, where a bias of 5 m and 30 m respectively is added to the measurements. We have shown these two cases because the first one represents the lower limit of the bias considered in this work, and the second one represents a bias for which a significant improvement of positioning accuracy starts to be noticed. According to the results, with a 30 m bias, the subset with the second BS missing shows that 81% of the test statistic calculated for each Monte Carlo iteration is smaller than the given threshold. This is a significantly high percentage compared to the other subsets, where the test statistic exceeds the given threshold. The achieved results allow us to deduce that the second BS is the faulty one. However, since the differential pseudo-range measurements are slowly varying, is not always easy to apply a fixed threshold to the test statistic. This is noticed with small biases when the resulting error is more difficult to detect. For instance, in the case of 5 m bias depicted in Fig. 4.3 the presence of the bias becomes less easy to be detected than before. In each subset there is a percentage where the calculated test statistic is smaller than the given threshold. Also, the use of a small bandwidth affects the accuracy of OTDoA measurements and the ability of LS algorithm itself to dissolve or minimize the error and therefore can affect the performance of RAIM.

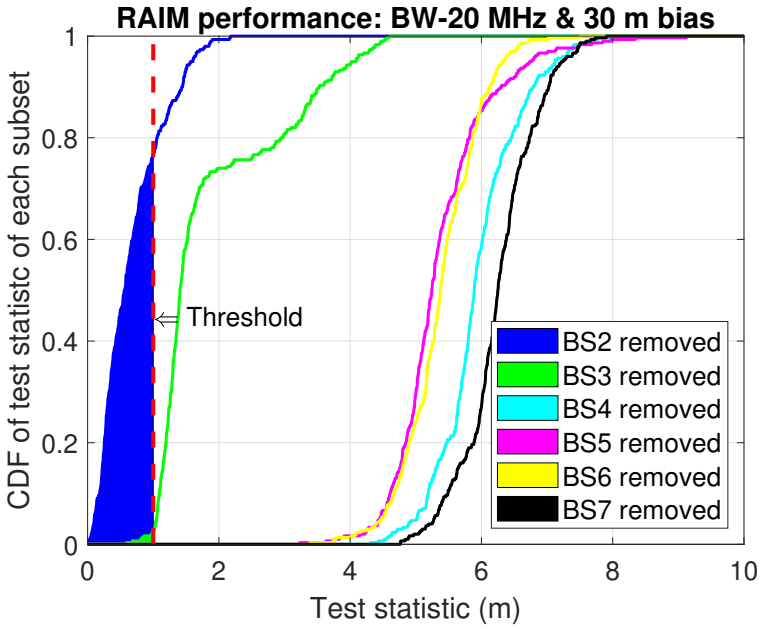


Figure 4.2: CDF of the NLoS test T for BW=20 MHz with an 30 m bias.

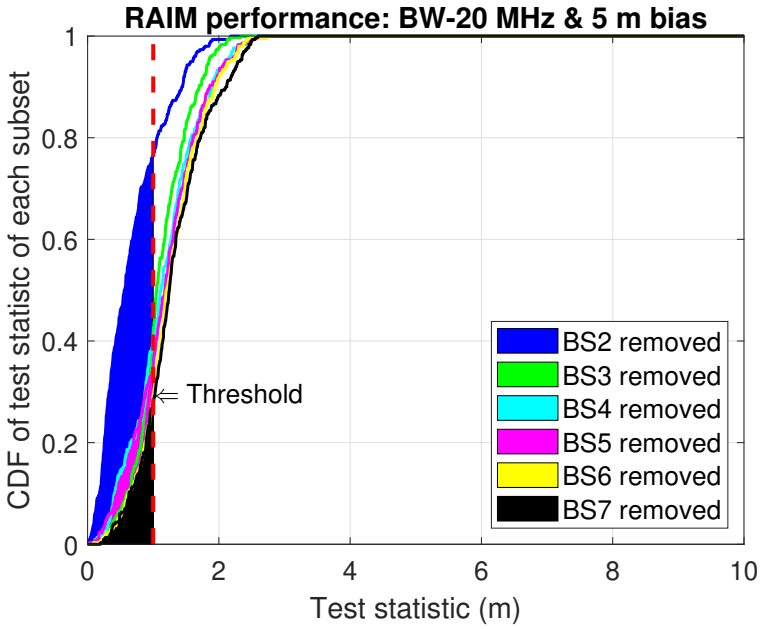


Figure 4.3: CDF of the NLoS test T for BW=20 MHz with an 5 m bias.

4.4.2 Results when BW=100 MHz

Results in Fig. 4.4 show that the second BS is the faulty one because removing it makes 80% of the calculated test statistics smaller than the given threshold, while its presence makes that all test statistics exceed the given threshold. Despite having similar results with the previous scenario, the use of a bigger bandwidth makes the detection of bias easier for the case in Fig. 4.5 and therefore the monitoring integrity method is more reliable.

Apart from observing the statistical performance of the proposed NLoS test, it is important to assess the actual gain we obtain in terms of the UE positioning performance. Fig. 4.6 and Fig. 4.7 present the UE horizontal position errors for the cases when the NLoS detection method

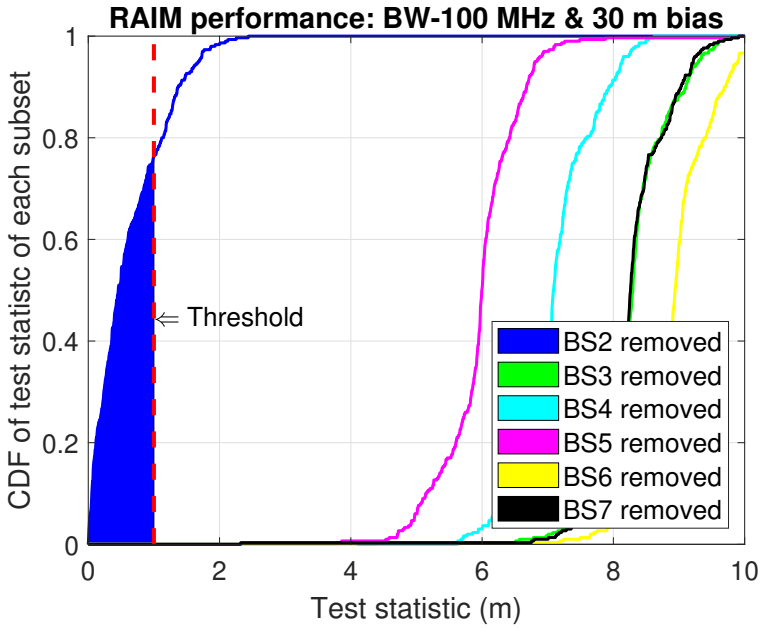


Figure 4.4: CDF of the NLoS test T of BW=100 MHz with an 30 m bias.

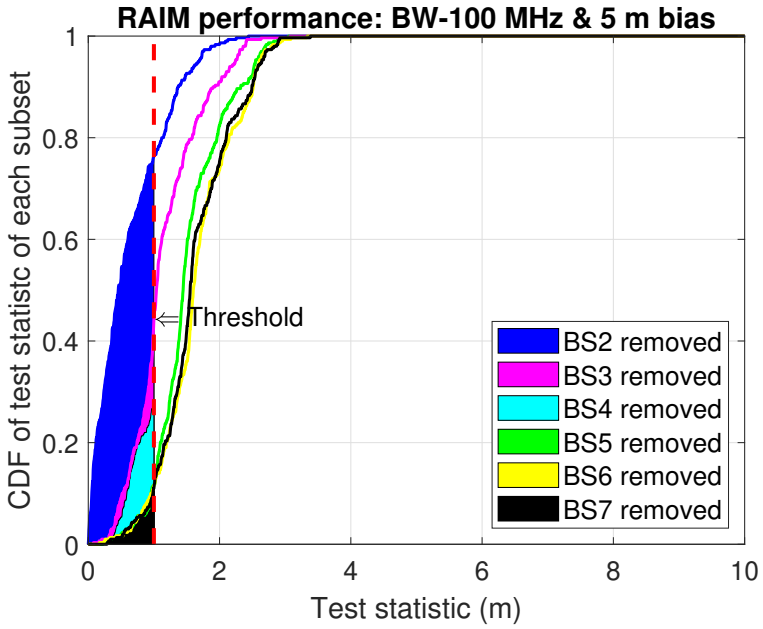


Figure 4.5: CDF of the NLoS test T for BW=100 MHz with an 5 m bias.

is used and when it is not. In conditions of perfect network synchronization, with the use of wide bandwidth, we expect optimistic results that meet the performance target, where the OTDoA horizontal positioning error is smaller than 10 m for 80% of UEs in outdoor deployments scenarios. However, a significant degradation of the OTDoA accuracy is noticed when the NLoS exclusion method is not used, even for the case of maximum bandwidth. In both figures (Fig. 4.6 and Fig. 4.7), it can be seen that the probability of having a position error smaller than 10 m is significantly higher when the method is used. On the other hand, in the case of small bias, is not always possible to detect the faulty BS. We believe this happens because it is more difficult to discern the wrong measurement when the error is more precise.

General observations on the simulation results have shown that the proposed method is

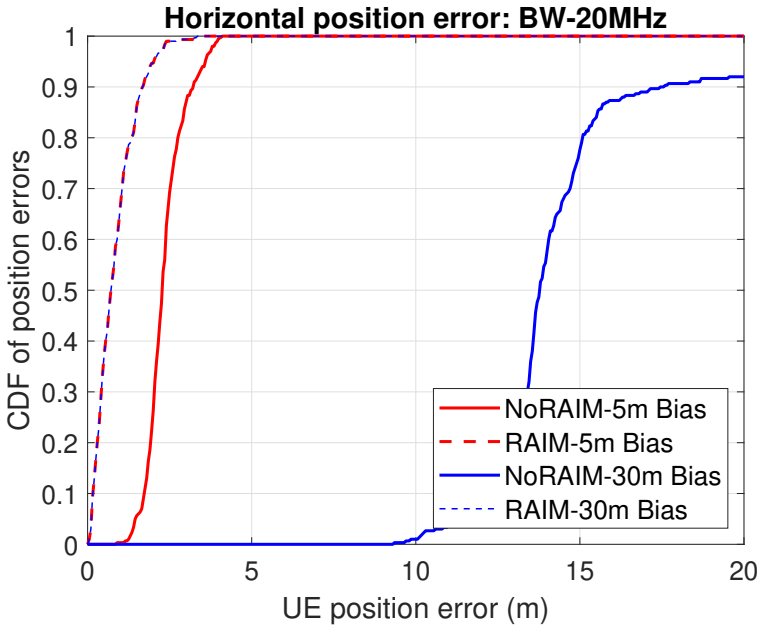


Figure 4.6: UE error positions when using RAIM or not.

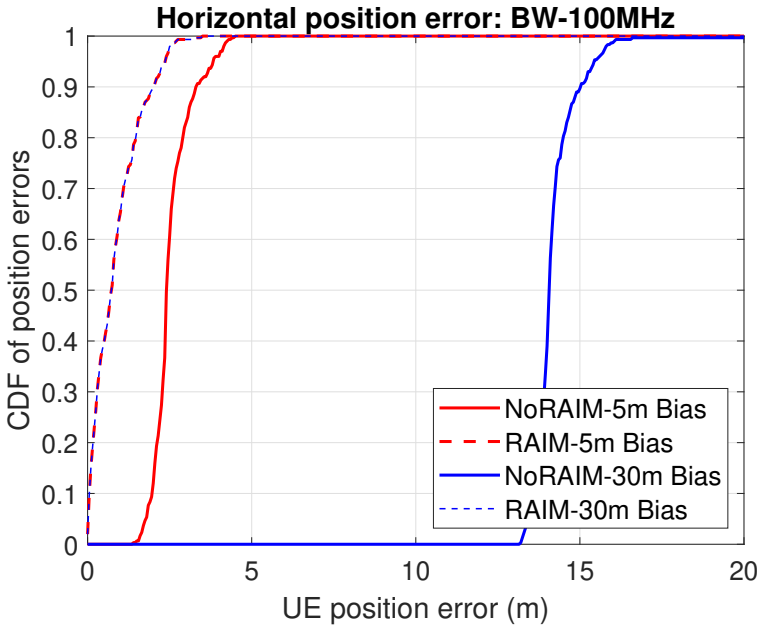


Figure 4.7: UE error positions when using RAIM or not.

able to detect a bias as low as 2 m and hence exclude the faulty BS. Moreover, the maximum horizontal position error is reduced by 55.6% on average.

4.5 Conclusion

In conclusion, this chapter has proposed a solution to address the challenge of maintaining position integrity in cellular network positioning systems, with a specific focus on urban scenarios characterized by signal propagation obstacles. Our approach, centered around excluding base stations affected by NLoS conditions, has demonstrated notable advantages.

By analyzing LS residuals during the positioning process, our proposed algorithm has shown promising results. Simulations conducted within an urban channel model featuring seven visible base stations have validated the efficacy of our approach, emphasizing the practical utility of incorporating such mechanisms to evaluate 5G positioning performance in realistic scenarios.

Moreover, we have provided a brief overview of the fundamental principles of integrity considerations within urban contexts. To ensure the desired level of integrity, two pivotal requirements must be fulfilled: the existence of a position solution with an associated PL, depending upon a sufficient number of measurements, and an appropriately sized PL that aligns with application specifications.

In the context of urban integrity monitoring, encountering a balance between PL size and the targeted integrity level remains a persistent challenge. Given the context-dependent nature of integrity requisites, the development of tailored algorithms and specifications for different urban applications becomes imperative.

To sum up, this chapter emphasizes the importance of our proposed solution in improving the accuracy of position integrity. This is particularly relevant when we deal with the complexities of positioning within urban cellular network systems. The potential benefit of achieving a high level of accuracy and provide a reliable location solution in all environments is very promising for 5G networks. 5G will be able to locate UE with sub-meter accuracy and provide high network utility, such as seamless coverage, low delay, and high throughput, placing higher requirements for cellular communication systems.

This motivation has led us to propose a hybrid algorithm to access their positioning capabilities over outdoor scenarios, especially in harsh environments like urban areas with tall buildings (urban canyons). So, in the next chapter, we will present this hybrid algorithm where we will emphasize how powerful cellular systems are on their own, ensuring precise positioning even in challenging situations. This means they are not seen just as an addition in order to complement the availability of GNSS in such environment, but also as a standalone technology capable of delivering accurate results.

Chapter 5

Joint TDoA and AoA localization in deep urban deployment

Up until this point, we have discussed the most relevant cellular positioning technologies, examined their potential to enhance location estimation accuracy, and highlighted the advancements introduced by 5G networks in Chapter 1. The requirement for accurate and reliable localization is expanding rapidly, particularly in the context of autonomous and unmanned vehicles, as noted in [55]. With the rapid increase of such applications in urban environments, the necessity for centimeter-level positioning accuracy has become critical.

However, in Chapter 4 it was stated that, unfortunately, in 5G urban communications, the dominance of Non Line of Sight (NLoS) conditions, coupled with network synchronization errors, confines achievable positioning capabilities predominantly due to obstruction. Therefore, in this chapter, we want to demonstrate the use of the method proposed in Chapter 4 and its impact in improving position accuracy. Because the positioning accuracy deteriorates significantly in challenging environments such as urban canyons due to signal multipath and blockage, a deep urban environment with narrow streets and tall buildings, typical of big cities, is considered. It consists in a realistic deep urban scenario in the presence of NLoS with a tight network synchronization, using the uplink signals of 5G New Radio (NR) operating within the cmWave band. Each User Equipment (UE) position is used to further decompose urban Base Station (BS) positions into Urban Macro (UMa) and Urban Micro (UMi) cellular deployments, where the deployment ratios will define the network densities.

The main objective of this part of the work is to assess the achievable positioning performance of a hybrid Uplink Time Difference of Arrival (UTDoA) and Angle of Arrival (AoA) approach, leveraging advanced antenna arrays. This technology helps to characterize the effects of 5G cmWave observables, described in Section 5.1, in 5G positioning and adds value to the use of advanced antennas in a relevant application, namely positioning. Furthermore, we want to demonstrate that incorporating the identification and exclusion of ranging observations affected by NLoS, described in Chapter 4, in the positioning computation (see Section 5.2) yields accuracy improvements. The proposed methodology finds applicability in outdoor scenarios, such as the one presented in Section 5.3, with stringent high-accuracy positioning requisites. Consequently, this approach lays the foundation for meeting demanding positioning criteria in challenging environments through the utilization of cellular networks. The discussions of findings in this

chapter are concluded in Section 5.4.

5.1 Characterization of the observables

This section outlines the procedure for characterizing observables associated with each positioning method utilized in this phase of the study. All the process has been explained in Chapter 2 and here is it summarized in the context of the proposed work in this chapter. We will consider a non-zero probability of 5G system fault, leveraging regularly transmitted Downlink (DL) and Uplink (UL) pilot signals for both channel estimation and positioning purposes.

5.1.1 Observable based on time of arrival

One of the main sources of ranging error in cellular networks is due to the presence of NLoS. Therefore, our characterization of the observable is based only on the NLoS-induced error. The ranging errors are computed for specific propagation conditions, channel models, system bandwidth, Signal-to-Noise Ratio (SNR) levels, and time-delay estimator. The Line of Sight (LoS) conditions are computed according to the distance between the receiver and BS and a random probability variable drawn from a uniform distribution between 0 and 1 following the physical-layer abstraction of 5G observables proposed in [25]. The channel models are based on the ones provided in [26]. Since this work is focused on cmWave scenarios, UMa and UMi scenarios of the 3rd Generation Partnership Project (3GPP) standard models are considered. Its network operates at frequency bands between 900 MHz and 6 GHz, and the system bandwidth is limited up to 100 MHz. The time-delay estimator computes the maximum peak of the correlation between the received signal and the transmitted positioning pilots within a correlation range. The ranging errors are finally added with the Euclidean distance between the user terminal and the BS to model the Time of Arrival (ToA) observables computed together with the Time Difference of Arrival (TDoA) estimates as explained in 4.2.1. The TDoA estimates are computed with downlink and uplink 5G signals, resulting in the Observed Time Difference of Arrival (OTDoA) and UTDoA location methods, respectively. Since the physical propagation channel is the same for both OTDoA and UTDoA methods, the main performance difference between both methods is due to inter-UE interference. For the downlink positioning, the UE is in charge of measuring the time delays on the reference or pilot signals it receives from serving and neighboring BSs, which actually provide the Euclidean distance between UE and BS. For the case of uplink positioning, the only task on the UE side is to generate and transmit the Sounding Reference Signal (SRS), which needs less computational effort than calculating a time estimation. This means that, in comparison with the downlink part, where the reference signal is generated by the network and the time estimation is done by the UE, the computational effort on the UE is reduced. Both received signals are simulated to estimate the respective ranging errors for different SNR levels. The calculation of SNR differs in the power, gain and noise figure of antennas.

On the other hand, Round Trip Time (RTT) is based on the time-delay estimates on the signals transmitted in the downlink and uplink. The computation process of RTT observables is slightly different from TDoA case. The m-th 5G RTT observable is formulated as

$$\hat{\rho}_{\mathrm{RTT},m} = c \cdot \hat{\tau}_{\mathrm{RTT},m} = \| \mathbf{x}_{\mathrm{BS},m} - \mathbf{x} \| + e_{\mathrm{RTT},m}. \tag{5.1}$$

The position error with RTT follows approximately the same relation with the DL and UL position error as the corresponding observables do. Moreover, if the noise in UL is bigger than the noise in DL, then the position error with UTDoA should be worse than the position error with the OTDoA. Thanks to the two-way transmission between receiver and transmitter, there is no UE clock offset present in the RTT observables, which relaxes the positioning problem. For a detailed explanation of the computation process refer to Section 2.3.3.1 in Chapter 2.

5.1.2 Observable based on angle of arrival

The computation process of ranging observables presented in Section 5.1.1 (in terms of physical-layer abstraction) can also be extrapolated to other observables, e.g., angle observable. The computational complexity of the characterization process also scales with the degrees of freedom. For instance, the calculation of angle observables requires an additional dimension for the antenna array orientation with respect to the transmitter, leading to a four-dimensional (4D) interpolator in terms of angle error, antenna array orientation, SNR and propagation probability. In this work, the angular estimation is based on analytical models. Since NLoS measurements are expected to not improve the localization accuracy, this method focuses only on LoS measurements. The Cramér-Rao Bound (CRB) for AoA is used to assess the positioning capabilities in Additive White Gaussian Noise (AWGN) channel, presenting a feasible estimator. The CRB is a well-known lower bound that describes the maximum achievable accuracy of any unbiased estimator in the moderate- to high-SNR region. According to the 5G specifications, the uplink positioning procedure defined in AoA uses the angle of arrival from multiple-array base stations to compute the user position. A Uniform Plannar Array (UPA) antenna with M antenna elements in the x-direction and N antenna elements in the y-direction, depicted in Figure 2.14, is used to estimate AoA (composed of the azimuth and elevation angles). This antenna array is used in all thesis, where UPA is applicable. The distance between adjacent antenna elements is assigned to be $d = \lambda/2$, where $\lambda = c/f_c$ is the received signal wavelength, c is the speed of light and f_c is the carrier frequency.

Sectorized antennas were used, and the orientation of the BS array was chosen so that the array's normal vector points approximately in the direction of the target. From Figure 2.14, one can distinguish the azimuth angle ϕ, which is the angle between the x-axis and the orthogonal projection of the vector onto the xy-plane, and the elevation angle θ, which is the angle between the vector and its orthogonal projection onto the xy-plane. The boresight direction of the array is aligned with the positive z-axis. Knowing the array sectors of each BS sectorized antenna, it is possible to calculate the array direction of BS to UE, which is the angle of incidence at which the signal travels from the UE to the BS. The angle observable computation process is explained in details in Section 2.3.3.2 of Chapter 2.

The n-th 5G AoA observables of elevation and azimuth are computed using the following formulas, respectively:

$$\theta_{obs,m} = \angle \mathrm{A}_{\theta_m} + \sigma_{\theta_m} \cdot \alpha, \quad \alpha \sim N(\mu, \sigma^2), \tag{5.2}$$

$$\phi_{obs,m} = \angle \mathrm{A}_{\phi_m} + \sigma_{\phi_m} \cdot \beta, \quad \beta \sim N(\mu, \sigma^2), \tag{5.3}$$

where σ_{θ_m} and σ_{ϕ_m} are the angle errors calculated in (2.34) and (2.33), $\angle \mathrm{A}_{\theta_m}$ and $\angle \mathrm{A}_{\phi_m}$ are the azimuth and elevation angles calculated in (2.31) and (2.32), respectively. Note that

increasing the number of antenna elements reduces the angle errors.

5.2 Position solution and measurement exclusion

This section describes the positioning algorithms considered for observables of time of arrival (i.e., UTDoA and RTT), one of the AoA and the joint UTDoA-AoA. The position computation of the receiver using UTDoA is done with and without the use of NLoS BS exclusion mechanism (explained in 4.3). The unknown parameter for all cases is the 3D receiver position. These solutions consider both downlink and uplink positioning approaches. Both derivations are applicable in the same way to the location approach.

5.2.1 Location solution based on Time of Arrival

The location solution for the case of OTDoA and UTDoA has been carried out in 4.7. The computation position approach applies to RTT positioning solution as well, with some minor changes. Using (4.4),

$$\hat{\boldsymbol{\rho}}(\hat{\mathbf{x}}_{l-1}) = [\hat{\rho}_1(\hat{\mathbf{x}}_{l-1}), \hat{\rho}_2(\hat{\mathbf{x}}_{l-1}), \ldots, \hat{\rho}_{M_{\mathrm{BS}}}(\hat{\mathbf{x}}_{l-1})]^T \tag{5.4}$$

is the vector of measured pseudo-ranges corresponding to the linearization reference position $\hat{\mathbf{x}}$,

$$\begin{aligned} \rho_n(\hat{\mathbf{x}}_{l-1}) = &\parallel \mathbf{x}_{\mathrm{BS},m} - \hat{\mathbf{x}} \parallel, for\ 1 \leq m < M_{\mathrm{BS}}, \\ &\hat{\boldsymbol{\rho}} = [\rho_{\mathrm{RTT},1}, \cdots, \rho_{\mathrm{RTT},M_{\mathrm{BS}}}]^T, \end{aligned} \tag{5.5}$$

is the vector of predicted pseudo-ranges corresponding to the real receiver position $\mathbf{x}$, $\mathbf{W}_{\mathrm{RTT}}$ is the weighting matrix formed by the weighting coefficients of the RTT observables as:

$$\mathbf{W}_{\mathrm{RTT}} = \begin{bmatrix} \sigma_1^2 & 0 & \cdots & 0 \\ 0 & \sigma_2^2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \sigma_{M_{\mathrm{BS}}}^2 \end{bmatrix} \tag{5.6}$$

with σ_m^2 being the variance of the m-th ranging errors and $\mathbf{G}_{\mathrm{RTT}}$ is the geometry matrix defined as:

$$\mathbf{G}_{\mathrm{RTT},(m,1:3)} = \left[\frac{\mathbf{x}_{\mathrm{BS},m} - \hat{\mathbf{x}}}{\|\mathbf{x}_{\mathrm{BS},m} - \hat{\mathbf{x}}\|} \right], for\ 1 \leq m < M_{\mathrm{BS}}. \tag{5.7}$$

5.2.2 Location solution based on Angle of Arrival

For the case of AoA, the GN solution at the l-th iteration is defined as:

$$\hat{\mathbf{x}}_l = \hat{\mathbf{x}}_{l-1} + (\mathbf{G}_{\mathrm{AoA},(l-1)}^T \mathbf{W}_{\mathrm{AoA}}^{-1} \mathbf{G}_{\mathrm{AoA},(l-1)})^{-1} \mathbf{G}_{\mathrm{AoA},(l-1)}^T \mathbf{W}_{\mathrm{AoA}}^{-1} \boldsymbol{b}, \tag{5.8}$$

where $\mathbf{G}_{\mathrm{AoA}}$ is the geometry matrix defined as:

$$\mathbf{G}_{\mathrm{AoA},(2m,1:3)} = \begin{bmatrix} \frac{\partial \phi_m}{\partial x} & \frac{\partial \phi_n}{\partial y} & \frac{\partial \phi_m}{\partial z} \\ \frac{\partial \theta_m}{\partial x} & \frac{\partial \theta_m}{\partial y} & \frac{\partial \theta_m}{\partial z} \end{bmatrix}, \tag{5.9}$$

composed by the partial derivatives of the azimuth and elevation angles as a function of UE-BS vector's position coordinates $\mathbf{P}'_m$ calculated in (2.29). The partial derivatives of both azimuth and elevation angles are derived from the expressions in (2.31) and (2.32), respectively. Moreover, $\mathbf{W}_{\text{AoA}}$ is the weighting matrix defined as:

$$\mathbf{W}_{\text{AoA}} = diag(\sigma_{\phi_{m,CRB}}, \sigma_{\theta_{m,CRB}}), \tag{5.10}$$

and $\mathbf{b}$ is the vector of residuals:

$$\mathbf{b} = \left[\mathbf{b}_{\phi_m};\, \mathbf{b}_{\theta_m}\right], \tag{5.11}$$

being the difference between angle estimation and AoA observables computed in Section 2.3.3.1. The residuals are wrapped in radians to $\left[-\pi\ \pi\right]$.

5.2.3 Location solution based on joint UTDoA-AoA

The location solution derived in (4.4) can also be used for the hybrid approach, where the total number of BSs used for the hybrid positioning is the sum of the number of the strongest BSs of the TDoA position based-method and those in LoS condition for the angle position based method, i.e., $M'_{\text{BS}} = M_{\text{BS}_{\text{TDoA}}} + M_{\text{BS}_{\text{AoA}}}$. The WLS classical solution of this trilateration problem is similar to the one in (4.4) and (5.8), where the geometry matrix $\mathbf{G}_{\text{Hyb}}$ is a $M'_{\text{BS}} \times 3$ matrix defined for $1 \leq m \leq M_{BS_{TDoA}}$ as:

$$\mathbf{G}_{\text{Hyb},(m,1:3)} = \left[\frac{\mathbf{x}_{\text{BS},1} - \hat{\mathbf{x}}}{\|\mathbf{x}_{\text{BS},1} - \hat{\mathbf{x}}\|} - \frac{\mathbf{x}_{\text{BS},(m+1)} - \hat{\mathbf{x}}}{\|\mathbf{x}_{\text{BS},(m+1)} - \hat{\mathbf{x}}\|}\right]. \tag{5.12}$$

and defined for $M_{\text{BS}_{\text{TDoA}}} + 1 \leq m \leq M_{\text{BS}_{\text{TDoA}}}$ as:

$$\mathbf{G}_{\text{Hyb},(m,1:3)} = \begin{bmatrix} \frac{\partial \phi_m}{\partial x} & \frac{\partial \phi_m}{\partial y} & \frac{\partial \phi_m}{\partial z} \\ \frac{\partial \theta_m}{\partial x} & \frac{\partial \theta_m}{\partial y} & \frac{\partial \theta_m}{\partial z} \end{bmatrix}, \tag{5.13}$$

and $\mathbf{W}_{\text{Hyb}}$ is the weighting matrix defined as:

$$\mathbf{W}_{\text{Hyb}} = blkdiag(\mathbf{W}_{\text{TDoA}}, \mathbf{W}_{\text{AoA}}), \tag{5.14}$$

$\mathbf{W}_{\text{TDoA}}$, $\mathbf{W}_{\text{AoA}}$ being the matrix of UTDoA and AoA weighting coefficients, respectively, computed in (4.7) and (5.10).

5.3 Simulation results and evaluation

In this section, the evaluation of the localization improvements of the proposed positioning methods is performed. For downlink transmission, a dedicated Positioning Reference Signal (PRS) is employed. This signal relies on a multi-carrier waveform, specifically defined as an Orthogonal Frequency Division Multiplexing (OFDM) scheme. Simulation involves convolving a single OFDM PRS symbol to simulate the received signal. The generation of PRS involves two key steps: generating PRS sequences based on Gold sequences and PRS mapping. These PRS sequences undergo Quadrature Phase Shift Keying (QPSK) modulation. In contrast, for uplink transmission, no dedicated signal is allocated for positioning. Instead, the SRS is chosen for this purpose. Generating the SRS involves two sequential steps: generating the Zadoff-

Chu sequence and its subsequent mapping. Signal mapping is carried out with an interleaving factor of two subcarriers (FR = 2). The UE transmits the SRS for uplink channel sounding, encompassing frequency domain channel estimation and synchronization. The SRS, essentially an uplink OFDM signal, incorporates a Zadoff–Chu sequence across distinct subcarriers. It is transmitted as OFDM symbols, allocated at specific frequency (subcarrier) and time (slot) positions within 5G NR subframes. It is important to note that both the PRS and SRS signals follow the specifications outlined in the 5G standard, as detailed in TS 38.211 [24]. For more comprehensive insights into the process, please refer to Chapter 2.

5.3.1 Scenario definition

The scenario considered in this work is based on the simulation methodology for outdoor environments within the 5G positioning study in 3GPP Release 16 [43]. It is a predefined UMa and UMi network scenario based on a deep urban deployment map with BSs deployed above the building rooftops, i.e., BS heights between 20 and 40 m. The deployment consists of a hexagonal grid with seven macro sites, where each has three sectors with an Inter-Site Distance (ISD) of around 1732 m in rural areas, 500 m and 200 m in dense urban areas. The method was tested through simulations based on a deep urban deployment map, which comes with an experimental data file of the user's position. The UEs are randomly placed within the coverage area of the predefined deployment scenario. For reference, see Figure 5.1. The deep urban area is widely characterized with 75% of the positions, while the low-density scenario is only shown in 25% of the positions. The distance between the BS and UE is used to determine the propagation conditions based on the distance-dependent LoS probability and path-loss models. The multipath channel is stochastically generated following the tabulated channel parameters in 3GPP standard [18]. For each receiver position, the positioning performance is evaluated over 96 iterations of Monte Carlo. The ranging observables are calculated for specific propagation conditions, channel model, system Bandwidth (BW), SNR levels and time-delay estimator, and the angle observables are calculated with mathematical models for specific system BW, SNR levels and antenna elements. For the 5G PRS and SRS signal, a BW of 20 MHz and 50 MHz at a carrier frequency of 4 GHz, within the cmWave Frequency Range 1 (FR1) of 5G NR and antenna arrays of M = N = 11 elements have been considered. The orientation of the BS arrays is set to three typical sectors $(0°, 120°, 240°)$. The network is supposed to have a synchronization error among BSs. Table 5.1 summarizes the simulation parameters used in this work.

5.3.2 Performance results

To evaluate the 5G positioning performance in dense urban areas, two scenarios have been considered, as mentioned above. Scenario 1 considers a narrow BW of 20 MHz and scenario 2 considers a wide BW of 50 MHz, both at a carrier frequency of 4 GHz with -50 ns or 50 ns Root-Mean-Square Error (RMSE) for the network synchronization, distributed randomly every four BS among all available BSs for positioning. Each UE considers a maximum of six BSs to calculate the position. For each of the scenarios, the impact of the angle accuracy of the additional AoA observables and the use of NLoS monitoring method has been analyzed.

The positioning performance is first assessed from a geometric perspective. The additional use of AoA observables with the TDoA observables improves the geometry. This is typically

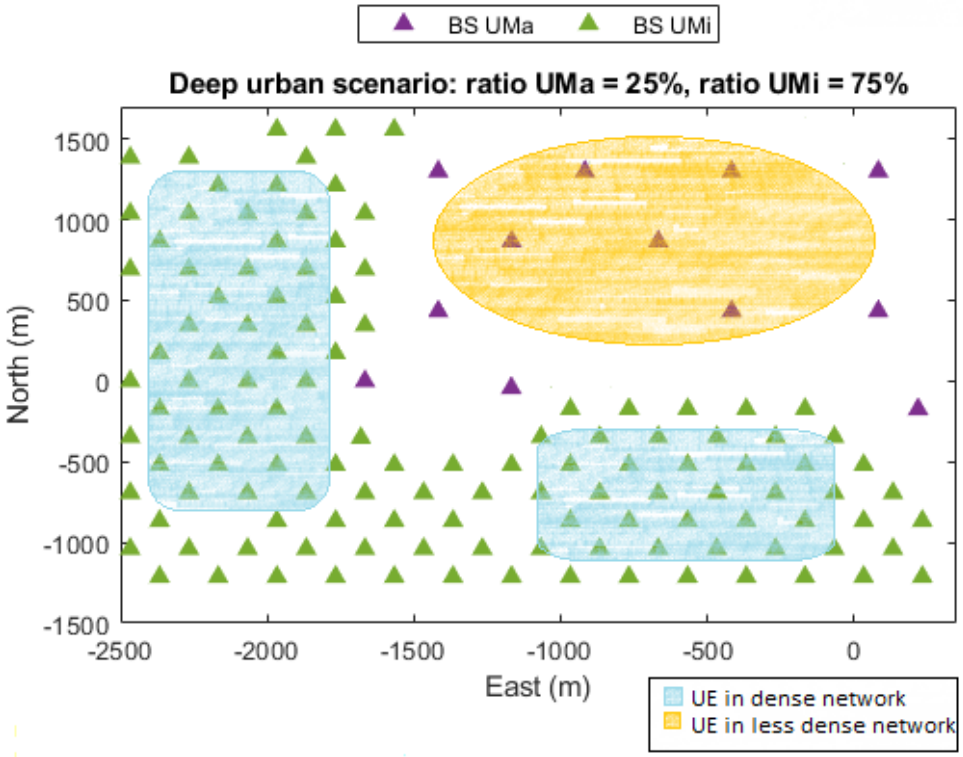


Figure 5.1: Simulation scenario

Table 5.1: Simulation parameters.

Parameter	**Scenario 1 FR1, 20 MHz**	**Scenario 2 FR1, 50 MHz**
Channel model	Baseline Channel Model based on common assumptions defined related to the channel models of 3GPP TR 38.901	
Carrier frequency	4 GHz	
System Bandwidth	20 MHz	50 MHz
Reference Signal	1-symbol PRS, SRS	
Number of subcarrier	1200	3300
Number of sites	7 (3-sector each)	
Antenna elements	M = N = 11	
Network synchronization assumptions	Perfect sync. and realistic Sync. with T1 = 50 nsec	
Applied positioning algorithm	UTDoA, AoA, RTT joint UTDoA-AoA, joint UTDoA+FDE-AoA, Gauss–Newton algorithm	

assessed with the Geometric Dilution of Precision (GDOP). Since we are dealing with terrestrial deployment, we are only interested in the horizontal positioning and therefore in the Horizontal Dilution of Precision (HDOP). This parameter for the joint TDoA-AoA is calculated following the derivations in [36], defined as:

$$\text{HDOP} = \sqrt{\mathbf{P}_{1,1}^{-1} + \mathbf{P}_{2,2}^{-1}}, \tag{5.15}$$

where

$$\mathbf{P} = k_\phi^2 \mathbf{G}_\phi^T \mathbf{G}_\phi + k_\theta^2 \mathbf{G}_\theta^T \mathbf{G}_\theta + \mathbf{G}_{\text{TDoA}}^T \mathbf{G}_{\text{TDoA}}, \tag{5.16}$$

with $\mathbf{G}_\phi$, $\mathbf{G}_\theta$ and $\mathbf{G}_{\text{TDoA}}$ being the geometry matrix of elevation angles, azimuth angles and time delays, respectively, computed as in (5.9) and (4.8), k_ϕ and k_θ representing the relationship between the variance of time delays and the variance of angles (elevation and azimuth, respectively), defined as in 2.47.

These coefficients serve to make the HDOP of AoA dimensionless and comparable to the HDOP of the TDoA. The HDOP value for the angle part can be obtained by extracting the first two terms of the sum in (5.16) and then using the result in (5.15). The same method also works for the calculation of HDOP for the time delay part separately. In this case, only the third term of the sum in (5.16) is needed. Smaller values of HDOP are preferred, meaning that small changes in the measurement will not result in large errors in the location output.

The Cumulative Density Function (CDF) of the HDOP is shown in Figure 5.2 for UTDoA, AoA and the hybrid solution. The HDOP values below 2 are expected to provide precise position estimation. For the cases when AoA and TDoA are treated as a stand-alone positioning method, the HDOP value is independent of the values of σ_{TDoA}, σ_ϕ and σ_θ. In the hybrid approach, their ratio, defined in (2.47), is a factor that affects the HDOP values. When the values of k_ϕ and k_θ are very small, the HDOP tends to be equal to the one of TDoA and vice versa. For the case of AoA, the HDOP values are also associated with the size of the deployment area of the positioning system. This is reflected in the small values of the HDOP of AoA, meaning that the BSs are deployed closer in distance.

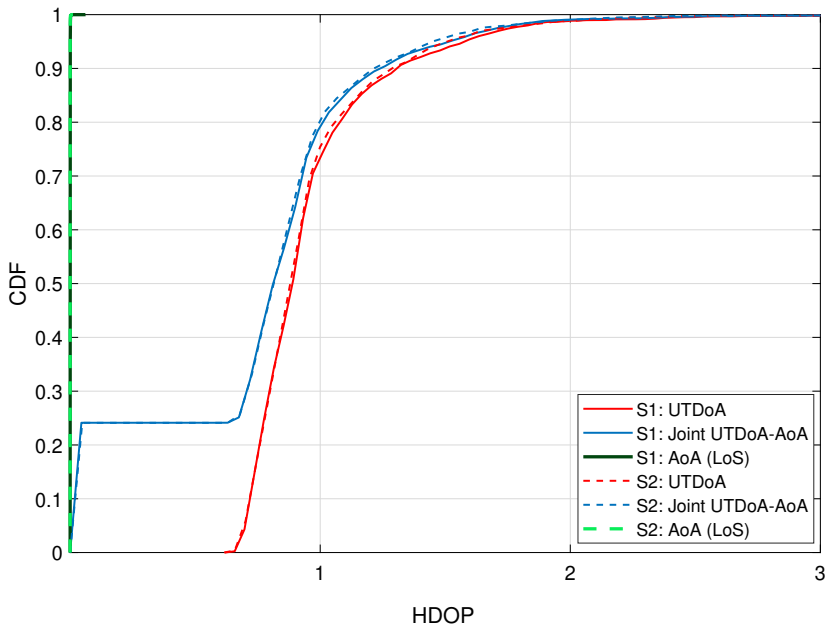


Figure 5.2: CDF of the HDOP for UTDoA, AoA and hybrid solution. S1 refers to first scenario and S2 refers to the second scenario.

The positioning accuracy is now evaluated by assessing the actual gain that is obtained in terms of the UE positioning performance. In conditions of synchronization error, with the presence of NLoS and multipath, UTDoA leads to poor accuracy and reliability of the computation position. This is reflected in the simulation results for both scenarios shown in Figures

5.3 and 5.4, where severe degradation errors are clearly seen compared to what is expected in ideal conditions (see Figures 5.5 and 5.6). The combination of angle observables with those of time delay has already been shown to provide a significant improvement with UTDoA solutions, where the positioning accuracy is less than 30 m for 80% of the UEs. The maximum horizontal position error is reduced by 27.5%. However, this improvement does not overtake the performance achieved by RTT, which relaxes the constrained positioning problem, i.e., the presence of synchronization error, giving a position accuracy improvement of 5%. This can be noticed above the 80th percentile in Figures 5.3 and 5.4.

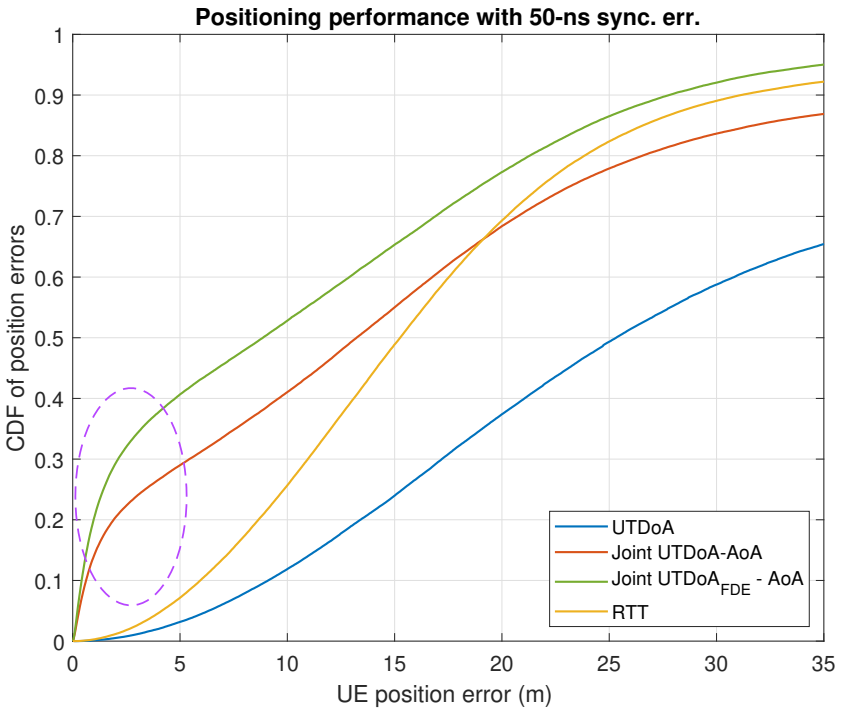


Figure 5.3: Results for 20 MHz bandwidth with 50 ns sync. err.

Since there is a predominance of NLoS conditions in 5G urban transmissions, the BS selective solution is of high interest for its ability to eliminate such impairments, in order to achieve a better performance assessment under realistic assumptions while using 5G positioning signals. We therefore analyze the impact of the BS Fault Detection and Exclusion (FDE) mechanism on the joint UTDoA-AoA positioning performance. The probability of false alarm is set to $P_{fa} = 0.1$, resulting in a threshold of $\gamma = 1.4797$ m for scenario 1, and $\gamma = 1.4879$ m for scenario 2, calculated as explained in Section 4.2.4. Results are reported in Figures 5.3 and 5.4 with the label "Joint UTDoA$_{FDE}$-AoA" and show a significantly improved hybrid solution when the NLoS exclusion mechanism is applied. The maximum horizontal position error is reduced by 40% compared with the results achieved using UTDoA as the stand-alone technology. The use of this mechanism has improved the accuracy of the hybrid method of 18.51%. It also overcomes the performance achieved using RTT and tends to reach the performance of hybrid solutions in conditions of perfect synchronization with an improvement of 12.5%. Another observation related to the performance of the positioning methods is the significant improvement in accuracy until the 30% percentile for the first scenario (see dashed circle). This is explained by the presence of more than one LoS angle measurements in the computation solution and ranging measurements in LoS conditions.

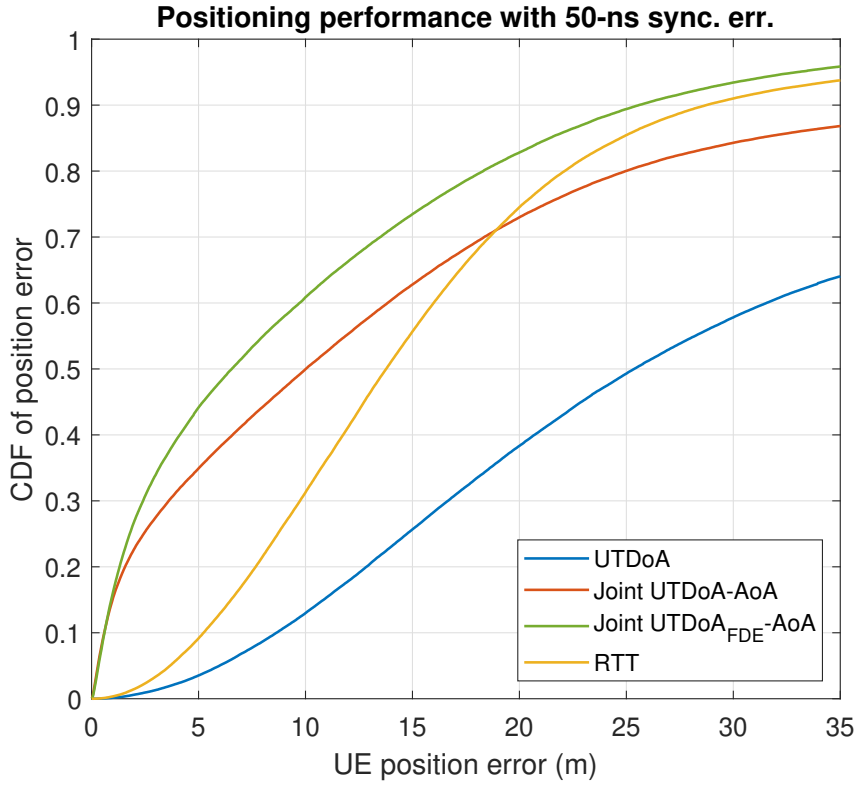


Figure 5.4: Results for 50 MHz bandwidth with 50 ns sync. err.

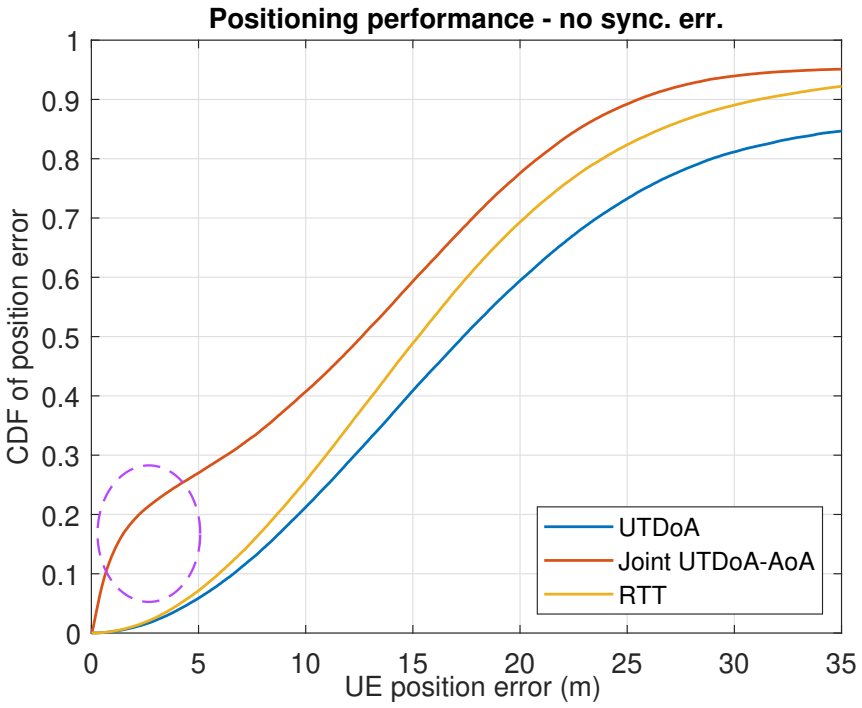


Figure 5.5: Results for 20 MHz bandwidth with perfect sync.

Apart from the statistical performance of each method, it is also important to assess the actual gain we obtain through the BS exclusion mechanism in terms of UE positioning performance. The results have shown that the BS exclusion mechanism has only met the regulatory requirements for emergency services, i.e., having an accuracy of < 50 m on 80% of the cases.

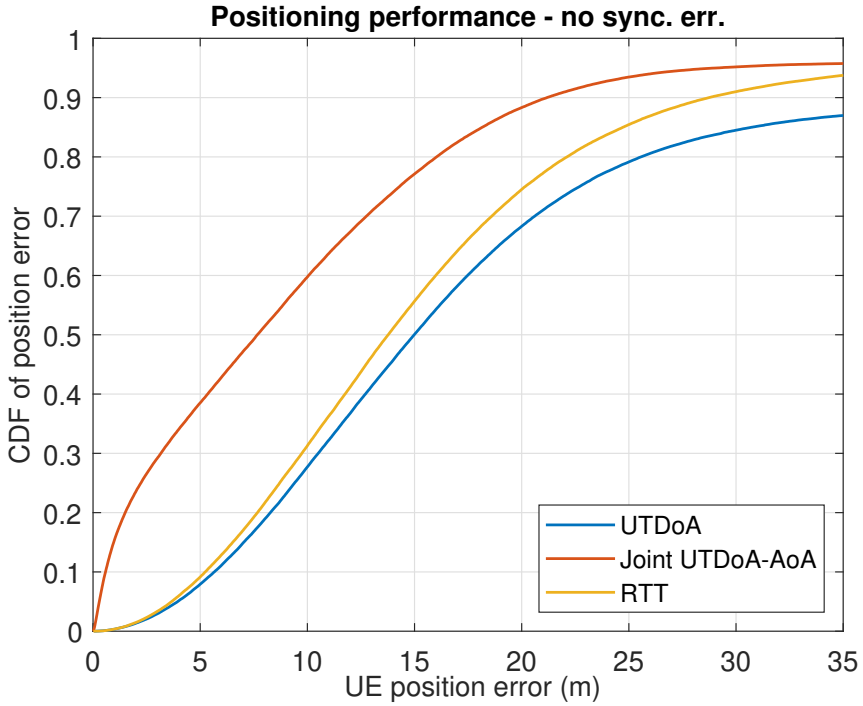


Figure 5.6: Results for 50 MHz bandwidth with perfect sync.

Table 5.2: Performance of BS exclusion mechanism in positioning accuracy.

		Scenario 1 (%)	**Scenario 2** (%)
UTDoA measurements	Sync. err.	81.86	
	No sync. err.	18.14	
BS for UTDoA positioning	One BS with sync. err.	38.75	
	More than one BS with sync. err.	43.11	
	No BS with sync. err.	18.14	
FDE performance	BS exclusion	55.46	56.47
	BS no exclusion	6.9	6.85

However, the use of this method enhances the positioning availability. Table 5.2 compares the performance of the NLoS monitoring method for both scenarios. From all the BSs that contributed to the positioning computation, 81.86% of them have a synchronization error of -50 ns or 50 ns, and from which 38.75% of the cases, in the group of BSs dedicated for the positioning of each receiver, there is one BS with synchronization error. For 43.11% of the cases, more than one BS has a synchronization error. Only 18.14% of the BSs has perfect synchronization. Having a low P_{fa}, we are expecting that the probability of detecting the faulty BS is low. Results show that for both scenarios, the method was used less than 65% of the time, and in 55% of the cases, the method was able to remove the abnormal measurement. About 7% of the time where the method has been used, the method was not able to remove the faulty BS but managed to remove those whose multipath was large in the majority of cases. The rest of the time, it was not able to perform the monitoring and hence to exclude the faulty BS. This is because the method could remove one BS at a time, and therefore, during 43% of the time that there is more than one biased measurement, even if it manages to remove one, the rest of malicious BS will still contribute to the degradation of the accuracy. Finally, the increase in P_{pfa} increased the

percentage of failure of the method, and this will therefore affect the performance of positioning. For example, when $P_{pfa} = 0.5$, the percentage of the time where the method does not manage to exclude a BS increased almost double compared with the one when $P_{pfa} = 0.1$. All in all, in conditions of a wide bandwidth, the performance is better compared to a narrower bandwidth.

5.4 Conclusion

In this chapter, we showed the advantages of using array antennas in combination with a time-delay-based positioning method to significantly improve positioning accuracy in deep urban environments. Simulations based on a deep urban deployment map to assess the improvement compared to the case when UTDoA performs as a stand-alone technology were performed. The combination of angle observables with those of time delay already provides an improvement of 27.5% in positioning accuracy with respect to the UTDoA solutions. Additional accuracy can be obtained with the use of the BS exclusion method proposed in Chapter 4. This method allows us to identify and remove abnormal measurements from BS affected by NLoS and synchronization error. The method manages to remove the malicious BS in the majority of cases. The maximum horizontal position error is reduced by 40% compared to UTDoA solution and 18.15% compared to the hybrid case without the BS exclusion mechanism. All in all, the obtained results contribute towards the fulfillment of high-accuracy positioning requirements in challenging environments when using cellular networks. Moreover, they show the value of using advanced antennas in 5G positioning.

Chapter 6

5G SDR receiver and AoA estimation

So far in this work, we discussed how to enhance the performance of 5G positioning, taking advantage of the fully integrated simulator presented in Chapter 2. The simulator allows to model configurations that are fully representative of the use-cases and the user environments described in Chapter 1. The results of the simulations, presented in Chapter 3, help to assess the positioning performance of various technologies based on base station locations. The analysis contributes to a better understanding of how 5G signals can deliver accurate and reliable location-based services. Moreover, in Chapter 4 we addressed the problem of outliers in Non Line of Sight (NLoS) conditions and explained how the pseudo-range measurements will contribute to their detection and exclusion. This solution was later used in Chapter 5, together with the exploration of the potential of the Angle of Arrival (AoA) estimation, to improve the position accuracy in dense environments. All these simulation-based studies have provided important insights. However, experimental evaluations with actual 5G signals and open-source platforms, whose ability is to adapt and reconfigure their functionality through software updates based on the Radio Frequency (RF) requirements, are crucial for a comprehensive understanding of the system's performance.

Results in Chapter 3 reaffirmed that, when it comes to real implementations, a gap between theoretical expectations and real-case scenarios can be faced. Therefore, in this chapter, we will focus on the implementation of a real scenario to achieve a high-accuracy AoA estimation. Classical and modern AoA estimation techniques (Section 6.3) will be used in this context, as they provide essential information for robust localization in complex environments. Incorporating AoA estimation into 5G positioning relies on a combination of array processing and calibration techniques. An experimental platform testbed based on versatile Software-Defined Radio (SDR) devices, that can easily customize the transmission and reception processes, is used. It is presented in Section 6.1. The developed platform consists of an SDR-based transmitter and receiver where the signal configuration and baseband signal processing are incorporated (see Section 6.2).

Angular estimation faces a lot of challenges when it comes to real implementation. Its estimation accuracy is highly sensitive to hardware impairments, clock stability, synchronization, and phase misalignment. Additional challenges such as manufacturing inaccuracies, temper-

ature variations, hardware-related issues compound environmental challenges (multipath, interference), and time-frequency misalignment between transmitter and receiver are also a big influence in the degradation of AoA estimation. Therefore, the aims of this chapter are several. The first one is to shed light on the challenging problem of achieving coherent phase reception between the RF channels of existing multi-channel SDR described in Section 6.5. This is a key problem that must be solved when dealing with 5G positioning when the angle of arrival estimation is needed. To solve this problem, the process of RF channel error estimation and compensation is described. Apart from the calibration related to phase coherence, practical recommendations are provided to achieve the highest possible data throughput between the SDR and the controlling computer. Moreover, a comparison among the most relevant features of different models of Universal Software Radio Peripheral (USRP) SDR devices is discussed, including an analysis of their performance in terms of phase differences between RF channels.

To achieve high-fidelity results, antenna calibration, presented in Section 6.5, becomes also indispensable. Array processing methods leverage multiple antennas to receive RF signals and exploit their spatial properties for accurate AoA estimation. Both an In-Situ antenna calibration (where the transmitter is used with a known direction to calibrate the antennas, but no propagation condition is known) and an antenna calibration in a controlled environment (i.e. in a dedicated measurement chamber, without multipath propagation and interference) are carried out. The calibration in array processing ensures the alignment of antenna elements, mitigates hardware imperfections, and compensates for system-level errors. By combining the power of AoA estimation and calibration, 5G networks can deliver precise and reliable location-based services.

Synchronization, described in Section 6.4, is also an important issue that affects the performance of AoA estimation. In particular, Orthogonal Frequency Division Multiplexing (OFDM) systems are very sensitive to synchronization errors affecting the subcarrier orthogonality and therefore facing performance degradation. To maintain synchronization, a Carrier Frequency Offset (CFO), Symbol Timing Offset (STO), Sampling Clock Offset (SCO), and time offset compensation scheme are implemented. The compensation of these offsets is done before demodulating the incoming waveform and applying the antenna error calibration.

Finally, the results of some indoor and outdoor experiments are presented in Section 6.7. For the indoor experiment, the In-Situ calibration is used, while for the outdoor experiment, the anechoic chamber calibration is used. In the outdoor experiments, the presence of a reflector for the performance of AoA estimation is considered.

Additionally, a deep analysis, presented in Section 6.6, through simulations of the synchronization error effects in AoA estimation accuracy and the achievable angle precision in the scenarios with the presence of multipath and without are derived. Several AoA estimation algorithms are explored to evaluate their practical applicability in real-world settings, especially in environments with the presence of multipath and interference. All these results are used to derive the statistics of the angle estimation error.

By providing insights and a systematic approach for conducting experimental 5G localization studies, this work seeks to expedite the development of accurate and robust AoA estimation for 5G networks. As the field of 5G localization evolves rapidly, the proposed methodology and the obtained results offer a valuable framework to advance the understanding and implementation of precise AoA estimation and calibration in the context of 5G positioning. It will enable new

positioning paradigms such as single Base Station (BS) positioning, where measurements from only one BS are needed to determine the user's position [56], [57].

6.1 5G receiver structure

In this section, a 5G experimental platform for AoA estimation based on SDR devices is proposed. The developed platform can customize the transmission and reception of 5G New Radio (NR) Uplink signal, Sounding Reference Signal (SRS). The angle measurement estimation is the first step to provide uplink positioning that involves the transmission of signals from the User Equipment (UE) to the BS. Since the UE is responsible for actively transmitting positioning-related signals, the infrastructure at the BS side is less complex compared to downlink positioning. It is very suitable also for mobile devices as they are typically equipped with transmitters for communication.

The experimental platform consists of an SDR-based transmitter and receiver as depicted in Figure 6.1. On the transmitter side, the USRP hardware N310 is used for periodic transmissions of the 5G uplink signal SRS through one single channel node. The USRP N310 has three master clock rates that allow a higher diversity in-sample rate, which makes it suitable when dealing with 5G signals where sampling rate and bandwidth are important. Each channel node (four in total for transmission and only one used for the experimental part) provides up to 100 MHz instantaneous bandwidth and covers an extended frequency range from 10 MHz to 6 GHz. Therefore, this SDR-based transmitter is suitable for estimating the AoA in the sub-6 GHz. The transmission process has been deployed on a PC with an Intel i5-9500 CPU @ 3GHz and 32GB of RAM and an Ubuntu 22.04 LTS OS installed. The USRP is connected to the computer unit through two 10 Gigabit Ethernet cables. On the receiver side, the USRP NI-2955 is used to capture the baseband signal streamed at all receiving radio channels. Note that the employment of multiple antennas in the receiver is pivotal for precise AoA determination. The signal reception process through NI-2955 has been deployed on a PC with an Intel i7-10700 CPU @ 2.9GHz and 32GB of RAM and a Windows 10 OS installed that will allow the use of LabVIEW. Apart from the reception, LabVIEW will also help to enable the Local Oscillator (LO)-sharing capability that will be explained later on. The NI-2955 is connected to the PC through a four-line MXIe 1st generation cable. In both transmitter and receiver, the PCs utilized are equipped with Solid Stated Drives (SSD) NVMe-based Category 3. 5G monopole antennas covering sub-6GHz 5G NR bands are used for both transmitter and receiver.

The 5G receiver software (see Figure 6.2) is composed of several blocks such as the calibration module (RF channel error calibration and antenna error calibration), the synchronization module (time delay and frequency offset estimation and data processing module), the data extraction block, and the AoA estimation. In the calibration module, the RF channel calibration is in charge of the estimation and compensation of phase misalignment between the receiver's RF channels and the antenna calibration is responsible for estimating and compensating the offset between antenna elements of the array. In the synchronization module, time delay and frequency offset estimation are done through both coarse and fine synchronization processes. The synchronization process is based on the pilot symbols of the transmitted waveform. This means that the transmitter sends known pilot symbols in the data stream. These pilot symbols are designed to be easily distinguishable at the receiver. By comparing the received pilot

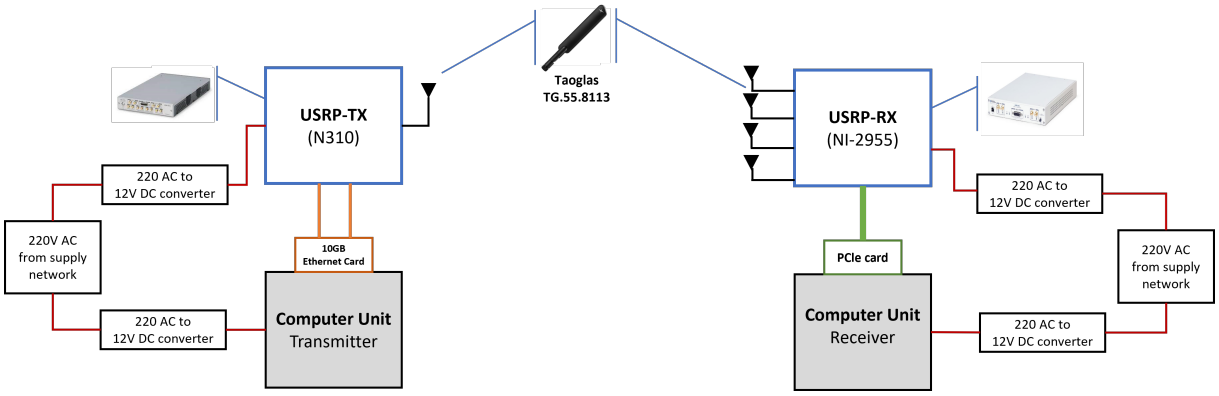


Figure 6.1: Block diagram of the testbed. On the left side is depicted the transmitter and on the right is depicted the receiver. The inverted black triangles represent antenna elements. The red cables represent the power-based type, the orange ones represent the Ethernet cables and the green one represents the MXIe cable.

symbols with the transmitted ones, the receiver can infer the time and frequency offset and make the corrections of the distortions. Note that the synchronization is performed after the compensation from hardware impairments is applied. Then, the antenna error compensation is done after the demodulation of the compensated incoming waveforms, incorporated in the algorithms for AoA estimation to be explained in Section 6.3. The data extraction part of the data processing module performs the demodulation of each incoming waveform by using the Fast Fourier Transform (FFT) after Cycle Prefix (CP) is removed. The OFDM symbols containing the transmitted pilots will then be used for the AoA estimation, where the estimated antenna errors have been compensated before angle computation.

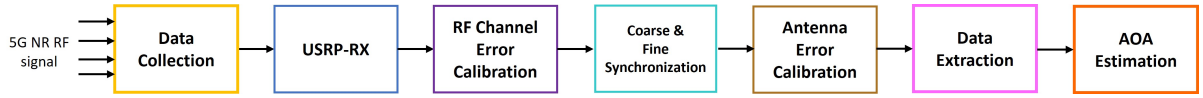


Figure 6.2: 5G SDR receiver top-level block diagram.

The software is implemented in MATLAB by post-processing the signal captured with the USRP NI-2955 platform. Each radio channel of the device represents a separate baseband stream provided by the hardware front-end. They are configured with a common carrier frequency, front-end gain, and sampling rate. The same configuration parameters are used for the transmitter side. The RF module down-converts the received RF signals to a baseband signal and converts it to an I/Q digital signal using a 14-bit Analog-to-Digital Converter (ADC). The quantization bit of the converted digital signal is changed to 16-bit by signal processing implemented on the FPGA module and the captured data for each channel are first stored on a drive before being processed. Each stage of the receiver (Figure 6.2) plays a fundamental role in ensuring the successful and accurate estimation of AoA. For a comprehensive understanding, we will now delve into each stage in detail.

6.2 5G NR signal generation and receiver data reception

Before the periodic transmission of the 5G uplink SRS signal, on the transmitter side, the signal generation and modulation are carried out. The uplink waveform generation is based on the process depicted in Figure 6.3. The data is generated through a modulation block composed by the symbol mapping, where the waveform is organized into frames of 10 ms duration, each

divided into 10 subframes of 1 ms, named slots. Each slot is built from 14 OFDM symbols, each prepended with a cyclic prefix. For the experimentation, 4 SRS symbols will be assigned as the last 4 OFDM symbols of the subframe (see Figure 6.4). Each subcarrier, i.e. the resource element (RE), being the smallest unit of the resource grid, is mapped in the frequency domain within the whole transmission allocation (see the resource grid allocation in the upper-left part of Figure 6.4). A spacing of 15 kHz between SRS RE is assigned with a span of two subcarriers between two adjacent pilot entries for each of the SRS symbols used. This comb structure of 2 gives a high density in the time domain. Therefore the 1596 transmitted RE is mapped to the N available subcarriers (2048 in total per symbol). A full band of 25 MHz SRS transmission has been used as shown in the waveform plot in the frequency domain in the upper-right part of Figure 6.4.

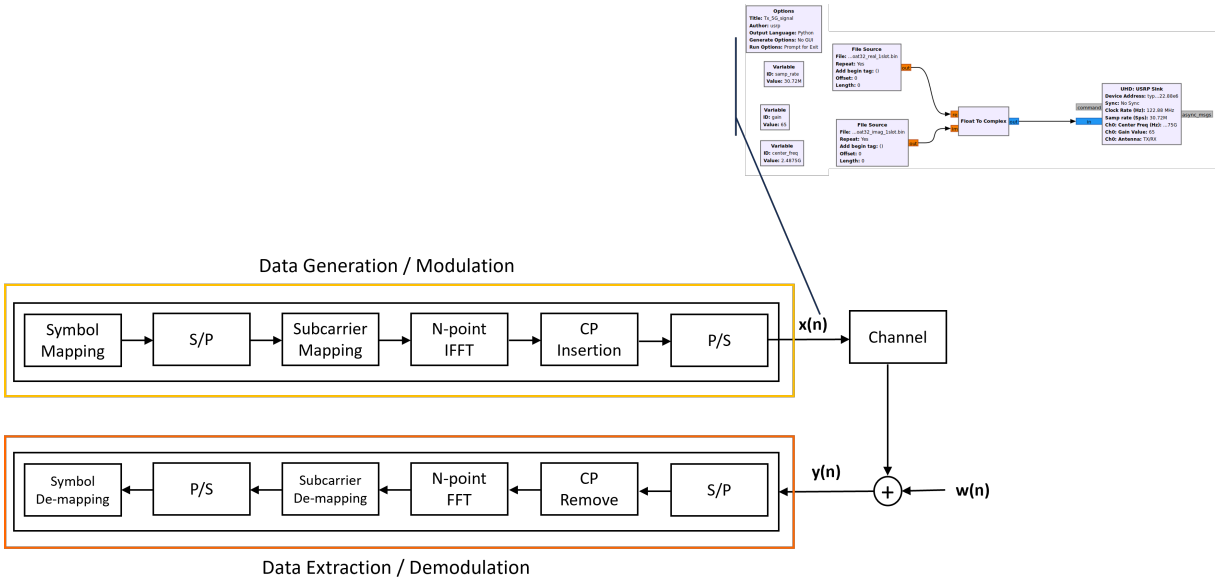


Figure 6.3: Data generation and extraction process. The 5G NR waveform is saved in a binary file, where the I and Q samples are interleaved and transmitted periodically for 2 sec.

The digital base-band of the l-th OFDM symbol in the time-domain is generated using the Inverse Fast Fourier Transform (IFFT):

$$x_l[n] = \frac{1}{N} \sum_{k=-\frac{N}{2}}^{\frac{N}{2}-1} b_l[k] e^{j\frac{2\pi k(n-N_{CP})}{N}}, \tag{6.1}$$

with $n = 0, 1, \ldots, N + N_{cp} - 1$ being the sample index of an OFDM symbol, and k-th the OFDM subcarrier index. The waveform of one slot duration is saved in a binary input file where the I/Q samples are interleaved. The transmitter converts the baseband signal to an RF signal and outputs it via the SMA connector where the antenna is linked. The digital signal $\mathbf{x}$ is transmitted through GNU Radio [58], by one source, periodically at a fixed repetition of time, i.e. one slot at a time. Moreover, the signal is transmitted at a predefined AoA and impinges on an antenna array of M elements. The 5G NR configuration parameters and the OFDM numerology scaling have been summarized in Table 6.1. For a detailed explanation of 5G signal generation and parameter configurations refer to Chapter 2.

On the receiver side, time-domain multichannel SRS signals are transformed to the frequency

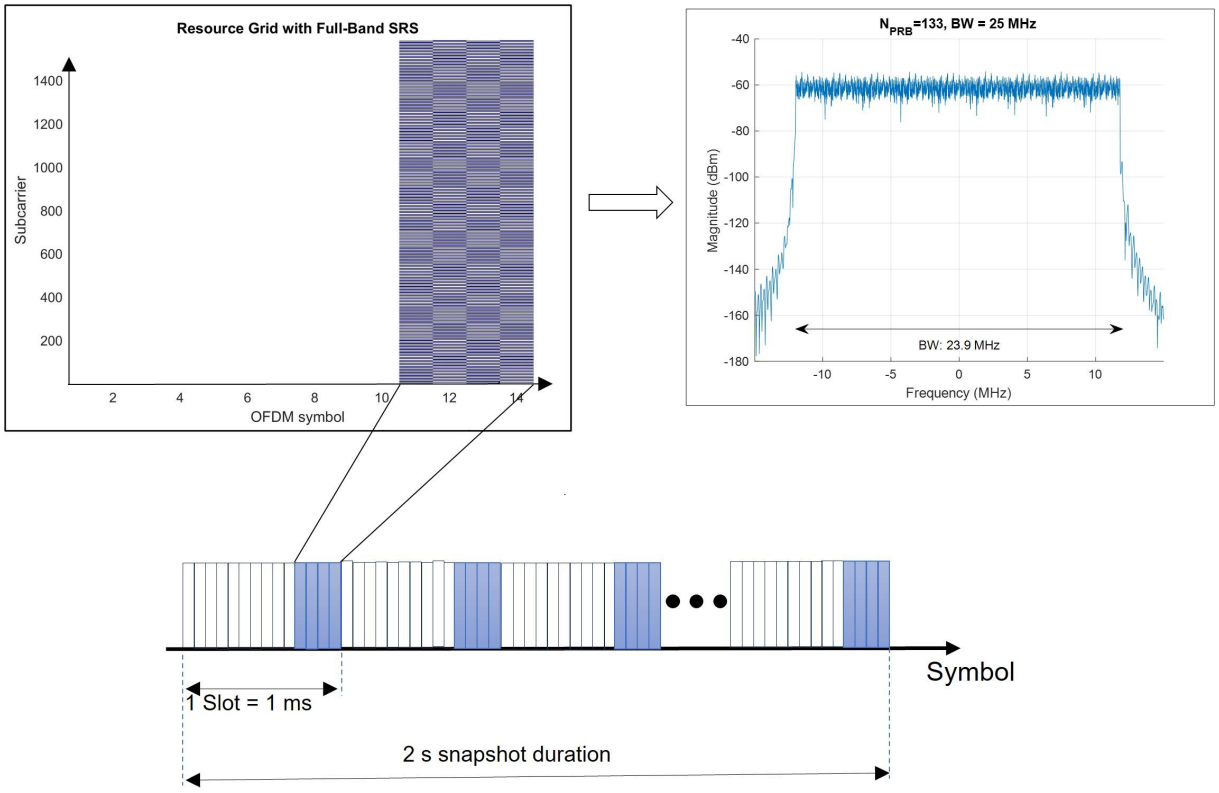


Figure 6.4: 5G NR RF signal transmission characteristics.

Table 6.1: 5G NR Uplink signal specifications.

Parameter	**Value**
Nr. of antenna elements	4
Array model	ULA
Carrier frequency [GHz]	2.4875
Subcarrier spacing [kHz]	15
OFDM Symbol duration [μs]	66.67
Cyclic prefix duration [μs]	4.69
Pattern	Comb-two
Bandwidth [MHz]	25
Sampling rate* [MHz]	30.72
Slot duration (14 symbols) [μs]	1000
Slots in subframe	1
Periodicity	every 1 ms

domain using FFT and removing the CP from each OFDM symbol. The stream at the i-th received radio channel of the receiver, at the l-th OFDM symbol and k-th subcarrier is denoted as:

$$Y_{l,k}^{(i)} = a^{(i)}(\theta) b_{l,k}^{(i)} e^{\frac{-j2\pi(k\tau+l\varepsilon)}{N}} e^{j\Phi'^{(i)}} e^{j\beta^{(i)}} + w_{l,k}^{(i)}, \tag{6.2}$$

where $a(\theta) = \sqrt{\alpha(\theta)} e^{j\Phi(\theta)}$ is the antenna response at i-th front-end channel composed by the gain pattern $\alpha(\theta)$ and phase pattern $\Phi(\theta)$, τ is the time delay, and ε is the CFO. Note that, for each of the four received RF channels, τ, and CFO are estimated and the respected error offset for compensation is taken as the mean value. Then, the estimated offsets are compensated to each of the four received waveforms. Φ' is the phase offset of i-th received RF channel

introduced by the front-end hardware, and β represents the rest of phase offsets affecting the error of the i-th antenna response of the corresponding RF channel, such as antenna non-idealities (including mutual coupling and manufacturing imperfections), structures surrounding the installation, multipath and/or interference. Lastly, $w_{l,k}^{(i)}$ represents the noise of i-th channel at l-th OFDM symbol and k-th subcarrier. Each radio channel of the receiver represents a separated baseband received signal provided by the hardware front end. They are arranged into a single matrix $\mathbf{G} = [\mathbf{y_1}, \mathbf{y_2}, \ldots, \mathbf{y_M}]^T \in \mathbb{C}^{M,N}$.

6.3 Techniques for AoA estimation

In this section, a description of the techniques for AoA estimation will be presented. There are several techniques considered in this chapter from classical to more modern, that can be divided into three categories: classical, subspace, and parameter-free iterative AoA techniques. In the classical AoA techniques, the delay and sum technique [59] (the classical beamformer) is considered. For the subspace AoA techniques, MUltiple SIgnal Classification (MUSIC) [60] and Estimation of Signal Parameters via Rotational Invariance Techniques (ESPRIT) [61] are considered. Finally, about the parameter-free iterative AoA techniques, Iterative Adaptive Approaches (IAA) [62], Sparse Asymptotic Minimum Variance (SAMV), and SAMV-Stochastic ML (SAMV-SML) methods [63] are considered. For the estimation of AoA we consider a Uniform

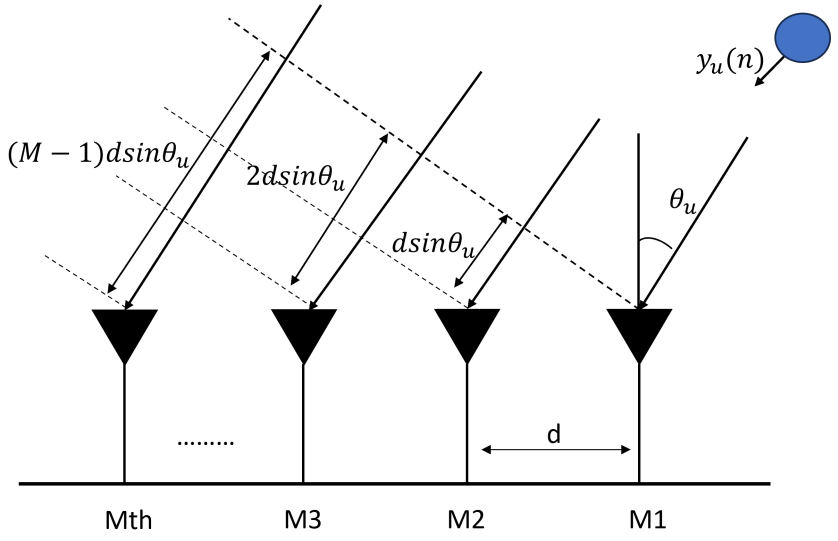


Figure 6.5: ULA with M elements for AoA estimation.

Linear Array (ULA) with M omnidirectional antennas (see Figure 6.5), that are spaced linearly with equal distance d. The ULA receive D signals, generated by D sources. Each signal $\mathbf{x}_u$ of the u-th source impinges on the array at an angle θ_u. Then it travels at a speed of c over a distance d_d and reaches the first rightmost elements. If we consider all the signals generated by all the D sources, the total signal and noises received by the m-th array element at time n can be expressed as:

$$y_m(n) = \sum_{u=1}^{D} x_u(n) e^{-j(m-1)\frac{2\pi}{\lambda}\sin(\theta_u)} + w_m(n). \tag{6.3}$$

The steering vector used for the AoA estimation (θ_u) is:

$$\mathbf{a}_u(\theta) = [1 \quad e^{-j\frac{2\pi}{\lambda}\sin(\theta_u)} \quad e^{-j2\frac{2\pi}{\lambda}\sin(\theta_u)} \quad \dots \quad e^{-j\frac{(M-1)\pi}{\lambda}\sin(\theta_u)}]^T. \tag{6.4}$$

For the case of time delay (τ_u) estimation, the steering vector will be modified as:

$$\mathbf{r}_u(\tau) = [1 \quad e^{-j2\pi K_{\mathrm{TC}} f_{\mathrm{sc}} \tau_u} \quad e^{-j2\pi 2K_{\mathrm{TC}} f_{\mathrm{sc}} \tau_u} \quad \dots \quad e^{-j2\pi(N_{\mathrm{FFT}}-1)K_{\mathrm{TC}} f_{\mathrm{sc}} \tau_u}]^T, \tag{6.5}$$

where N_{FFT} is the total number of subcarriers per OFDM symbol, f_{sc} is the subcarrier frequency, and K_{TC} represents the transmission comb number (see Section 2.2 in Chapter 2). Note that in this part of the work, the SRS signal is transmitted every $K_{\mathrm{TC}} = 2$ subcarriers.

6.3.1 Classical Beamformer

The classical or conventional beamforming method is commonly known as the delay and sum method or the Bartlett method. A ULA comprising M elements is used, where $\mathbf{a}(\theta)$ represents the steering vector corresponding to a scanning angle θ. The fundamental concept involves scanning across the angular region of interest, with the weight vector given by:

$$\mathbf{w}_{\mathrm{BF}} = \mathbf{a}(\theta). \tag{6.6}$$

Integrating the weight vector into the equation below, we can derive the output power of the classical beamformer as a function of the angle of arrival:

$$P_{\mathrm{BF}}(\theta) = \mathbf{w}_{\mathrm{BF}}^H \mathbf{R}_y \mathbf{w}_{\mathrm{BF}} = \mathbf{a}(\theta)^H \mathbf{R}_y \mathbf{a}(\theta), \tag{6.7}$$

where $\mathbf{R}_y$ is the covariance matrix computed as an average of multiple snapshots of the received data:

$$\mathbf{R}_y = \frac{1}{T}\sum_{t=1}^{T} \mathbf{y}_t \mathbf{y}_t^H. \tag{6.8}$$

The $\mathbf{y}$ is a $M \times 1$ vector of a received snapshot of antenna element data consisting signal and the Additive White Gaussian Noise (AWGN), whereas T is the number of snapshots, respectively. The direction yielding the maximum output power serves as the estimate for the desired signal's direction.

6.3.2 MUltiple SIgnal Classification (MUSIC)

When referring to subspace techniques, the MUSIC algorithm is a common technique for AoA estimation, providing high resolution in angular estimation. However, this comes at the cost of requiring full a priori knowledge of the number of sources and the array response. The signal and noise subspaces are distinguished through an eigen decomposition operation applied to the covariance matrix of the received signal, incurring substantial computational complexity. The received data at the M elements of the array be expressed as

$$\mathbf{y} = \mathbf{a}(\theta)\mathbf{x} + \mathbf{w}, \tag{6.9}$$

where $\mathbf{x}$ and $\mathbf{y}$ are the transmitted and received signal vectors, respectively. The vector $\mathbf{w}$ represents AWGN, and $\mathbf{a}(\theta)$ is the steering vector defined as in 6.4 for the ULA with elements separated by element spacing d. The covariance matrix $\mathbf{R}_y$ is a crucial quantity in any subspace technique and it is derived from the received signal data. When the signal is uncorrelated with the noise, the sensor covariance matrix has two components, the signal covariance matrix and the noise covariance matrix. The signal covariance matrix is a M-by-M matrix with rank $D < M$, where D is the number of sources.

The MUSIC algorithm assumes that the noise powers are equal at all antenna elements and uncorrelated between antenna elements. Under this assumption, the noise covariance matrix becomes a M-by-M diagonal matrix with equal values along the diagonal.

As the true covariance matrix is not known, MUSIC estimates the covariance matrix $\mathbf{R}_y$ from an average of multiple snapshots of the received data as in 6.8. When noise is added, the eigenvectors of the sensor covariance matrix with noise present are the same as the noise-free covariance matrix. In practice, an eigen decomposition is performed, where the D largest eigenvalues correspond to the signal subspace $\mathcal{U}_s$, consisting of the vectors $[\mathbf{u}_1, \ldots, \mathbf{u}_D]$. The eigenvectors corresponding to the remaining $(M - D)$ zero eigenvalues span the null subspace $\mathcal{U}_n$ consisting of the vectors $[\mathbf{u}_{D+1}, \ldots, \mathbf{u}_M]$. The arrival vectors, which also belong to the signal subspace, are orthogonal to the null subspace.

The MUSIC algorithm searches for all arrival vectors that are orthogonal to the noise subspace by constructing an arrival-angle dependent power expression, i.e.,

$$P_{\text{MUSIC}}(\theta) = \frac{1}{\mathbf{a}^H(\theta)\mathcal{U}_n\mathcal{U}_n^H\mathbf{a}(\theta)}. \tag{6.10}$$

When an arrival vector is orthogonal to the noise subspace, the peaks of the MUSIC spectrum are infinite. However, due to added noise in real conditions, the arrival vectors are never exactly orthogonal to the noise subspace. The algorithm identifies the D largest peaks.

MUSIC algorithm can be extended into the 2-dimensional (2-D) space to simultaneously estimate the multipath propagation delay and the AoA. Propagation delay estimation becomes crucial when multiple signals arrive at the same angle. In such cases, the traditional 1-dimensional (1-D) MUSIC algorithm struggles to separate the signals, unlike the 2-D MUSIC algorithm, which utilizes a 2-D spectrum for both angle and delay estimation. The 2-D MUSIC spectrum is computed as follows:

$$P_{\text{MUSIC}}(\theta, \tau) = \frac{1}{(\mathbf{a}(\theta) \otimes \mathbf{r}(\tau))^H\mathcal{U}_n\mathcal{U}_n^H(\mathbf{a}(\theta) \otimes \mathbf{r}(\tau))} \tag{6.11}$$

Here, the operator $\otimes$ denotes the Kronecker product between the angle computed as in 6.4 and delay pair computed as in 6.5. The 2-D MUSIC algorithm acquires the angle-delay pair through a two-dimensional search. Assuming D impinging waves, the D largest peaks in the spectrum correspond to the angle-delay pairs of these signals. Note that a similar modification in the steering vector is done for the classical beamforming to convert it into a 2-D spectrum.

6.3.3 Estimation of Signal Parameters via Rotational Invariance Techniques (ESPRIT)

The ESPRIT algorithm is grounded in the analysis of a subspace utilized for localizing a source or estimating signal parameters (such as frequency and phase). The fundamental concept of this algorithm involves "splitting" the antenna array into subarrays separated by an equivalent displacement. The inherent lower complexity of the ESPRIT algorithm provides it with an advantage over the MUSIC algorithm in applications where resource constraints are a limiting factor.

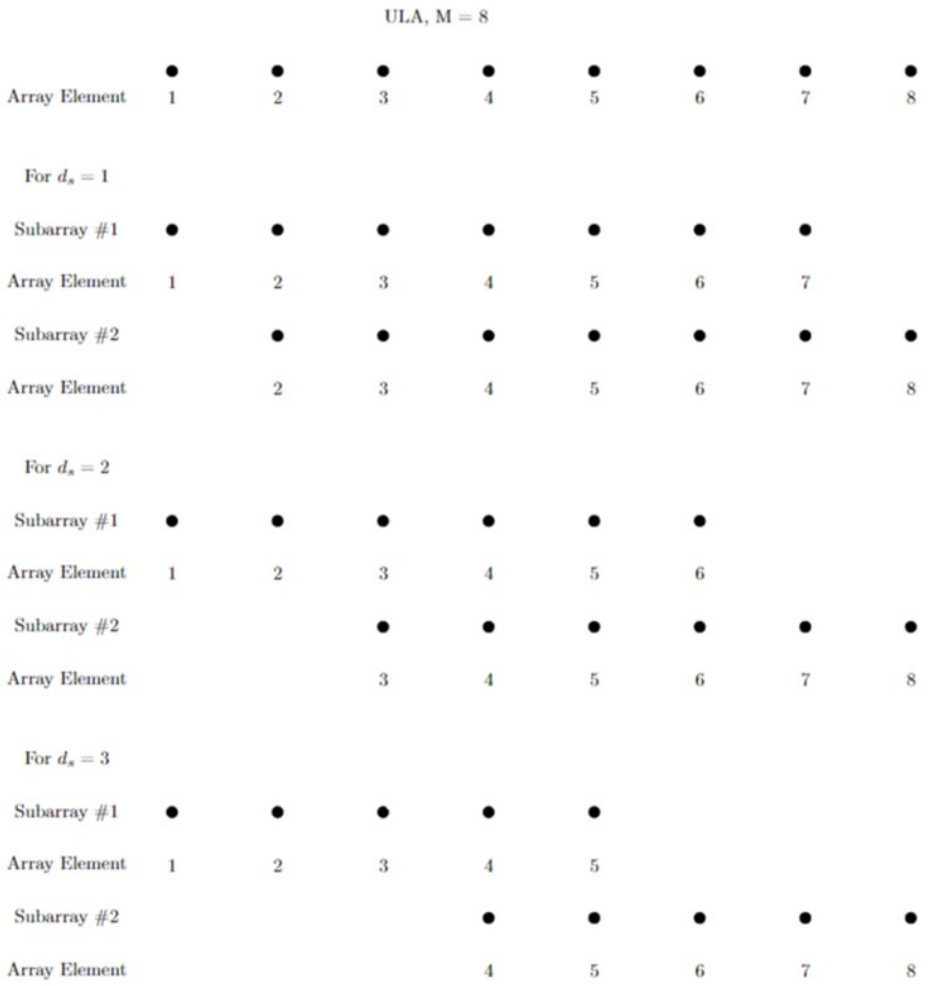


Figure 6.6: Subarray arrangement for the ESPRIT algorithm [64].

Figure 6.6 illustrates the process of splitting the array into subarrays. For this purpose, a ULA with M elements separated by an element spacing d is considered. The number of elements in the subarrays is denoted as M_s, and d_s is the distance between two subarrays. The first element of the first subarray corresponds to the first element of the original ULA, while the first element of the second subarray corresponds to the $(d_s + 1)$-th element of the original ULA. The relationship between the two subarrays $\mathbf{A}_0$ and $\mathbf{A}_1$ is then given by

$$\mathbf{A}_1 = \mathbf{A}_0 \mathbf{\Phi}, \tag{6.12}$$

where Φ is a diagonal matrix defined as:

$$\mathbf{\Phi} = \begin{bmatrix} \phi_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \phi_N \end{bmatrix}, \tag{6.13}$$

and $\phi_u = e^{-j2\pi d \sin\theta_u}$ for $u = 1, \ldots, D$, where D denotes the number of sources. The matrix $\mathbf{\Phi}$ applies a rotation to the matrix $\mathbf{A}_1$, forming the basis of the ESPRIT algorithm, which leverages similar rotations from the covariance matrix of the received data. Given the full array, with $\mathbf{Q}_s$ being a matrix whose columns form a basis for its signal subspace, and its steering matrix $\mathbf{A}$ spanning the same subspace as $\mathbf{Q}_s$, there exists an invertible transformation matrix $\mathbf{T}$ such that:

$$\mathbf{Q}_s = \mathbf{AT}. \tag{6.14}$$

Define matrices $\mathbf{Q}_{s0}$ and $\mathbf{Q}_{s1}$, derived from $\mathbf{Q}_s$ in the same manner as $\mathbf{A}_0$ and $\mathbf{A}_1$ were derived from $\mathbf{A}$. Similarly, the transformation can be applied to them:

$$\mathbf{Q}_{s_0} = \mathbf{A}_0\mathbf{T}, \tag{6.15}$$

$$\mathbf{Q}_{s_1} = \mathbf{A}_1\mathbf{T} = \mathbf{A}_0\mathbf{\Phi}\mathbf{T}. \tag{6.16}$$

Multiplying (6.16) by $\mathbf{T}^{-1}\mathbf{\Phi}^{-1}\mathbf{T}$, it is obtained:

$$\mathbf{Q}_{s_1}\mathbf{T}^{-1}\mathbf{\Phi}^{-1}\mathbf{T} = \mathbf{A}_0\mathbf{T} = \mathbf{Q}_{s_0} \tag{6.17}$$

Let $\mathbf{\Psi}^{-1} = \mathbf{T}^{-1}\mathbf{\Phi}^{-1}\mathbf{T}$. Then, it follows that:

$$\mathbf{Q}_{s_0}\mathbf{\Psi} = \mathbf{Q}_{s_1}, \tag{6.18}$$

where $\mathbf{\Psi} = \mathbf{T}^{-1}\mathbf{\Phi}\mathbf{T}$. This implies that the diagonal elements of the matrix $\mathbf{\Phi}$ contains the eigenvalues of $\mathbf{\Psi}$. Once the eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_D$ are calculated, the AoAs can be computed as

$$\theta_i = \arcsin\left(-\frac{\lambda_i}{2\pi d}\right). \tag{6.19}$$

Note that the ESPRIT algorithm operates in the signal subspace, in contrast to the MUSIC algorithm, which operates in the noise subspace.

6.3.4 Iterative Adaptive Approach (IAA)

The IAA solution involves defining a scanning grid of S directions by constructing a set of S steering vectors $\mathbf{A}(\theta) = [\mathbf{a}(\theta_1), \ldots, \mathbf{a}(\theta_S)]$, where $\theta = [\theta_1, \ldots, \theta_S]$ is a vector containing the angles considered at the scanning grid. In a 1D angle estimation problem, the scanning vector $\mathbf{A}(\theta)$ must cover the region ($0° \leq \theta \leq 90°$). Considering one degree of resolution, for example, implies that this matrix should contain $\mathbf{S} = 1 \times 90$ steering vectors related to all possible directions in the grid.

Once this scanning grid is defined, the algorithm estimates the powers at each direction and gathers them in the matrix $\hat{\mathbf{P}} = \text{diag}\{P_1, \ldots, P_S\}$. After that, the beamformer for each direction s is computed as:

$$\mathbf{w}_s^H = \frac{\mathbf{a}^H(\theta_s)\bar{\mathbf{R}}^{-1}}{\mathbf{a}^H(\theta_s)\bar{\mathbf{R}}^{-1}\mathbf{a}(\theta_s)}, \tag{6.20}$$

where $\bar{\mathbf{R}}$ is an estimate of the covariance matrix iteratively computed by considering the received signal $\mathbf{y}(t)$ for T snapshots as presented in Algorithm 2.

Algorithm 2 IAA Algorithm

1: Define the scanning vector $\mathbf{A}(\theta)$:

$$\mathbf{A}(\theta) = [\mathbf{a}(\theta_1), \ldots, \mathbf{a}(\theta_S)]$$

2: Compute the signal waveform vector for each direction:

$$\hat{\mathbf{s}}_s(t) = \mathbf{a}_{iter}^H(\theta_S)\mathbf{y}(t)/M, \quad t = 1, \ldots, T; \quad s = 1, \ldots, S \quad \text{(a)}$$

3: Estimate the powers at each direction:

$$\hat{P}_s = \frac{1}{T}\sum_{t=1}^{T} |\mathbf{s}_s(t)|^2, \quad s = 1, \ldots, S \quad \text{(b)}$$

4: Form the diagonal matrix $\mathbf{P}$:

$$\mathbf{P} = \text{diag}\{P_1, \ldots, P_S\}$$

5: **repeat**
6: $\quad \bar{\mathbf{R}} = \mathbf{A}(\theta)\mathbf{P}\mathbf{A}^H(\theta)$ (c)
7: $\quad$ **for** $s = 1, \ldots, S$ **do**
8: $\quad\quad \mathbf{w}_s^H = \mathbf{a}_s^H(\theta_s)\bar{\mathbf{R}}^{-1}/\mathbf{a}_s^H(\theta_s)\bar{\mathbf{R}}^{-1}\mathbf{a}_s(\theta_s)$
9: $\quad\quad \hat{P}_s = \mathbf{w}_s^H\hat{\mathbf{R}}_y\mathbf{w}_s$
10: $\quad$ **end for**
11: **until** convergence

Notice that the beamforming solution is similar to the classical Capon approach [65], and the robustness against array perturbations and coherent signals comes from two facts: (1) the matrix $\mathbf{P}$ is defined by considering that the sources are uncorrelated, and (2) the covariance matrix is estimated by taking into account the power arriving from the directions where the different beamformers are pointing. Power estimates are computed by taking into account the sample covariance matrix $\mathbf{R}_y$ as in (6.8). Finally, it is worth noting that 60 iterations are considered for this work. It is a sufficient number for algorithm convergence. The convergence criterion is based on the evolution of the estimated powers. By defining $\hat{\mathbf{p}}^{iter}$ as the vector containing the power estimates at the *iter*-th iteration of the algorithm, convergence is considered achieved when $\|\hat{\mathbf{p}}^{iter} - \hat{\mathbf{p}}^{iter-1}\|/\|\hat{\mathbf{p}}^{iter-1}\|$ saturates for values lower than 10^{-6}. For the rest of the algorithms presented in the paper, the same convergence criterion is applied.

6.3.5 Iterative SAMV Approaches

In this subsection, the iterative SAMV approaches proposed by [63] to estimate p (being the power estimates) is described. These approaches can estimate the power of the signal even when the number of grid points S exceeds the number of sources, and only a few non-zero components

are present in p. This scenario is common in spectral analysis applications where only the estimation of p is considered relevant (e.g., [66], [67]).

The updated power estimate $\hat{p}_s^{(iter+1)}$ at the $(iter+1)$th iteration is computed as:

$$\hat{p}_s^{(iter+1)} = \frac{\mathbf{a}_s^H \mathbf{R}^{-1(iter)} \mathbf{R}_N \mathbf{R}^{-1(iter)} \mathbf{a}_s}{(\mathbf{a}_s^H \mathbf{R}^{-1(iter)} \mathbf{a}_s)^2} + \hat{p}_s^{(iter)} - \frac{1}{\mathbf{a}_s^H \mathbf{R}^{-1(iter)} a_s}, \quad s = 1, \ldots, S, \tag{6.21}$$

and the noise variance $\hat{\sigma}^{(iter+1)}$ at the $(iter+1)$th iteration as:

$$\hat{\sigma}^{(iter+1)} = \frac{\mathrm{Tr}(\mathbf{R}^{-2(iter)} \mathbf{R}_N) + \hat{\sigma}^{(iter)} \mathrm{Tr}(\mathbf{R}^{-2(iter)}) - \mathrm{Tr}(\mathbf{R}^{-1(iter)})}{\mathrm{Tr}(\mathbf{R}^{-2(iter)})}, \tag{6.22}$$

where the estimate of $\mathbf{R}$ at the lth iteration is given by $\mathbf{R}^{(iter)} = \mathbf{A}\mathbf{P}^{(iter)}\mathbf{A}H + \hat{\sigma}^{(iter)}\mathbf{I}$ with $\mathbf{P}^{(iter)} = \mathrm{diag}(\hat{p}_1^{(iter)}, \ldots, \hat{p}_S^{(iter)})$, and the traditional covariance matrix $\mathbf{R}_N$ computed as in (6.8).

The estimates of power and noise given above may yield irrational negative values due to the presence of the non-zero terms $p_s - 1/(\mathbf{a}_s^H \mathbf{R}^{-1(iter)} \mathbf{a}_s)$ and $\sigma - \mathrm{Tr}(\mathbf{R}^{-1})/\mathrm{Tr}(\mathbf{R}^{-2})$. To resolve this difficulty, the following SAMV approaches are proposed:

- SAMV-0 approach:

  The estimates of p_s and σ are updated at the $(iter+1)$th iteration as:

$$\hat{p}_s^{(iter+1)} = (\hat{p}_s^{(iter)})^2 (\mathbf{a}_s^H \mathbf{R}^{-1(iter)} \mathbf{R}_N \mathbf{R}^{-1(iter)} \mathbf{a}_s), \quad s = 1, \ldots, S, \tag{6.23}$$

$$\hat{\sigma}^{(iter+1)} = \frac{\mathrm{Tr}(\mathbf{R}^{-2(iter)} \mathbf{R}_N)}{\mathrm{Tr}(\mathbf{R}^{-2(iter)})}. \tag{6.24}$$

- SAMV-1 approach:

  The estimates of p_s and σ are updated at the $(iter+1)$th iteration as:

$$\hat{p}_s^{(iter+1)} = \frac{\mathbf{a}_s^H \mathbf{R}^{-1(iter)} \mathbf{R}_N \mathbf{R}^{-1(iter)} \mathbf{a}_s}{(\mathbf{a}_s^H \mathbf{R}^{-1(iter)} \mathbf{a}_s)^2} + \hat{p}_s^{(iter)} - \frac{1}{\mathbf{a}_s^H \mathbf{R}^{-1(iter)} a_s}, \quad s = 1, \ldots, S, \tag{6.25}$$

$$\hat{\sigma}^{(iter+1)} = \frac{\mathrm{Tr}(\mathbf{R}^{-2(iter)} \mathbf{R}_N)}{\mathrm{Tr}(\mathbf{R}^{-2(iter)})}. \tag{6.26}$$

- SAMV-2 approach:

  The estimates of p_s and σ are updated at the $(iter+1)$th iteration as:

$$\hat{p}_s^{(iter+1)} = \hat{p}_s^{(iter)} \frac{\mathbf{a}_s^H \mathbf{R}^{-1(iter)} \mathbf{R}_N \mathbf{R}^{-1(iter)} \mathbf{a}_s}{(\mathbf{a}_s^H \mathbf{R}^{-1(iter)} \mathbf{a}_s)^2} + \hat{p}_s^{(iter)} - \frac{1}{\mathbf{a}_s^H \mathbf{R}^{-1(iter)} a_s}, \quad s = 1, \ldots, S, \tag{6.27}$$

$$\hat{\sigma}^{(iter+1)} = \frac{\mathrm{Tr}(\mathbf{R}^{-2(iter)} \mathbf{R}_N)}{\mathrm{Tr}(\mathbf{R}^{-2(iter)})}. \tag{6.28}$$

The implementation steps of these SAMV approaches are summarized in Table 6.2.

For more details into the implementation of the methods see [63]. In this chapter, a modification of the SAMV formulas is done by substituting the steering vector of the AoA with the one of the time delay using the formula as in (6.5).

Table 6.2: The SAMV approaches

Initialization: $\{\hat{p}_s^{(0)}\}_{s=1}^{S}$ and $\hat{\sigma}^{(0)}$ using, e.g., (8) and (9).
Repeat:
- Update $\mathbf{R}^{(iter)} = \mathbf{A}\mathbf{P}^{(iter)}\mathbf{A}H + \hat{\sigma}^{(iter)}\mathbf{I}$.
- Update $\hat{p}_s^{(iter+1)}$ using corresponding SAMV formulas in (6.3.5).
- Update $\hat{\sigma}^{(iter+1)}$ corresponding formulas in (6.3.5).

Until convergence.

6.3.6 Grid-Free SAMV-SML Approaches

The resolution of most power-based sparse source localization techniques is limited by the fineness of the direction grid that covers the location parameter space. In the sparse signal recovery model, the sparsity of the truth depends on the distance between adjacent elements in the overcomplete dictionary. Thus, the challenge of choosing the optimum AoA scanning direction grid, arises. Since computational complexity is proportional to the fineness of the direction grid, a highly dense grid is not computationally practical. To overcome the resolution limitation imposed by the grid size a grifd-free SAMV-SML approaches are proposed (see [63]). These approaches refine the location estimates $\theta = (\theta_1, \ldots, \theta_S)^T$ by iteratively minimizing a stochastic Maximum Likelihood (ML) cost function with respect to a single scalar parameter θ_s. The proposed SAMV-SML algorithms use derivative-free uphill search methods such as the Nelder-Mead algorithm [68]. The SAMV-SML approaches are summarized in Table 6.3.

Table 6.3: The SAMV-SML approaches

Initialization: $\{p_s^{(0)}\}_{s=1}^{S}$, $\hat{\sigma}^{(0)}$, and $\{\hat{\theta}_s^{(0)}\}_{s=1}^{S}$ based on the result of SAMV-2 estimates.
Repeat:
- Compute $\mathbf{R}^{(iter)}$ and $\mathbf{Q}_s^{(iter)}$.
- Update p_s and σ using using corresponding SAMV formulas in (6.3.5).
- Minimize ML function with respect to θ_s to obtain the stochastic ML estimates.

The covariance matrix of the interference and noise $\mathbf{Q}_s$ is computed as:

$$\mathbf{Q}_s = \mathbf{R} - \mathrm{p}_s\mathbf{a}_s{\mathbf{a}_s}^H \quad s = 1, \ldots, S. \tag{6.29}$$

For more details into the implementation of the methods see [63].

6.4 Synchronization

OFDM systems are very sensitive to synchronization errors, leading to the disruption of subcarrier orthogonality and performance degradation. Thus, the synchronization error compensation at the OFDM receiver side is of paramount importance. The remarkable spectral efficiency of OFDM technology is rooted in the inherent orthogonality among its subcarriers. Nevertheless, within an OFDM link, circumstances can arise that compromise this orthogonality. Contributing factors encompass the Doppler shift resulting from relative motion between the transmitter and receiver, frequency mismatch between oscillators at both ends, large timing inconsistencies, and the introduction of phase noise. Therefore, prior to the demodulation of subcarriers, the OFDM receiver must execute synchronization processes to uphold their orthogonality. This process is

done after the RF channel error calibration, to be explained in Subsection 6.5.1.

In this section, the impact of time and frequency offset in OFDM systems is described in Subsection 6.4.1. Note that non-synchronization will lead to wrong OFDM demodulation and therefore poor AoA estimation due to additional offset added to the data. Moreover, the process of estimation and compensation of time and frequency offset is presented in Subsection 6.4.2, to continue with the frame synchronization process outlined in Subsection 6.4.3. Finally, it is worth pointing out the residual CFO, which can impact signal demodulation accuracy (to be explained in Subsection 6.4.4).

6.4.1 Impact of time and frequency error estimation

The timing offset in OFDM systems introduces three main effects.

- **Phase rotation** - The time offset causes a phase rotation that is related to both the subcarrier index (m) and the time offset value itself. This rotation affects the useful part of the demodulated symbol, i.e. pilot symbols.
- **Inter-symbol Interference** - Due to the time offset, some samples from the next symbol extend into the time interval of the current symbol due to timing offset, causing interference or mixing between symbols. This mixing of symbols can degrade the quality of received signals.
- **Inter-carrier Interference** - Adjacent subcarriers can experience interference because of the time offset, resulting in a loss of orthogonality between subcarriers. This interference impacts the overall signal integrity.

In addition to the challenges posed by timing offsets, which affect the alignment of symbols in OFDM systems, an even more pronounced problem is the system's sensitivity to frequency offsets. These frequency offsets, resulting from two distinct types of misalignments, introduce further complexities that need to be addressed to maintain the integrity and performance of the OFDM communication. These misalignments are the following.

- **Carrier Frequency Offset (CFO)** - In an ideal scenario, where there is perfect frequency synchronization ($\Delta f_c = 0$) with f_c being the carrier frequency, the FFT output of a specific subcarrier (m-th) reflects only the intended signal sent on that subcarrier, without interference from neighboring subcarriers. However, in the presence of CFO ($\Delta f_c > 0$), the spectrum loses its singular peaks at the intended subcarriers. Interference from adjacent subcarriers occurs, causing the spectrum to exhibit non-null values at frequencies corresponding to these adjacent subcarriers.
- **Fractional Frequency Offset (FFO) and Integer Frequency Offset (IFO)** - Describe how the whole set of frequencies might shift or rotate due to frequency misalignments. This shifting or rotating can result in two main problems:
  - **FFO**: If left uncompensated, introduces interference between subcarriers at the FFT output, leading to a loss of subcarrier orthogonality.

– **IFO**: Causes a circular shift of subcarriers in the FFT output, moving them away from their original positions. This shift can prevent the correct decoding of the entire OFDM burst. Note that IFO merely shifts the subcarrier's positions in the spectrum without affecting their shapes or orthogonality.

Thus, proper frequency synchronization is crucial for OFDM systems. Uncompensated CFO can degrade subcarrier orthogonality, leading to inter-carrier interference and compromised system performance. The correct management of IFO is essential to maintain the correct subcarrier alignment and ensure the successful decoding of OFDM signals. In summary, frequency offset issues in OFDM systems can disrupt subcarrier orthogonality, introduce interference, and hinder proper signal decoding. Addressing these issues through accurate frequency synchronization is vital for maintaining the high performance of OFDM systems. In this chapter, only the symbol time and frequency estimation, frame synchronization, and residual CFO will be used. They will be applied after the RF channel calibration.

6.4.2 Symbol timing and frequency offset estimation

The baseband In-phase and Quadrature (I&Q) samples are checked to estimate and establish the time and frequency synchronization to the uplink received signal with a local replica signal as a reference. Firstly, a coarse estimate of time and frequency offset is done in the time domain. Then, a fine estimation and correction process is undertaken to refine the initial estimates and increase precision. Note that both processes are done for each of the received waveforms and before demodulation. The estimated error offset values are chosen as the mean value of all four RF channels and compensated to each of them. In this way, this process synchronizes the received data streams at each of the RF channels to the beginning of the radio frame.

The initial CFO estimation is performed by the strongest correlation peak between the received waveform with the local replica of the signal. The CFO (ε) is estimated by searching a frequency range of residual carrier frequency to estimate, i.e. from $-\Delta f$ to Δf with a step of one-thousandth of Δf, where Δf represents the value of the subcarrier spacing. For each of the frequencies in the search range, a compensation on the received signal is applied:

$$\hat{y}[n] = y[n]e^{\frac{-j2\pi n\varepsilon}{N}}. \tag{6.30}$$

Then a correlation between the corrected received signal $\hat{y}[n]$ with a shifted and conjugated version of the reference signal $\mathbf{s}[n]$ is computed. Note that n is the discrete-time in samples. The resulting correlation is defined by:

$$R_{ys}(\tau) = \sum_{n=0}^{N+N_{CP}-1} \hat{y}[n]s_c^*[n-\tau], \tag{6.31}$$

where $s_c[n]$ is a circular shift of the local replica waveform resulting in a matched filter of the OFDM signal. The process is repeated for each set of frequencies in the search range. The estimated time offset is the position of the peak of correlation.Then, the coarse frequency offset is chosen to be the one that gives the strongest correlation values after correction. The estimated delay can be expressed as:

$$\hat{\tau} = \arg\max_{\tau}\{|R_{ys}(\tau)|^2\}. \tag{6.32}$$

A data interpolation is performed in order to make a fine estimation of time and frequency offset around the coarse estimation value. The accuracy of the carrier frequency offset estimation is limited to the subcarrier spacing.

6.4.3 Frame synchronization

Once the time and frequency offset compensation is applied, frame synchronization to detect the start of the frame is carried out. Frame synchronization is essential because the transmitting process uses parallel-to-serial conversion to send symbols through the channel. Conversely, at the receiver, symbol samples arrive sequentially. As OFDM operates in frames, the receiver needs to gather a set of OFDM symbols to perform demodulation. The technique used here involves incorporating pilot signals generated in a local replica as markers for the start of frames. These pilots, exhibiting unique correlation properties in the time domain (i.e. high correlation peak when the replica frame is aligned with the received frame and low correlation peak for the rest of unaligned sequences), enable the OFDM receiver to detect the frame beginnings accurately. Therefore, the receiver capitalizes on this correlation pattern by cross-correlating the incoming sample stream with the local replica sequences (similar to formula 6.31), generating prominent peaks. These peak patterns serve as indicators to estimate the starting position of the frame, which dictates the alignment of the FFT window in the receiver with the useful part of the OFDM symbol.

When the estimated time offset is negative, meaning that the received signal at the RF channel has arrived earlier compared to the local replica, the $\Theta_{\hat{\tau}}$ samples of the first frame are discarded so that it is situated at the beginning of the frame. Otherwise, when the time offset is positive, meaning that the local replica has arrived earlier than the received stream, the frame is situated $\Theta_{\hat{\tau}}$ samples after the beginning of the received stream.

At the end of the process, the compensated received stream at i-th RF channel has the form:

$$y'^{(i)}[n] = \mathbf{y}[n + \Theta_{\hat{\tau}}] \cdot e^{-j2\pi n \frac{\varepsilon}{N}} \cdot e^{-j\Phi'} + w[n]. \tag{6.33}$$

Note that the RF channel error calibration and synchronization errors have been compensated to the received waveform.

6.4.4 Residual carrier frequency offset estimation

Even after synchronization (explained in Subsections 6.4.2, 6.4.3) and RF channel error compensations (explained in Subsection 6.5.1), timing errors or synchronization inaccuracies can cause the receiver to sample the signal at slightly different instants than intended, leading to a perceived frequency offset. This leads to the residual CFO, which can impact signal demodulation accuracy. Therefore, additional phase offset compensation is done to ensure reliable data recovery and therefore an accurate calibration computation.

Thus, at the receiver side, after synchronization, an N-point Discrete Fourier Transform (DFT) is applied after the removal of the CP. The resulting i-th received signal after demodulation, at the l-th symbol and k-th subcarrier is written as:

$$Y'(l,k) = H(l,k) \cdot b(l,k) \cdot e^{j\theta_{offset}(l,k)} + w(l,k), \tag{6.34}$$

where $H(l,k)$ is the channel response, $b(l,k)$ is the complex-valued symbol transmitted, $\theta_{offset}(l,k)$ is the residual phase offset at the l-th OFDM symbol and k-th subcarrier, and $w(l,k)$ is thermal noise, which is statistically uncorrelated with $w(l,k) \sim \mathcal{CN}(0,\sigma_W^2)$.

The residual carrier offset can vary with the subcarrier due to several reasons such as:

- **Channel effect**: The channel can introduce frequency-selective fading, causing different subcarriers to experience varying degrees of attenuation and phase shift.
- **Channel Delay Spread**: Different subcarriers can experience different levels of delay spread, which is the spreading of the signal in time due to multipath propagation. This can result in different subcarriers having different phase shifts.
- **Synchronization Errors**: Errors in timing and frequency synchronization during signal reception can also contribute to phase shift variations among subcarriers.
- **Interference**: In some cases, interference from adjacent subcarriers can affect certain subcarriers more than others.

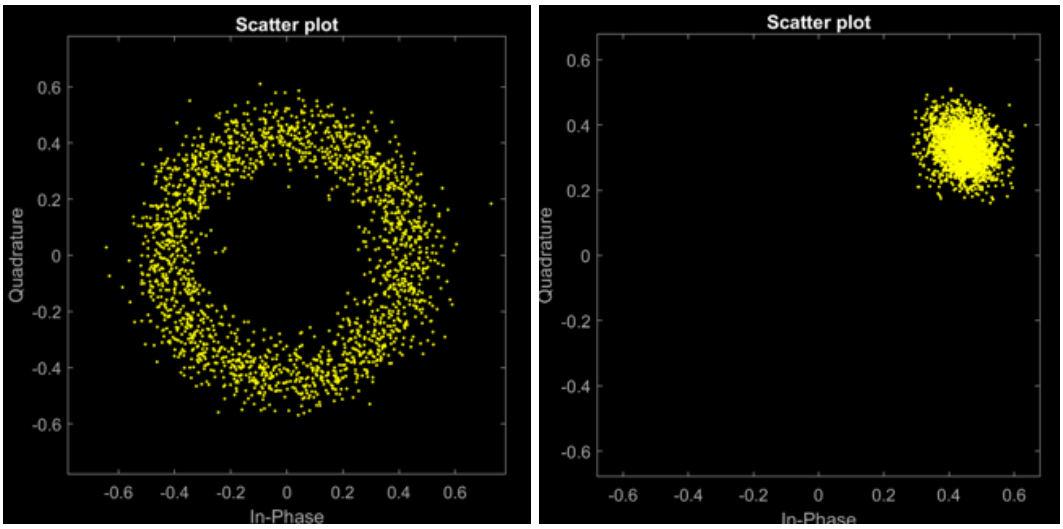
Because of the variation in subcarriers, the phase shift estimation is done per subcarrier during the whole reception time. It requires knowledge of the pattern of the 5G NR uplink signal SRS so that the estimator can collect the received symbols of a frame where SRS pilots are encountered. Note that in this work, 4 OFDM symbols of a frame of 14 OFDM symbols contain SRS pilots, that are streamed periodically to the RF channels. Recall that 4 is the maximum number of OFDM symbols per frame according to the standard as explained in Chapter 2. For each of these OFDM symbols, the received pilots of each subcarrier during T time duration are multiplied with the complex conjugate of the corresponding local replica. It aligns the subcarriers closely together and keeps only the effect of the phase shift, making it easier to perform accurate channel estimation and equalization since the impact of subcarrier spacing is removed. Since a four-element array antenna is used at the receiver, the phase shift for each subcarrier (see 6.35) will be estimated to the first RF channel receiver and then applied to the rest of the RF channels so that the delay between channels is maintained. After DFT, the pilot symbols of the SRS are first wiped off as:

$$R(l,k) = Y'(l,k) \cdot b^*(l,k), \tag{6.35}$$

where $b^*(l,k)$ is the conjugate pilot. The process is repeated for each RF channel receiver. The residual phase offset of first RF channel at the k-th subcarrier during the reception time is computed as:

$$\theta_{\text{offset}}(l,k) = \angle R(l,k). \tag{6.36}$$

The computed phase offset is then applied to the corresponding subcarriers of the rest of the RF channels and the compensation result is depicted in Figure 6.7. Moreover, the phase difference between channels is computed by having the first channel as a reference. This is explained in Subsection 6.5.2 and will correspond to the manifold mismatch that will then serve as calibration measurement for AoA estimation.



(a) I/Q samples with phase offset (b) I/Q samples with phase offset compensation

Figure 6.7: Constellation diagram: Residual carrier frequency offset estimation and compensation.

6.5 Calibration

The critical nature of radio direction finding in high-accuracy position and orientation estimation in 5G systems makes phase coherence a prerequisite for antenna array-based AoA estimation [69]. However, achieving precise angular estimation is challenging due to hardware impairments experienced by the multiple RF chains of the receiving SDR device responsible for processing the signal [70, 71]. As stated at the beginning of this chapter, both hardware and antenna-related factors contribute to offset errors, including clock stability, synchronization issues, and phase misalignment between channels, which pose a considerable challenge. Moreover, manufacturing inaccuracies, temperature variations, and mismatches with the ideal antenna array model [72] aggravate the problem. Additionally, the radio environment introduces its own set of issues, such as multipath and interference, along with misalignment in the frequency and time domain adds to the challenges of achieving accurate AoA estimation. Therefore, in this section, we report a comprehensive exploration of two fundamental calibration procedures: RF channel error calibration, described in Subsection 6.5.1, and antenna error calibration, presented in Subsection 6.5.2. Both calibration processes are crucial in achieving reliable angle estimation accuracy.

The RF channel error calibration addresses the critical need for coherent phase reception across multiple RF channels within an SDR device. Given the aforementioned hardware-related impairments, ensuring phase coherence among RF channels in USRP-based systems proves to be a nontrivial task, lacking comprehensive documentation even within SDR user manuals. While some existing contributions do acknowledge this issue [73], [74], [75], [72], they often provide limited practical insights into tackling this challenge. The objective here is not only to explain RF channel calibration presented in 6.5.1.2 for the receiver platform, but to extend this understanding more broadly, by presenting a set of invaluable guidelines to achieve coherent phase reception across multiple RF channels within an SDR device outlined in 6.5.1.1. The focus will be placed on USRP devices, and in particular, on model X300 equipped with two TwinRx daughterboards [76], model N310 [77] and model NI-2955 [78]. The last two: NI-2955 as a receiver and N310 as a transmitter will be used for the experimentation in the rest of

the chapter. Note that the two USRP models are chosen because they allow to use of the sampling rate and bandwidth needed for the generation of SRS used for the experimental part to be presented in Section 6.7. All three USRP boards are widely adopted for medium- to high-end applications necessitating two to four receive channels operating at high sampling rates, and therefore, the guidelines to be provided here are of utmost interest to a wide range of researchers. The discussion encompasses an analytical model of time, frequency, and phase error followed by a comparative analysis highlighting the benefits and limitations of three SDR models. The main focus lies in addressing the issue of phase synchronization, a critical factor that significantly impacts the accuracy of the AoA estimation setup.

In practical array processing applications, using ideal array steering vector models often leads to performance degradation and sub-optimal results for optimal array processors [79]. The accuracy of the employed array model, rather than measurement noise, is known to be the limiting factor affecting the performance of high-resolution array processing algorithms and related theoretical bounds [79, 80]. Similarly, using incorrectly specified sensor array models can result in severe performance losses in angle estimation techniques, leading to issues like steering energy towards unwanted directions, cancellation of the signal of interest (SOI), and amplification of interfering sources [81]. To overcome these limitations and ensure the precision of angular measurements, the antenna error calibration process comes into play to be presented in Subsection 6.5.2. This process enables the acquisition of realistic array steering vector models, taking into account various array nonidealities such as mounting platform reflections, errors in element positions, as well as gain and phase uncertainties arising from hardware and antenna-related issues. The central focus is on using array calibration measurements to obtain the array response, including its nonidealities. The calibration of the antennas is composed by two methods: an In-Situ calibration method [82] (see 6.5.2.1), where transmitters are used with a known direction to calibrate the antennas, but no propagation condition is known and in a controlled environment, one devoid of multipath propagation and interference, i.e., a dedicated measurement chamber (see 6.5.2.2). The In-Situ calibration is conducted in an indoor environment, whose calibration data will be tested in an indoor scenario presented in Subsection 6.7.2 and the anechoic chamber calibration data will be used for an outdoor scenario described in 6.7.3. It is worth noting that while array calibration measurements themselves may not yield an explicit formulation outlining the array's response as a function of wave-field parameters, the application of proper calibration and error correction techniques empowers array processing methods to leverage an accurate model of the real-world array response. This, in turn, augments the performance of high-resolution direction-finding algorithms.

6.5.1 RF channel error calibration

This subsection describes the process of RF channel calibration focusing on the challenging problem of achieving coherent phase reception between the RF channels. Additionally, experimental calibration and performance evaluation of it is presented in Section 6.5.1.3.

6.5.1.1 USRP main configuration features

The main features of the three USRPs under analysis (model X300 equipped with two TwinRx daughterboards [76], model N310 [77] and model NI-2955 [78]) are discussed and evaluated based

on their hardware capabilities in terms of performance, environmental application requirements, maximum sustained data rate throughput (that depends as well on the communication interface), etc. Moreover, an analysis of the available software environment to program the USRPs, as well as the configuration process to enable the LO sharing capability are covered. Before going into details, a summary of the main features of each considered USRP is presented next in Table 6.4.

Table 6.4: USRP main features comparison

USRP Model	**N310**	**X300-2TwinRx**	**NI-2955**
Selected connectivity [Total throughput] <Per channel >	2 x 10 Gb Ethernet [1600 MB/s] <100 MS/s >	2 x 10 Gb Ethernet [1600 MB/s] <100 MS/s >	MXIe [800 MB/s] <50 MS/s >
Sampling rate options	Even or odd division from three master clock options (in MS/s): 153.6, 125 and 122.88	Even or odd division from a master clock of 200 MS/s	Any value between 0 and 100 MS/s
Preferred environment	Linux OS (Ubuntu) UHD functions GNU radio	Linux OS (Ubuntu) UHD functions	Windows OS LabVIEW
Other relevant aspects	The 4 RF inputs can be configured as transmitter channels	Modular architecture	Accurate factory calibration

1. **USRP connectivity for maximum throughput**

   The throughput limit of the communication link between the USRP and the controlling personal computer (PC) becomes one of the main bottlenecks preventing us from reaching the maximum data rate. In the following, two main alternatives are considered to overcome this problem. The first one is to employ a four-line MXIe 1st generation cable connecting the USRP to a PCIe card at the PC. This approach can achieve a sustained transmission rate of 800 MB/s, which corresponds to an incoming sample rate of 50 MS/s per each of the four considered channels when dealing with I/Q data stream (interleaved I/Q samples) of 2 bytes (16 bits) per I/Q samples. The second alternative is to employ two 10 Gigabit Ethernet cables connected through dual SFP+ ports for establishing the connection between the USRP and the PC. This approach allows a combined transfer rate of 1600 MB/s corresponding to an incoming sample rate of 100 MS/s per channel under the same conditions. This option has a rate, which is double concerning the former one.

   Two of the selected USRP under analysis, the NI-2955 and the X300-2TwinRx, allow the use of both connections. However, at the time of the experimentation, the solution to utilize the 10 Gigabit Ethernet on NI-2955 required burning the NI-2955's FPGA image into an Ettus equivalent version. This means virtually converting the device into an X310-2TwinRx equivalent and consequently losing all the dedicated features and drivers provided by NI. The N310, instead, has only dual SFP+ ports for a 10 Gigabit connection each. Therefore, for the reasons mentioned, the recommended connectivity for maximum data throughput is an MXIe cable for the NI-2955 and two dual 10 Gigabit Ethernet cables for either the X300-2TwinRx or N310.

   Apart from using high throughput connections, high CPU clock rates, memory bandwidth, and I/O bandwidth, some additional parameter configurations are needed to ensure getting the most of the USRP host performance:

   - A Linux low-latency kernel is needed if real-time computations with very low tolerance

to delays are required to be performed.

- The CPU power management needs to be configured by disabling Hyper-Threading and thus increasing the single-core performance at the cost of having fewer core threads. Moreover, other power management functions such as sleep states and CPU frequency scaling should be disabled as well.
- The CPU frequency should be set to the highest value within the range of its scaling limits and enable the performance option of the CPU governor through the Linux utility *cpufrequtils*. Through these power schemes, it is possible to determine the desired frequency for the CPU and achieve maximum performance.
- The thread priority of the USRP Hardware Driver (UHD) software should be set to the highest scheduling priority.
- The Ethernet interface has its sub-net, and the corresponding USRP device should be assigned an address in that sub-net. The maximum size of the socket buffers to avoid potential overflows and underruns at high sample rates should be increased. The size of the buffer depends on the SDR model's recommendations. The following commands can be used:

  sudo sysctl -w net.core.rmem_max=sizeSocketBuffer

  sudo sysctl -w net.core.wmem_max=sizeSocketBuffer

- For the case of Ethernet 10 Gb interface, prevent flow control errors at higher rates by increasing the Ring Buffers on the Network Interface Card (NIC) using the following command:

  sudo ethtool -G <interface> tx sizeRingBuffer rx sizeRingBuffer

- To achieve maximum performance, the Maximum Transmission Unit (MTU) should be set to 9000 for 10 GigE and 1500 for 1 GigE. It is possible to use smaller MTUs, but this can affect performance. Setting the MTU size is done using the following command:

  10 GigE: *sudo ifconfig <interface > mtu 9000*

  1 GigE: *sudo ifconfig < interface > mtu 1500*

Note that the above-mentioned commands are compatible with the Linux operating system. For other operating systems, these commands should be substituted with the corresponding version. The tuning process is needed only for the case of Ethernet interfaces while for the MXIe interface is sufficient to fulfill the installation steps.

2. **USRP clock set-up**

The USRP series generates a master clock on the motherboard, which is then used to drive the ADC, Digital-to-Analog Converter (DAC), and the radio blocks. The clock rate is referred to as the "master clock rate". There is always a single master clock rate per motherboard. This rate is also the base sample rate of the radio blocks. Knowing the master clock rate, the actual sampling rate available can be an integer divisor of the master clock rate. The USRPs under analysis sustain different master clock rates. In general, the X300 series supports a 200 MHz and a 184.32 MHz master clock rate, with 200 MHz being the default one. However, X300-2TwinRx only supports 200 MHz, since

putting TwinRx locks the clock rate to 200 MHz. The N310 series support master-clock-rates: 122.88 MHz, 125 MHz, 153.6 MHz and NI-2955 supports a master-clock-rate of 200 MHz. Moreover, the X300-2TwinRx and NI-2955 are a 4-channel receiver while N310 is a 4-channel transmitter/receiver.

The transmission and reception of data depending on the master clock rate, transmission rate, and reception rate is not always possible. When working at higher rates, a high number of dropped samples, overruns, transmit and receive sequence errors and underruns may occur. Another common error that can be faced is that the receive packet handler fails to time-align packets. Even though several packets can be processed by the handler, a timestamp match cannot be determined. Note that only strict integer decimation and interpolation are used within USRP hardware to achieve the desired sample rate where the ratio *master-clock-rate/desired-sample-rate* should be an even integer ratio. For the rest of the sample rates where the ratio is odd, the performance of the USRP is not guaranteed, especially when phase-coherent operation among channels is required. In this context, NI-2955 provides a re-sampling process that allows to use of a wide range of sampling rates and, compared to the other USRPs under analysis, it gives better flexibility for applications where the sampling rate of signal to be streamed is a key factor.

Additionally, the sampling rate is closely related to time alignment and depends also on phase alignment. The received signals at all front ends should be sampled at the same time instance. All USRP models include options for using an internal or external clock reference with the added ability to export the clock reference and time base. For the external part, they accept a 10 MHz reference from which the ADC/DAC clocks and local oscillator are derived. When the internal clock of the USRP itself is used, a frequency accuracy of 2.5ppm is obtained. A common reference clock that can be used also by the USRP is PPS, a standard pulse per second port, or a general-purpose digital trigger input line. Additionally, the USRP NI-2955 includes a precision GPS-Disciplined OCXO (GPSDO), which provides improved frequency accuracy without using GPS and significantly improves frequency accuracy when disciplined to the GPS satellite network.

3. **USRP software environment**

USRP is controlled through the UHD support, which is an open-source software compatible with a large number of supported development frameworks, reference architectures, and open-source projects. The UHD architecture provides all the functional blocks for digital down-conversion and up-conversion, fine-frequency tuning, and other Digital Signal Processing (DSP) functions allowing it to be interchangeable with other USRP devices. UHD is supported by multiple signal processing software, like GNU Radio, LabVIEW, and Matlab. They support both operating systems: Linux and Windows. GNU Radio [58] is an open-source software package compatible with various SDR platforms. It provides solutions for developing wireless protocols at the PHYSICAL and DATA LINK layers of the protocol stack. The software is primarily written using Python, while performance signal processing blocks are implemented in C++. These blocks are basic operation units that process continuous data streams and can be connected to form a flow graph.

LabVIEW is also a flexible software platform that is compatible with USRP, especially with NI devices, where dedicated drivers code examples, and templates are available. In our analysis, NI-2955 is operated under this environment. To reach the maximum throughput,

two important modifications are required to be applied to the default templates for data acquisition: (1) the block diagram must follow a producer/consumer architecture, where the block that gets data from the USRP and the block that writes this data into the output file are located in parallel working threads (the data transfer between them is managed by a queue); and (2) the data samples have to be kept in their original 16-bit format (short integer) instead of being converted into a 64-bit format (double), as it is done by default.

Every development tool selected can run independently from the other (e.g. MATLAB for signal modeling and GNU Radio for USRP handling) or they can interact with each other (e.g. LabVIEW controlling the USRP while making MATLAB calls for data processing). Matlab has also its hardware support baggage, which can communicate with USRP. All the software drivers must be installed and configured in the host computer following the step-by-step installation guide. It is recommended to use the latest stable version of UHD that is available.

6.5.1.2 USRP RF and clock calibration

RF calibration plays a fundamental role in enhancing the accuracy and reliability of AoA estimation systems, especially in scenarios where multiple antennas are utilized to determine the direction of the signal arrival. It involves compensating for hardware imperfections in the RF front-end components. For this reason, here the focus will be specifically on achieving synchronization of channels in phase and time, as it significantly impacts AoA estimation accuracy. Different USRP models require distinct processes. They are explore below by providing a comprehensive guide on achieving phase alignment between channels.

1. **N310 calibration**

   N310 has built-in calibration procedures that can be enabled from UHD. The applicable calibrations for N310 can be enabled/disabled at initialization time using the *tracking_cals* and *init_cals* device arguments, i.e. command keys recognized by the UHD drivers. The device can be set to the precise bit mask the chip uses to set those calibrations (e.g., init_cals=0x4DFF,tracking_cals=0xC3) or they can use the following descriptive keys provided by UHD (e.g.init_cals=DEFAULT, tracking_cals=TX_QEC|RX_QEC), a preset for enabling most calibration's configuration. The | symbol can be used to combine keys (equivalent to a bitwise OR). Calibrations can significantly delay the initialization of a session. However, by only picking relevant calibrations, sessions can be initialized faster. Because the two draughtboards of N310 use different LO for references between the channels, the N310 itself has no way of aligning the phase between channels, and the phase will be random between runs. Therefore, to improve the phase alignment, it is recommended to apply an external LO source and split the signal source into the TX and RX, so that the phase ambiguity is reduced to ±180 degrees. Note that the external LO frequency must be twice the center frequency, which is therefore limited to the range from 300 MHz to 4 GHz. The N310 itself has inputs for external local oscillators, where for every daughter board, there is one input for TX and RX, respectively, resulting in 4 LO inputs total per N310.

   The phase alignment between channels through external LO, USRPs, is achieved by injecting a source signal from the external LO to the four TX/RX inputs of the N310 with

a 4-way splitter. The data streaming to the N310 device is run. Stream commands with a time spec property are used, which instructs the streaming to begin at the same time on all channels. Previously, an RF calibration [69] is performed by setting the necessary configurations defined in the device arguments property *–args*, a parameter that the UHD utility application uses to take the device address together with calibration settings. The following *init_cals* setting parameters to be used for the initial calculation are the ones that allow a minimal calibration:

- rx_lo_source=external,
- tx_lo_source=external,
- init_cals=BASIC|TX_ATTENUATION_DELAY|...
  RX_GAIN_DELAY|PATH_DELAY|...
  LOOPBACK_RX_LO_DELAY|RX_LO_DELAY|...
  RX_QEC_INIT|TX_QEC_INIT

Configuration parameters RX_QEC_INIT and TX_QEC_INIT require the external LO to be set to 5 GHz to perform the Quantum Error Correction (QEC) init calibration. Along with the above-mention parameters should be also set *force_reinit=1* and *tracking_cals=OFF*. The latter avoids the presence of frequencies that may distort the signal. The frequency value set is only necessary to perform calibration. After tuning the RF front-ends, the user can set the desired carrier frequency within the LO limited frequency range maintaining the same sampling rate and gain values with the calibration process and the same calibration settings as above without *force_reinit* argument. Each local oscillator may have a random phase offset due to the dividers in the VCO/PLL chains. This offset will remain constant after the device has been initialized until the device is closed or re-tuned. Thus, phase coherency is not repeatable after re-tuning or re-initialization of the device and the phases can suffer a 180° ambiguity. A phase re-calibration is required after these operations. Moreover, the quality of the onboard LO depends also on the external reference clock. By providing a custom LO signal, it is possible to increase accuracy assuming the externally generated LO signal is coming from a high-quality oscillator, and will eventually improve the phase noise.

2. **X300-2TwinRx calibration**

The TwinRX daughter board for the USRP X Series SDR platform is a two-channel superheterodyne receiver that can share the LO between channels across multiple daughter boards enabling the phase-aligned operation required to implement scalable multi-channel phased arrays. The antenna ports are MMCX connectors with 50Ω input impedance. By default Antenna 1 (RX1) is routed to Channel 1 and Antenna 2 (RX2) to Channel 2. This routing can be changed by swapping the antennas or sharing a single antenna between both channels (see Figure 6.8). Each channel of the TwinRx daughter board has two local oscillators, LO1 and LO2. The local oscillators of a channel can be sourced from the channel's internal synthesizers, the companion channel's synthesizers, or external inputs. The LO of each channel can be sourced as *Internal, Companion* or *External*. Therefore, to activate the sharing ability between channels, the configuration of calibration of each of the channels consists of *Internal, Companion, External, External* LO source respectively. The channel that has the property *Internal* will be the one that will serve as a reference and that will enable the capability to export its clock to the rest of the channels. The other channel

in the same daughter board will have the property *Companion*. The rest of the channels (in the other daughter-board) will be set to the property *External*, meaning that they will receive the reference from the other daughter-board. Apart from LO configurations, to synchronize the channels it is necessary to set the frequency using time commands. By using time commands, a timestamp will be set to make sure that the tune request is executed at the same time for all channels. This will ensure that the LOs of the X300 are returned synchronously on the same clock cycle therefore assuring phase coherent operation.

3. **NI-2955 calibration**

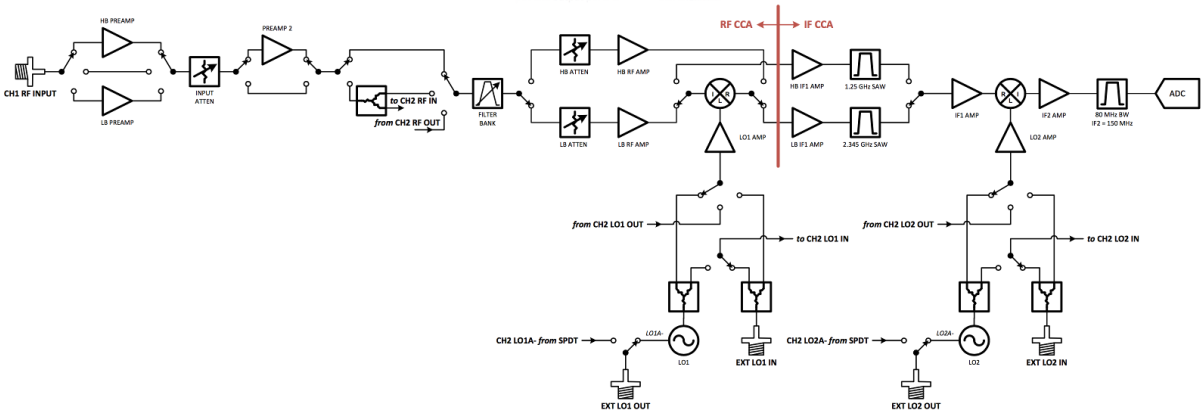


Figure 6.8: TwinRx block diagram. Image source: [76]

There are several possible LO configurations:

- *Independent*, where each channel will use its own LO, and the LO input ports will be disabled.
- *Import*, where channels will use the LO provided at the corresponding import ports.
- *Shared and Export*, where channels will use the same LO from the first channel, whose LO will be exported to their LO output ports.
- *Re-import*, where the LO from the first channel is exported and both channels will use the LO provided at the corresponding import ports.
- *Shared*, where both channels of the same daughter board will use the same LO from the first channel of the channel couple.

To achieve coherent phases among the four channels, two options are recommended:

- *LO-sharing*, where one pair of channels is configured with *Shared and Export* and the other pair is set to *Import*. Then, the LO signal from the first pair is injected into the other pair with external cables through the corresponding LO ports.
- *LO re-import*, where one pair of channels is configured with *Re-import* and the other is set to *Import*. The LO signal from the first pair is then amplified and shared among both pairs with external elements (cables, amplifiers, and power splitters). This mode offers maximum coherence between channels since it shares the same locally generated and re-imported LO signal.

For simplicity in the setup, the first option has been selected in our analysis and for the experimentation process later on.

6.5.1.3 USRP experimental calibration and performance evaluation

This subsection describes the experimental validation of the phase calibration that has been conducted on the testbed illustrated in Figure 6.2, which is built using the USRP SDR platforms addressed herein.

1. **Experimental setup**

   The calibration is done using two USRPs, one acting as a transmitter and the other one as a receiver as depicted in Figure 6.9. On the transmitter side, the USRP N200 [83] is used for periodic transmission of Gaussian pulses through its transmit RF port. The N200 has been deployed on a PC with an Intel i7-6700 CPU @ 3.4GHz and 16GB of RAM and an Ubuntu 22.04 LTS OS installed. The USRP is connected to the PC through a GB Ethernet cable. The transmit RF port of the USRP N200 is then linked to a four-port splitter to stream the Gaussian noise signal across all four RF channels in the reception section. The Gaussian noise signal has been chosen for the channel alignment and synchronization of the RF system due to its statistical properties and mathematical convenience. These statistical nature and wide-band characteristics make it easy to model and predict its behavior, which simplifies the synchronization process. Following the proposed configuration in 6.5.1.2, all phases should be aligned. However, it is essential to acknowledge that it is possible to use any signal limited to the capabilities of the chosen SDR model to generate said signal with the required sampling rate and bandwidth. For instance, recall that the Gaussian noise signal is used only for the experimental part of testing the phase coherence. For the rest of the work, the uplink NR signal SRS, described in Section 6.2, is used. On the receiver side, the USRPs N310, X300-2TwinRx, and NI-2955 are used for reception, one at a time. The USRPs N310 and X300-2TwinRx have been deployed on a PC with an Intel i5-9500 CPU @ 3GHz and 32GB of RAM and an Ubuntu 22.04 LTS OS installed. Both USRPs are connected to the PC through two 10 Gigabit Ethernet cables. The NI-2955 has been deployed on a PC with an Intel i7-10700 CPU @ 2.9GHz and 32GB of RAM and a Windows 10 OS installed that will allow the use of LabVIEW for the signal reception and enable the LO sharing capability explained in 6.5.1.2. The NI-2955 is connected to the PC through a four-line MXIe 1st generation cable. In all instances, the PCs utilized are equipped with Solid Stated Drives (SSD) NVMe-based of Category 3, which potentially achieve sustained writing rates above the data throughput of the two communication channels considered.

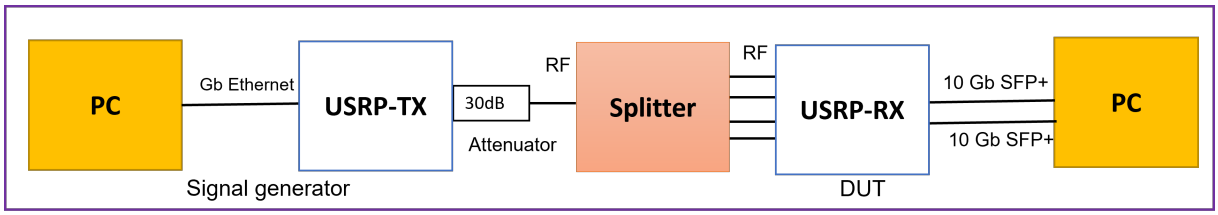


Figure 6.9: RF channel error calibration, where USRP N200 or N310 serves as TX and USRPs: N310, X300-2TwinRx or NI-2955 serve as RX. Note that, for the case of NI-2955, MXIe cables are used instead of 10 Gigabit Ethernet cables to connect with the PC.

Four experiments are conducted to perform phase calibration and evaluate its performance. One experiment for each SDR model NI-2955 and X300-2TwinRx; and two different experiments for the case of N310, one using the internal LO and the other using an external LO). For X300-2TwinRx and N310, two snapshots of 10 sec are taken in individual acquisitions within one power cycle. For the case of NI-2955, to achieve such interval recordings, the testing procedure works by acquiring small data segments of ∼20 ms every 200 ms, which represents a reduction of ∼90% of the total amount of data collected. Increasing these numbers fails our acquisition procedure. The main reason for such behavior is the limitation of Windows OS to perform high-demanding real-time operations. All experiments are repeated with the re-initialization of the device. For the case of N310, when using the external LO, a Valon 5009a Dual Frequency Synthesizer [84] module is used as an external LO that can work in a frequency range from 23 MHz to 6000 MHz.

Finally, the Gaussian noise signal is transmitted at a carrier frequency of 2.45 GHz, transmission gain of 20 dB, and sampling rate of 2 MHz. On the receiver side, the parameters used are given in Table 6.5. The gain values are set to avoid distortion of the signal and therefore this parameter is different for each of the USRPs under analysis.

Table 6.5: Experimental parameter configuration.

USRP	**X300-2TwinRX**	**N310**	**NI-2955**
Carrier frequency (GHz)	2.45	2.45	2.45
Sample rate (MHz)	50	61.44	50
Gain (dB)	60	40	40
Master clock rate (MHz)	200	122.88	200
I&Q samples (bits)	16	16	16
Nr. of power-cycles	2	2	2
Duration per power-cycle (sec)	20	20	20

2. **Performance results**

The experiments have been performed in conditions of CPU high performance achieved following the recommendations in 6.5.1.1. Results obtained from the measurements verify the performance of the LO-sharing synchronization for each of the USRP models. The phase difference between channels corresponds to the angle of the maximum peak of the cross-correlation between channels 1 to 3 with the first channel (0) taken as reference. Figure 6.10 presents the set of results to achieve synchronization between the SDR channels through the configuration of the LO to enable the sharing ability when using the USRP X300-2TwinRx. Even after power-cycling the system, the phase difference between channels is maintained constant. Apart from being phase-aligned, all channels are time-aligned as well. The distribution of the calibrated phase deviation of the channels shows that the maximum phase deviation is below ±0.08 degrees. There is a phase stability referred to as the averaged phase of all channels over the observed period. This constitutes the reliability of the system synchronization over time. However, to guarantee higher accuracy, it is recommended to perform phase calibration after some time.

Results depicted in Figure 6.11 are obtained when the USRP N310 uses its internal LO for the synchronization among channels. Because the first two channels use the same LO as a reference and the second two channels the same LO for reference but different from the previous ones, the phase deviation from the averaged phase differences is very small compared to the phase offsets between channels 2 and 3 having channel 0 as reference. This

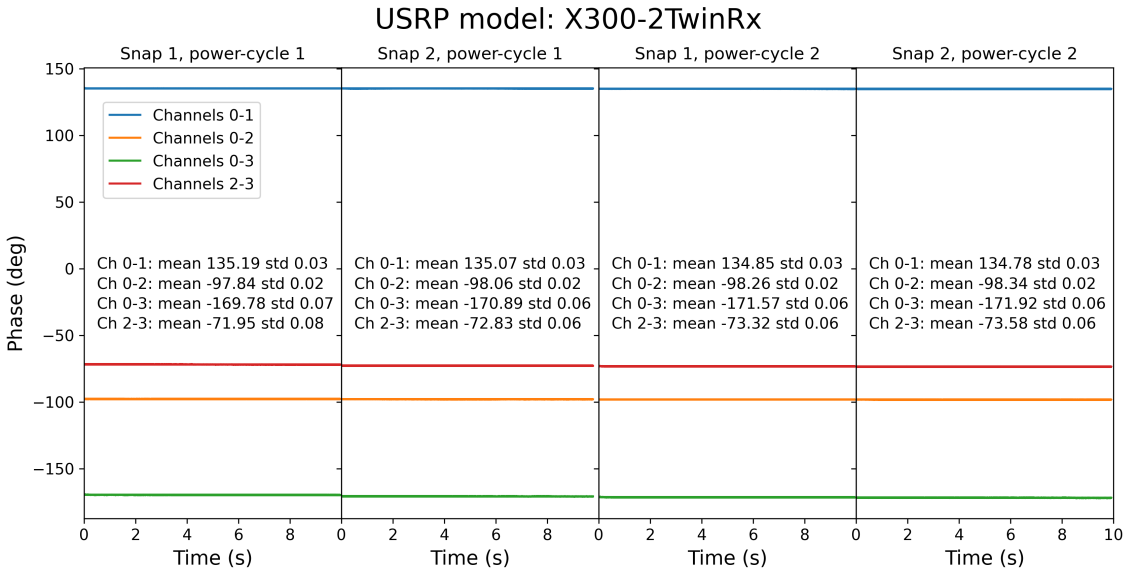


Figure 6.10: Phase coherence with X300-2TwinRx.

happens because the channels not sharing the same LO add different phase noise to the data by adding additional phase errors in the computation. The phase deviation reaches ±0.68 degrees, whilst the phase deviation stays below ±0.04 degrees when the same LO is shared. on the other hand, the phase difference among channels not sharing the same LO is not maintained constant during different acquisitions even after power-cycling the system. A better performance is achieved using an external LO. Results presented in Figure 6.12 show a decrease in the phase error at maximum with ±0.57 degrees. The phase difference between channels is maintained constant over time during the same power cycle. However, a phase ambiguity of 180 degree is applied. Therefore, it is recommended to perform phase calibration after every power cycle.

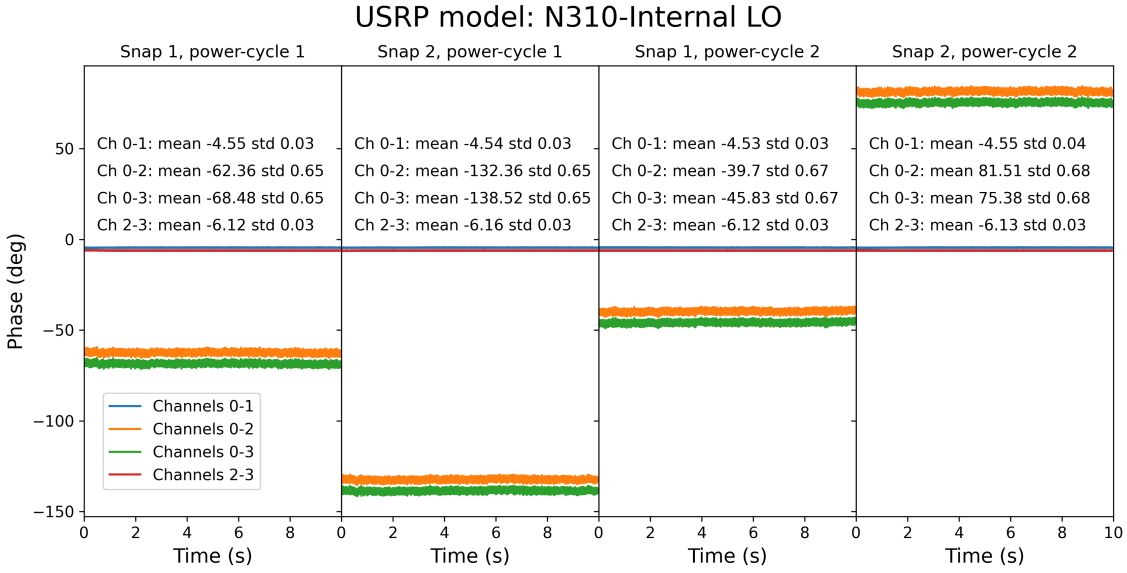


Figure 6.11: Phase coherence with N310 (internal LO).

Finally, Figure 6.13 shows that the phase deviation referred to the averaged phase of all channels in NI-2955 is below 0.12 degrees and it is maintained stable over time even after

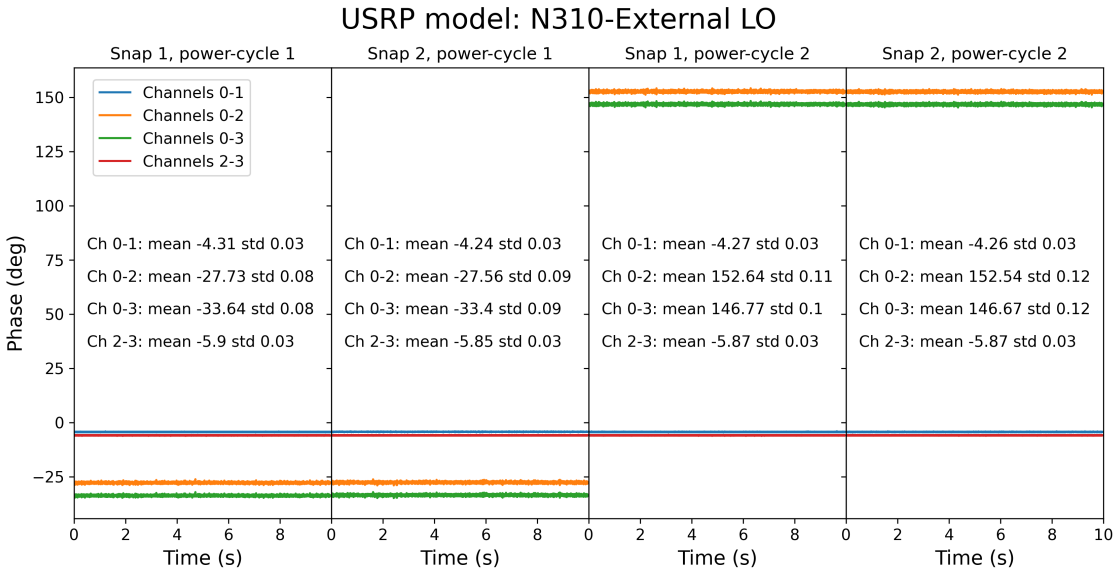


Figure 6.12: Phase coherence with N310 (external LO).

power-cycling the system. The results also show that the channels are aligned in time as well. However, it must be recalled that the dataset has not been acquired in a continuous and sustained manner (the gaps are not visible in the figure), as it was done for the other USRPs.

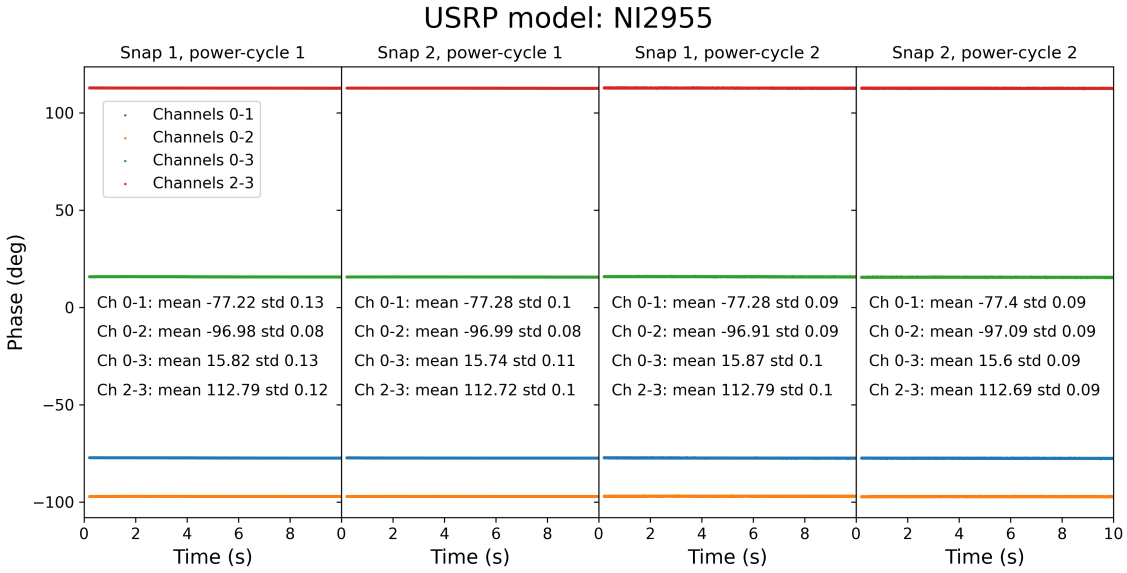


Figure 6.13: Phase coherence with NI-2955.

6.5.2 Antenna error calibration

Antenna calibration refers to the process of determining the antenna's response characteristics. This calibration typically occurs in a controlled setting, free from complications like multipath propagation and interference, often within a dedicated measurement chamber. Nevertheless, the antenna's behavior is also influenced by its surroundings. Therefore, to achieve a more

comprehensive understanding of the antenna's response, it is essential to conduct measurements in an environment that closely emulates real-world conditions. This approach, involving near-field measurement chambers, provides a more accurate depiction of the antenna's performance. However, it is worth noting that this method can be resource-intensive. Also note that in this work, the measurement will be conducted for far-field.

An alternative, practical, and cost-effective technique for antenna calibration is the In-Situ calibration method. In this approach, known-direction transmitters are employed to calibrate the antennas, though the propagation conditions are not fully characterized. While this method introduces factors such as mutual coupling [85] and errors in antenna element positioning, it is particularly suited for antenna arrays.

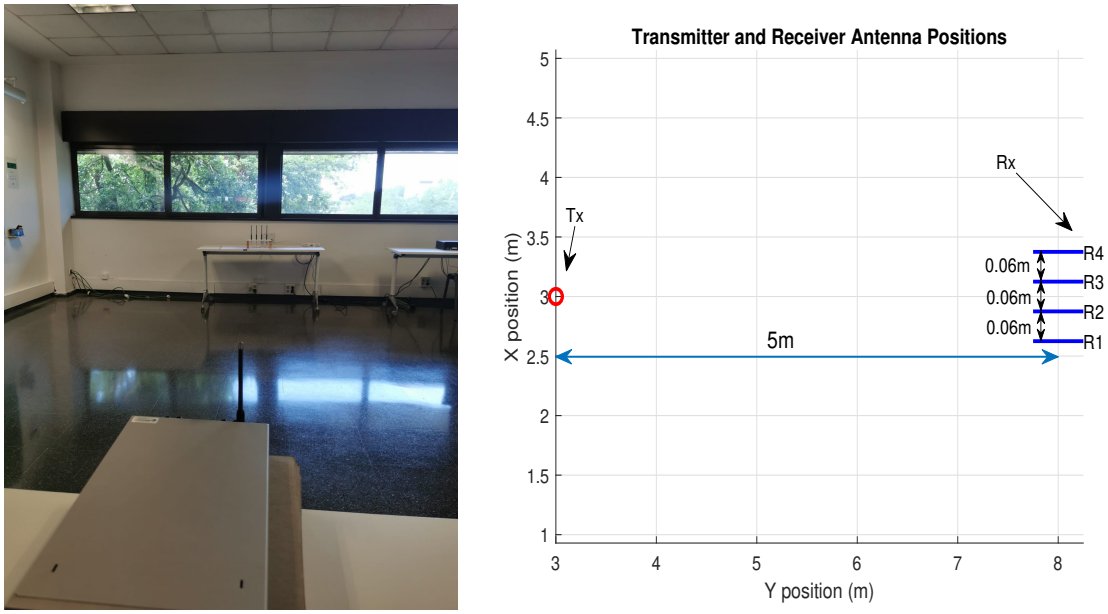
In contrast to the aforementioned technique, antennas can also be self-calibrated, simultaneously estimating the antenna parameters and the AoA. However, this approach it is not done often and it asks for specialized calibration environments. However, it comes with its own set of challenges, primarily stemming from the absence of precise antenna element identification and complete knowledge of propagation conditions [86].

Here, two of the above-mentioned methods: In-Situ calibration explained in Section 6.5.2.1 and calibration using an anechoic chamber explained in Section 6.5.2.2, are considered for the antenna error calibration. Both calibrations use a linear array antenna of 4 elements. The array modeling errors are based on calibration measurements. By array calibration, we refer to the procedure of correcting the assumed array response model for errors due to several imperfections. These can include gain and phase errors in the receivers, imbalance between the I and Q channels, an incorrectly specified mutual coupling model, and uncertain antenna element locations. First, we start by explaining the calibration process for both methods. Then, experiments where the calibrations are applied are presented. The In-Situ calibration is applied for an indoor scenario (see 6.7.2), that is carried out in the same environment as the calibration, while the calibration using an anechoic chamber is used in an outdoor scenario. The latter has been deployed considering two types of conditions: one in an Line of Sight (LoS) scenario and the other with the presence of a reflector placed in two different positionings: with the angle of arrival at 30° and at 45° (see 6.7.3).

6.5.2.1 In-Situ calibration

In-Situ calibration has been conducted in an indoor environment within a 56 m^2 empty laboratory space. This area is particularly chosen because of its environmental factors that can impact signal propagation. Moreover, this method is known for its effectiveness in addressing the challenges posed by harsh indoor conditions. A single transmitter and receiver were placed approximately 5 meters apart within this space (see 6.14(a) and 6.14(b)). The estimation of AoA is done by evaluating the phase offsets across receiving antennas. The receiving array elements (a ULA with a half-wavelength spacing) are swiveled within a specified sector coverage and a predefined angular step. The calibration was executed over a sector spanning 180°, corresponding to −90° to 90°, with a step of 5°, encompassing 37 pilot angles of arrival. Notably, the experiment's sector coverage aligns with the scenario in which the experiments were performed. The receiver is placed near the wall, at one side of the room, and the transmitter is placed 3 m away from the other side as in 6.14(b). To obtain different AoA, the array manifold at the

receiver side is swiveled. For each of the known AoA to estimate, after RF channel error (see 6.5.1), and synchronization error (see 6.4) corrections, the phase offsets caused by free-space propagation, i.e., $\phi = 2\pi d f_c/c$ for a given distance d between antenna elements at a specific carrier frequency f_c, are evaluated and compensated to the received data stream. The channel response of the array antenna at the receiver side is used to estimate the actual array manifold and compared with the true manifold $\mathbf{a}(\phi)$. The mismatch between manifolds (i.e., deviation of the actual manifold from the geometrical one) will serve as a reference metric for correcting the array response during the AoA estimation. The USRP-Tx N310 equipment, operating at a frequency of 2.4875 GHz, was utilized for signal transmission. The SRS signal is transmitted periodically every 1 millisecond during 2 sec. The system's parameters included a transmission gain of 65 dB and a sampling rate of 30.72 Msps, equating to a 25 MHz bandwidth with an FFT length of 2048. Both the transmitter and receiver employed identical omnidirectional monopole antennas. The transmission utilized a single antenna port on the USRP-Tx N310, while the receiver's antennas were positioned on a platform, spaced $\lambda/2$ apart.



(a) Environmental Layout (b) Experimental Setup

Figure 6.14: Set-ups for In-Situ calibration and AoA estimation experiments in a 56 m^2 room size. The X and Y positions in 6.14(b) correspond to the width and length of the room size respectively. The receiver is placed near the wall at one extreme of the room length and the transmitter is placed 3 m away from the other extreme of the room length (see 6.14(a), 6.14(b)). The Tx and Rx are placed within a distance of 5m and each antenna element on the receiver side has a spacing of 0.0603 m in between.

Finally, the calibrated array manifold $\hat{\mathbf{a}}(\phi)$ is used to delineate the true array response with the array error computed and corrected in the searching-based AoA estimation algorithms. The searching-based AoA estimation algorithm, e.g. MUSIC, beamforming, etc., can directly employ this calibrated array manifold. The calibrated array manifold can be expressed as

$$\hat{\mathbf{a}}(\phi) = diag(\zeta(\phi)) \cdot \mathbf{a}(\phi), \tag{6.37}$$

with $\zeta(\phi) = [1, e^{j\hat{b}_2}, ..., e^{j\hat{b}_M}]$ being the mismatch array error correction obtained from the In-Situ calibration process and $\mathbf{a}(\phi) = [1, e^{\frac{-j2\pi d \sin(\phi)}{\lambda}}, ..., e^{\frac{-j2\pi(M-1)d\sin(\phi)}{\lambda}}]$ being the theoretical antenna response where d is the antenna element distance. Then, dominant spectral peaks are used to

find the AoAs.

Two sets of measurements for each pilot angle of arrival are taken during calibration. One set is to be used for the antenna error calibration, and the other is to evaluate the AoA estimation performance under both calibrated and non-calibrated conditions presented in 6.7.2. Phase offsets between antennas were computed by averaging subcarriers with identical carrier frequencies. All experiments are carried out under LoS conditions. Because an ISM radio band is used for transmission, the presence of interference is inevitable. During the experimentation process, the presence of a signal at a center frequency of 2.479 GHz of 2 MHz bandwidth has been detected as depicted in Figure 6.15. To improve the resolution ability, interference correction is undertaken by choosing only the subcarriers that do not contain interference after the demodulation of the waveform.

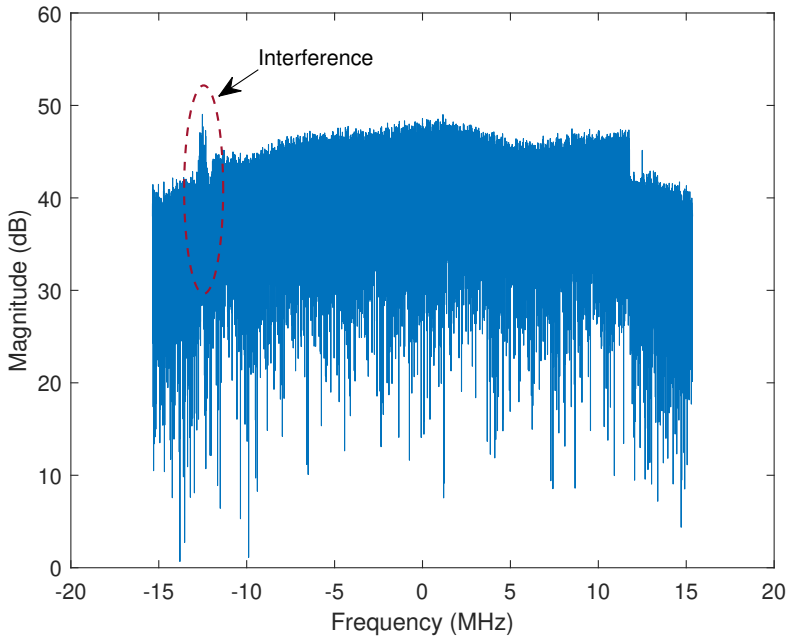


Figure 6.15: Example of the presence of interference in the received baseband signal.

The calibration results are depicted in Figure 6.16, where the theoretical array response corresponding to each incident direction is juxtaposed with the experimental array response and the computed array phase error deviation from the anticipated value. This deviation serves as a crucial parameter for rectifying phase errors originating from the antennas. These outcomes were derived after compensating for the phase offsets between channels stemming from the RF channels. Notably, the computed steering vector aligns closely with the behavior of the theoretical vector, accounting for an ideal antenna response.

6.5.2.2 Anechoic chamber antenna error calibration

In Section 6.5.2.1 it was shown that In-Situ calibration offers advantages in capturing real-world conditions, addressing interference and multipath effects, and being practical for indoor antenna arrays. However, the effectiveness of In-Situ calibration is confined to the specific environment in which it is carried out. Changes in the environment may affect calibration accuracy, making it less transferable to different settings. For this reason, in this part of the work, a calibration

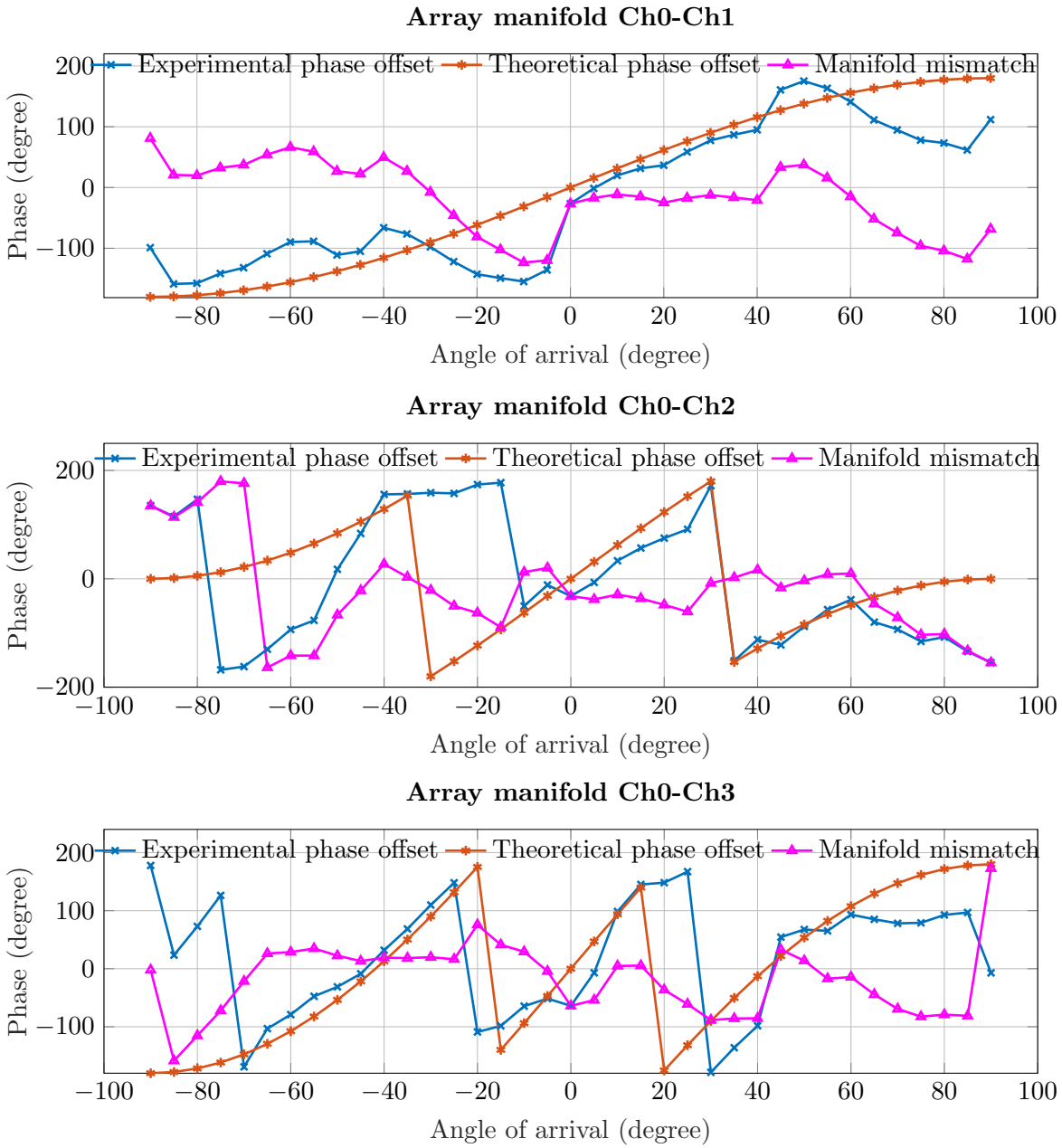
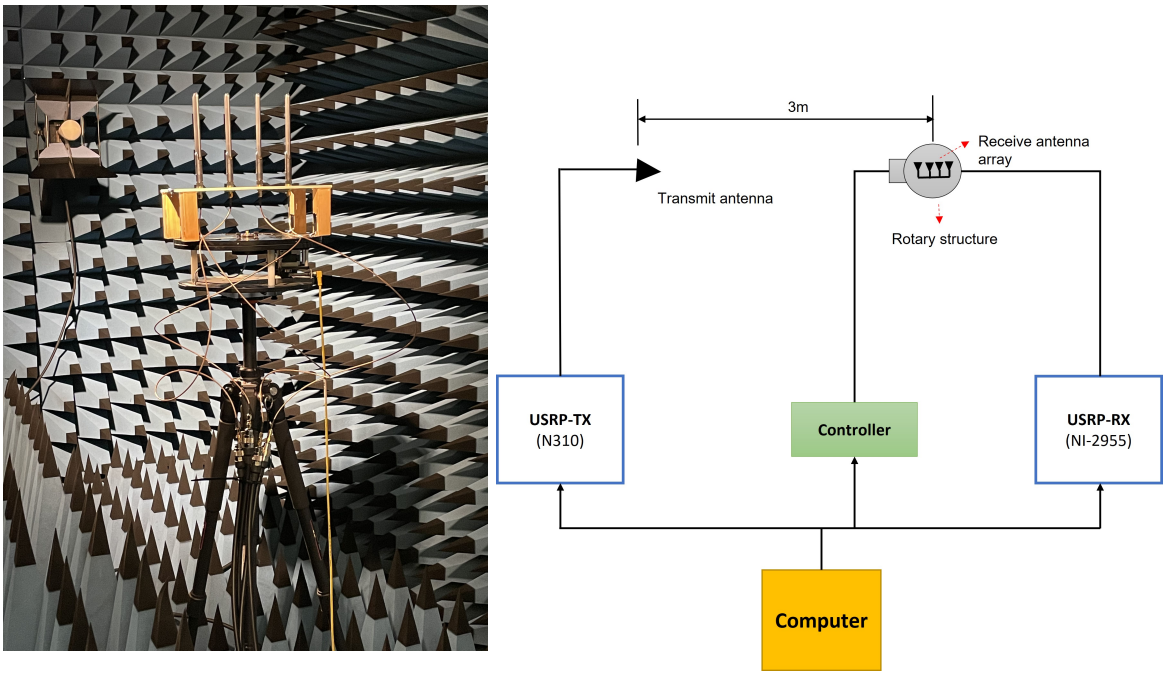


Figure 6.16: Ins-Situ Calibration: Antenna phase errors at the pilot direction of arrival.

process in a controlled environment such as an anechoic chamber is presented. Despite the environmental dependency, this method allows to minimize reflections and avoid interferences.

Similar to the In-Situ calibration, a linear array antenna placed in several known directions is used for the calibration in the anechoic chamber. The calibration range consists of a rotary stand where we mount the direction-finding array antenna along with the transmit antenna at a distance of 3 m as depicted in Figure 6.17(b). The angles to be used for the calibration are achieved by rotating the structure with small angular steps set to a controller program installed in the computer. The transmit power is set to the maximum output value +18 dBm so that the instrument noise does not influence the measurements. For each of the angular positions, the bearing errors $\Delta\phi_i$ are obtained from the difference of the estimated one $\hat{\phi}_i$ with the setting of the rotary stand ϕ_{pos_i}, so that we have $\Delta\phi_i = \phi_{pos_i} - \hat{\phi}_i$. To enable a dense calibration grid, a spline interpolation is used. Given an interpolated q($\hat{\theta}$) at a certain desired AoA θ,

the array response is then computed as done in 6.37 and depicted in Figure 6.18. Finally, the measured antenna signals are compensated with the estimated antenna errors similar to the In-Situ calibration process in Section 6.5.2.1. Recall that the calibration process has been performed after RF channel error compensation, carrier and time offset, and residual pilot carrier phase offset corrections as explained in Section 6.4 and Section 6.5.1. The calibration data will be later used in the outdoor scenario to be presented in Section 6.7.3.



(a) Environmental Layout (b) Experimental Setup

Figure 6.17: Antenna calibration using an Anechoic Chamber. A horn antenna is used as a transmitter for better antenna directivity and higher transmit power. The receiver is a four-element antenna array composed by monopole antennas and mounted on a rotary stand. Fixed angular positions are achieved by moving the rotary structure with small angular steps. The Tx and Rx are placed within a distance of 3m and each antenna element on the receiver side has a spacing of 0.0603 m in between.

6.6 Simulation results on time-delay, carrier frequency offset and angle estimation accuracy

Before going with the analysis of experimental part, it is worth analyzing the effects of the synchronization from the calibration process in terms of the estimation accuracy of AoA. Therefore, in this section, we will focus on the accuracy of carrier frequency offset estimation, time offset estimation, and angle estimation, which is also one of the main performance metrics in localization. The analysis presented in Subsection 6.6.1 is done through simulations for multipath-free environments and the antennas are considered perfectly calibrated. Moreover, since the presence of multipath and interference is inevitable in real scenarios, it is of interest to evaluate the angle estimation precision in such conditions by exploring the performance of several AoA estimation algorithms. The analysis presented in Subsection 6.6.2 has been done for the multipath environment to derive statistics of the angle estimation error.

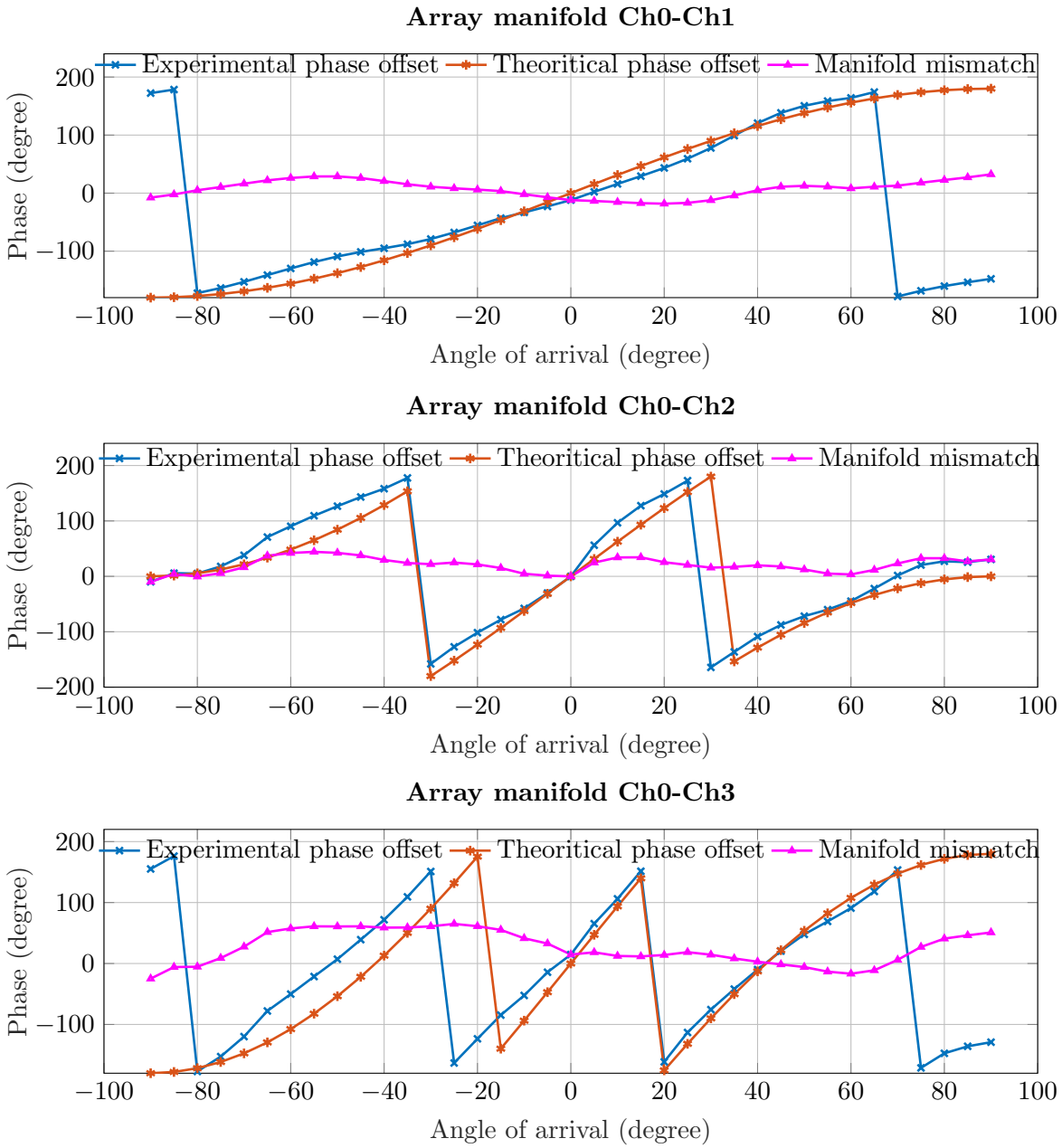


Figure 6.18: Anechoic-Chamber: Calibration: Antenna phase errors at the pilot direction of arrival.

6.6.1 Multipath free environment

In this subsection, Monte Carlo simulations are used to numerically analyze the statistics of error estimation in terms of frequency and time offset estimation to understand the impact of residuals after frequency and time synchronization in the AoA estimation. The idea is to explore the effect of error estimation because residuals remain after calibration for different Signal-to-Noise Ratio (SNR) levels. The CFO, time offset, and AoA estimation are compared with the corresponding Cramér-Rao Bound (CRB) derived as following.

- **CRB expression for time delay estimation**

  For this analysis, the CP is already removed in the previous stage. The SRS has been generated according to the high-level parameter configuration and mapped to the physical

resource unit as explained in detail in Chapter 2. Then, the OFDM baseband signal $x[n]$ of one symbol is implemented with the IFFT of the pilot symbols vector (without CP) defined as:

$$x[n] = \sqrt{\frac{C}{N}} \sum_{k \in N_a} p_k \cdot s_k \cdot e^{\frac{j2\pi nk}{N}} = \sqrt{\frac{C}{N}} e^{\frac{j2\pi nk_0}{N}} \sum_{k=0}^{N_a-1} p_k \cdot s_k \cdot e^{\frac{j2\pi nk}{N_a}}, \tag{6.38}$$

where C is the signal power, and s_k is the SRS pilot, k_0 is the index of the first subcarrier carrying SRS, $\mathcal{N}_a$ is the subset of active pilot subcarriers, N_a is the sthe total number of active pilot subcarriers, $p^2{}_k$ is the relative power weight of subcarrier k with $\sum p^2{}_k = N$. Having in mind that the OFDM symbol duration T_s is inverse to the subcarrier spacing Δf, i.e. $T_s = 1/\Delta f$ and according to general CRB derivation results of signals in Gaussian white noise given by Kay [87] and the derivation in [35], the CRB estimation of the delay offset is

$$CRB(\hat{\tau}) = \frac{6}{SNR \cdot N_{ant} \cdot N_{\text{OFDM}} \cdot N_a (N_a^2 - 1)(2\pi \Delta f K_{\text{TC}})^2}, \tag{6.39}$$

where SNR is the average SNR per resource element, N_{ant} is the number of the antenna element of the linear array, N_{OFDM} is the number of OFDM SRS symbols considered, and K_{TC} is the transmission comb number, in subcarriers, specifying the minimum frequency separation between two subcarriers that allocate SRS. Thus, the range estimation of CRB can be obtained as $CRB(R_{\text{r}}) = c^2 \cdot CRB(\hat{\tau})$ with c being the speed of light.

- **CRB expression for carrier frequency offset estimation**

  According to the theory on CRB [87], the variance of the ML estimate $\hat{\epsilon}_{ML}$ is lower bounded by:

$$Var(\hat{\epsilon}) \geq \frac{1}{-E\left\{\frac{\partial^2 \Lambda(y|\epsilon)}{\partial^2 \epsilon}\right\}}. \tag{6.40}$$

  For the traditional OFDM system, knowing the modulation symbols, the received signal can be expressed as

$$y_{l,k} = b_{l,k} \cdot e^{j2\pi K_{\text{TC}} k T_s \epsilon} + w_{l,k}, \tag{6.41}$$

  where $b_{l,k}$ is the transmitted symbol, T_s is the total duration of the OFDM symbol, $w_{l,k}$ is the AWGN with σ^2 variance and zero mean. The $\sigma^2{}_b = E\left\{|b_k|^2\right\}$ is the signal power and $\sigma^2{}_w = E\left\{|w_k|^2\right\}$ is the AWGN noise power. The evaluation of the second order differential of $\Lambda(y \mid \epsilon)$ and the derivation result for an OFDM system has been done based on [88]. So the CRB of the carrier frequency offset is

$$CRB(\hat{\epsilon}) = \frac{(1 - \rho^2)}{8\pi \rho^2 L}, \tag{6.42}$$

  where $\rho = \frac{\sigma^2{}_b}{\sigma^2{}_b + \sigma^2{}_w} = \frac{SNR}{SNR+1}$ with $SNR = \frac{\sigma^2{}_b}{\sigma^2{}_w}$ being the average SNR per resource element and L being the length of cyclic prefix. Because the CFO estimation is performed including the cyclic prefix (see 6.4.2), increasing its length, the CRB can be made arbitrarily small.

- **CRB expression for angle of arrival estimation**

  The CRB of the angle of estimation has been derived for a channel with only a LoS signal

based on the derivations presented in [35] as

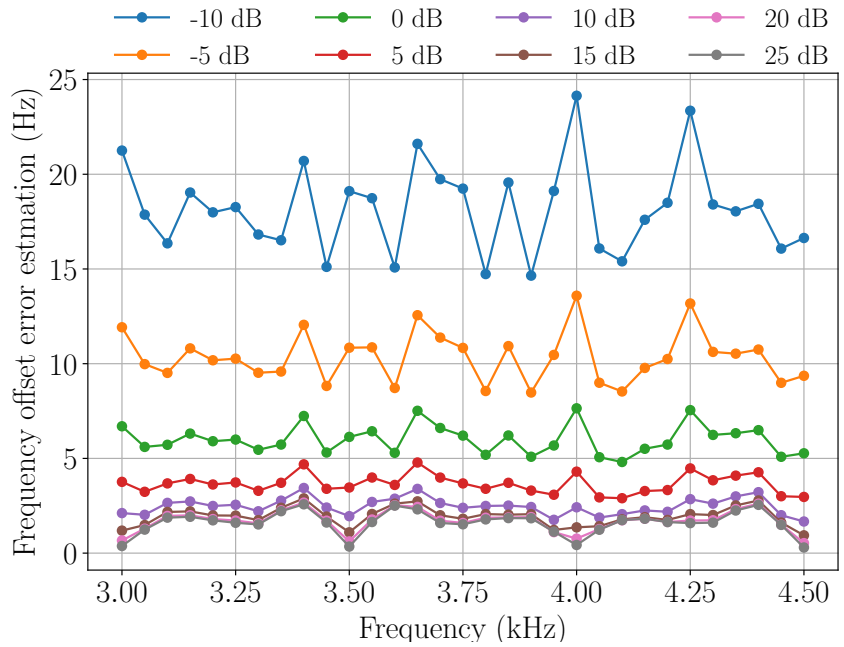
$$CRB(\hat{\theta}) = \frac{6}{SNRN_{ant}N_a(\frac{w_c d}{c})^2(N_{ant}^2 - 1)\sin^2\theta}, \tag{6.43}$$

where $w_c = 2\pi f_c$ with f_c being the carrier frequency. Note that increasing the number of antenna elements reduces the angle errors.

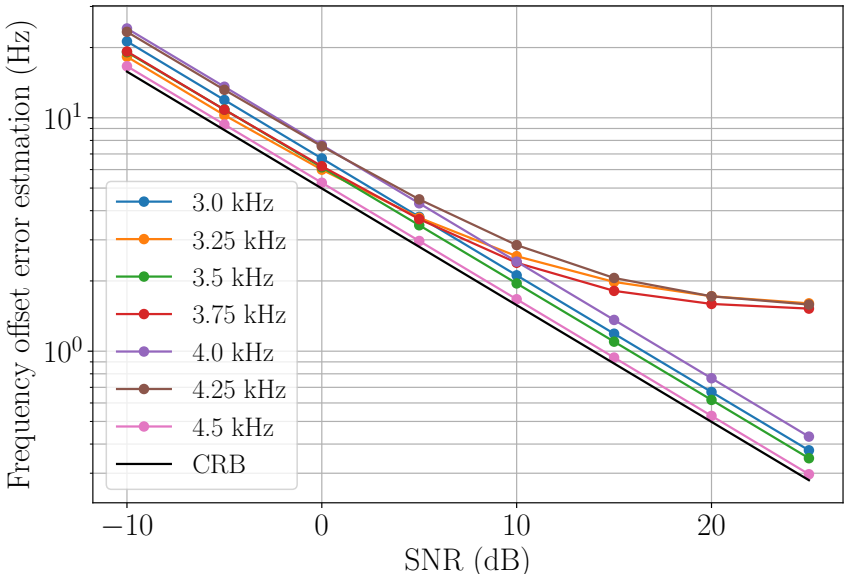
For the analysis, we consider the 5G uplink SRS signal composed by 4 SRS symbols following the configurations depicted in Table 6.1. Note that these specifications of the uplink 5G signal are the same for calibration, numerical analysis, and experimentation. A full-band SRS transmission has been used and a linear antenna array of 4 elements is considered. The phase offset introduced by the front-end hardware, where the first radio channel (Ch0) is taken as reference, is set as follows: $\Phi'_{Cho-Ch1} = \pi/3, \Phi'_{Cho-Ch2} = \pi/4, \Phi'_{Cho-Ch3} = \pi/6$. The carrier offset set is a fraction of the spacing between the subcarriers, a range from 3 kHz to 4.5 kHz in increments of 0.05 kHz. The time offset applied to the waveform is 0.97 ns and the direction of the angle of arrival to be estimated is set to 22°. For each carrier offset and SNR value (a range from −10 to 25 dB with a span of 5 dB), 30 realizations of the channel impulse response are generated, and frequency, time, and AoA estimation are performed. The range of carrier frequency offset is chosen because the coarse estimation has a searching accuracy of one-tenth of subcarrier spacing corresponding to 1.5 kHz step size as stated in 6.4.2. Therefore, for values between two search candidates with a distance of 1.5 kHz step size, it is important to see how accurate will be the estimation during the fine estimation process, as well as evaluate how the carrier frequency offset, within the chosen range, influences the accuracy of our AoA estimation.

The results obtained in Figures 6.19, in conditions of perfect antenna error calibration, show the Root-Mean-Square Error (RMSE) of the frequency offset estimation as a function of carrier frequency offset applied. It is seen that, when the frequency offset is within the frequency resolution, the method can distinguish the central maxima corresponding to the frequency offset target with an error estimation lower than 5 Hz for SNR greater than 0 dB and an error estimation greater than 10 Hz for low SNR. For the values in between, the estimation accuracy degrades with 1 Hz for high SNR and 6 Hz for low SNR. These results show an improvement of the performance for frequency offset estimation with the increase of the integrated SNR. It is also noted that, for frequency offsets in between the ones separated by the resolution distance of 1.5 kHz, the RMSE error for SNR above 20 dB is changing very slowly with an averaged error value of 1.5 Hz and the tendency is to keep it constant with the increase of SNR. This means that the carrier frequency offset resolution with a frequency distance resolution of 0.5 kHz reaches an estimation accuracy at a higher SNR. Therefore, to obtain a better frequency resolution, the offset distance should be in the range of Hz. For the experiments done in this part of the work that will be presented later on, a resolution of 10 Hz is considered. Note that this will lead to higher computation time.

On the other side, the estimation accuracy of time offset is reflected in the range delay and angle resolution depicted in Figure 6.20. Both range delay and angle resolution are compared with the corresponding CRB values. Note that the accuracy of carrier frequency offset explained previously has also affected in the results. The results show an improvement in estimation accuracy with the increase of SNR. Both results tend to follow the CRB graphs and even coincide at higher SNR. This means that in conditions of perfect antenna calibration and good



(a) Frequency offset error estimation for different carrier frequency offset.



(b) Frequency offset error estimation depending on SNR values.

Figure 6.19: Evaluating the accuracy of carrier frequency offset estimation.

estimation and compensation of RF channel errors when only one source is taken into account, even with frequency offset errors around 25 Hz, the algorithms can estimate the angle of arrival with resolution below 1 degree. These are promising results taking into account that an ULA array of 4 elements is considered, knowing that larger arrays will lead to better angle resolution.

6.6.2 Multipath environment

Real-world arrays may also be subject to nonidealities that change as a function of time or cannot be measured in controlled environments. For example, random fluctuations of the array

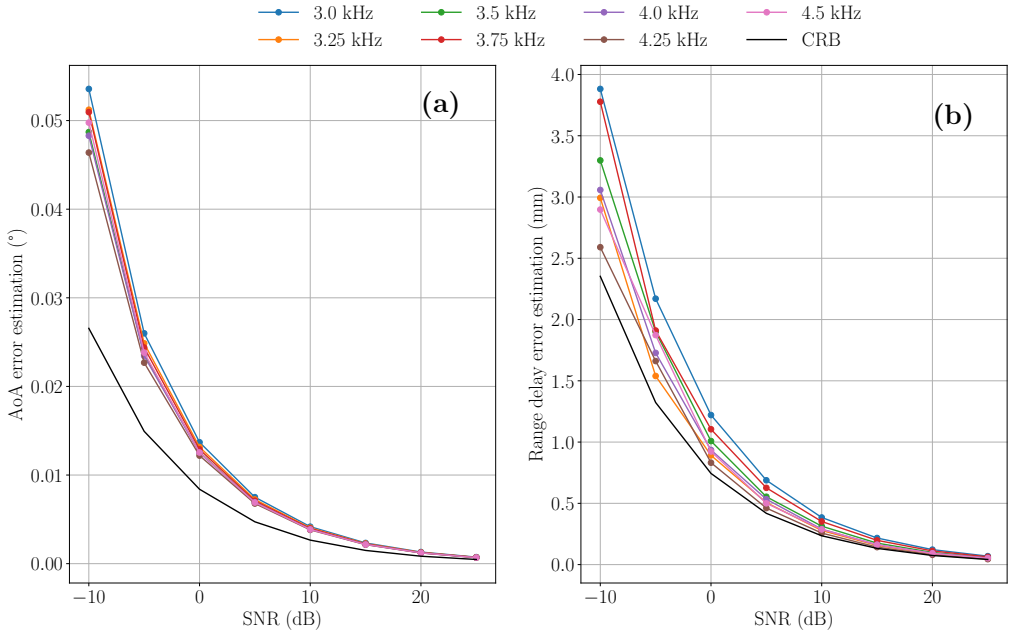


Figure 6.20: Evaluating the accuracy of time offset and angle of arrival estimation. In (a) it is presented the angle error estimation versus SNR values and in (b) the range delay error estimation versus SNR values.

response due to nearby scatters or the motion of the platform where the array is mounted are not captured in the calibration stage. In addition, imprecise knowledge of the AoAs may also lead to performance degradation of the angle estimation due to looking direction errors. This means that the system might not have accurate information about the angles from which signals are incoming. Therefore, this lack of accuracy can lead to errors in determining the direction of these signals. The consequence of this inaccuracy is a degradation in the performance of angle estimation. Therefore, here comes the need to use array processing techniques that are robust to general uncertainties in the steering vector of the real-world array. One persistent challenge is dealing with coherent sources. To address this issue, robust algorithms are needed to effectively handle multipath and coherent signals and successfully estimate the angle of arrival. In the context of AoA estimation, conventional subspace-based techniques such as MUSIC [89] and ESPRIT [90] have been widely used. However, coherent signals can cause these methods to perform poorly, as they lead to a rank deficiency in the source covariance matrix. Moreover, these techniques are only applicable when the number of antenna elements is greater than the number of incoming signals. These techniques require sufficient snapshots and high SNR to achieve high spatial resolution.

Having a large number of snapshots it is not always possible. It is an impractical choice, especially in a fast time-varying environment, where the construction accuracy of sub-spaces tends to deteriorate. In such conditions, even using array calibration, the subspace-based methods are incapable of guaranteeing accurate angle estimation when dealing with source coherence problems due to their sensitivity to subspace orthogonality. Various prior processing techniques, such as spatial smoothing [91, 92], have been used to decorrelate sources, but they often reduce the array's effective size. Alternatively, parametric maximum likelihood (ML) beamforming approaches offer robustness in the presence of coherent signals but require extensive knowledge of the scenario and involve complex optimizations, increasing computational demands.

Recently, to address these limitations, IAA [62, 93] rooted in sparse techniques have emerged as promising solutions. These algorithms efficiently handle various impairments, including coherent sources [91], array perturbations, and limited snapshots, and provide accurate AoA and signal power estimates. The iterative steps are based on the IAA covariance matrix, which can be singular in noise-free scenarios where only a few components of the signal power vector are non-zero. Additionally, they are computationally intensive due to scanning the entire visible region of the array. Thus, the performance of the power-based algorithms is mostly limited by the granularity of the grid size.

To further improve these problems, regularized versions and alternative algorithms like a series of iterative SAMV approaches [94, 95, 63] based on the asymptotically minimum variance approach have been proposed. These approaches can handle various scenarios, including situations with limited snapshots and a few non-zero signal power components. Additionally, SAMV-SML approaches [63] are introduced to enhance the direction grid's granularity. These techniques are extended to the time delay estimation in this work.

In this section, simulations to see the performance of the above-mentioned methods in conditions of multipath and coherent signals are carried out. These advancements in array signal processing are crucial for improving the accuracy of angle and time estimation of such scenarios. For the evaluation of the chosen methods, 50 Monte-Carlo trials for each SNR value of range -15 to 25 dB are considered. Two coherent sources are considered, where one is maintained fixed at a known angle of arrival ($0°$) with no time delay on the samples and the other with different angle and delay spread from short to long values. Both sources share the same phases. A $35°$ angle spread is used, such that the incoming signal will arrive from directions within a sector with a half-width of $35°$ centered around the reference direction. So, the range of possible angles could extend from $-35°$ to $+35°$ concerning that reference direction. The source waveforms are assumed to be identical for all two coherent sources. An ULA array of 4 antenna elements with half-wave-length inter-element spacing is considered and $N_{snap} = 63$ is the number of snapshots used for each of the estimation techniques considered for this part of the work.

The results have been grouped in different spread values as shown in Figures 6.21, 6.22. The first group has a maximum angle spread of $5°$ meaning that the distance to the reference (the LoS path) is from $-5°$ to $-5°$. The second group has a spread between $5°$ and $15°$, meaning that the path direction can be both the negative and positive values in between this range. The same concept is followed for the rest of the two groups having an angle spread between $15°$ and $25°$, and between $25°$ and $35°$ respectively. In this way, very short, short, and long angle direction is covered. For both subspace-based and power-based methods, a scanning direction grid with a step size of $0.2°$ is used. The grid is chosen to uniformly cover the entire region of interest ($-90°$ to $90°$). On the other side, a delay spread of 1, 2, and 3 samples corresponding to 32.55, 65.10, and 97.65 ns are assigned randomly to the multipath signal. These can be translated into a minimum distance of 10 m and a maximum distance of 30 m. Since the number of sources K is known in this case, it is set to 2 and no estimation of the number of signals is done. The iterative approached techniques (IAA, SAMV sparse methods) perform a maximum of 60 iterations for each estimation.

Results show that due to the smearing effect and the limited resolution, MUSIC, and beamforming techniques fail to correctly separate the closely spaced sources. For the case of coherent signals, it is known that the eigen-analysis-based MUSIC algorithm and the classical beamform-

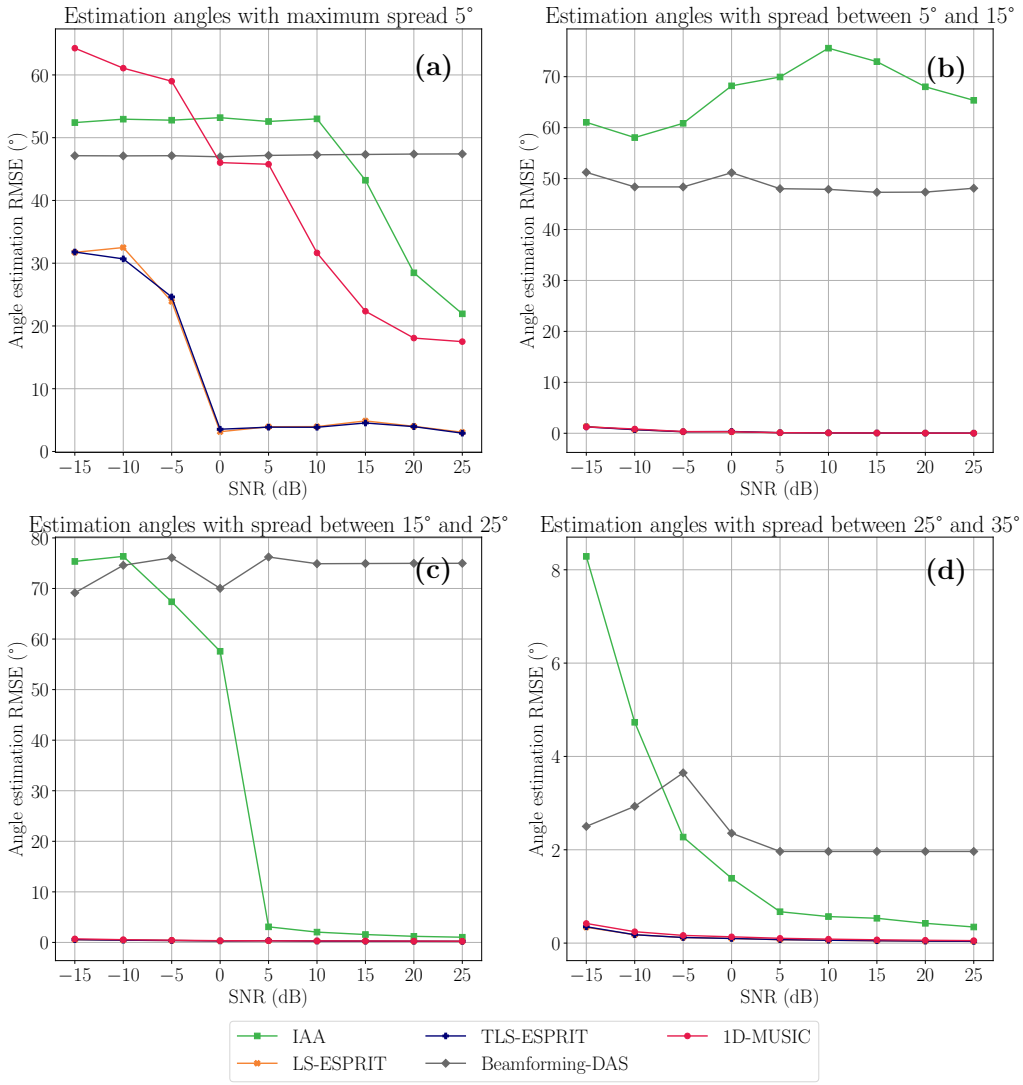


Figure 6.21: Angle estimation error for different angle spread.

ing technique in two dimension couples range and angle are not able to discriminate the two targets. However, the simulation results show that when being treated independently, i.e., dealing with only one dimension at a time, the two coherent signals with different angles of arrival and time delays, can perform source separation based on these differences in spatial and temporal characteristics, also known as "spatial source separation" thanks to their super-resolution characteristics. Thus, the incoming signals at different directions of arrival produce different spatial patterns due to the different time delays. Even in the presence of low SNR, a great improvement in angular estimation is obtained when the signals are well separated between them, greater than 5°. For close sources, the reduction in angle estimation error is noticed at high SNR. It is also noticed that the performance of AoA estimation is better when the multipath is not only well separated with the reference in the spatial domain, but also the temporal domain is above 1 sample delay. The Total Least Squares (TLS) ESPRIT solution is slightly better compared to the Least Squares (LS) ESPRIT. However, their difference in estimation accuracy is hardly noticeable for higher SNR and angle spreads. Nevertheless, they do show lower angle

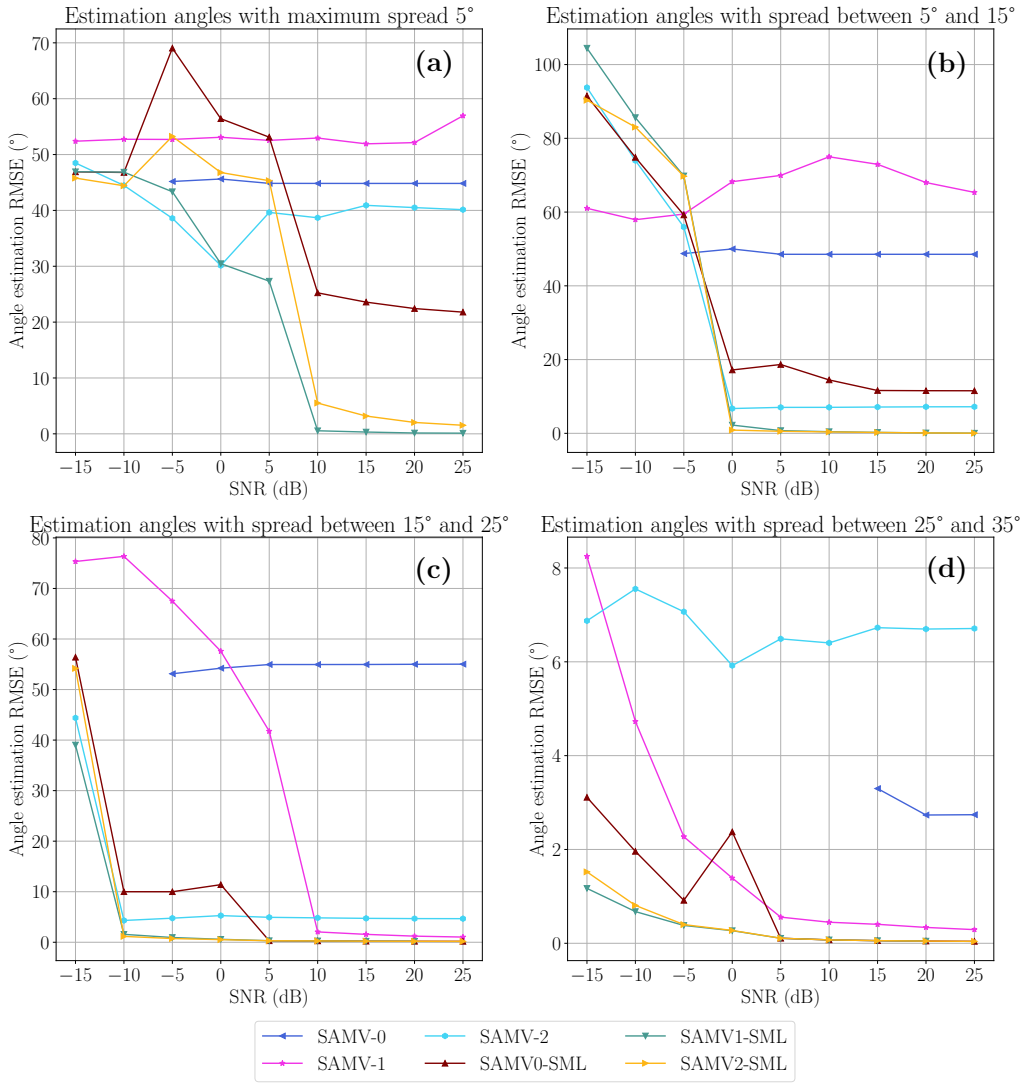


Figure 6.22: Angle estimation error for different angle spread using sparse asymptotic minimum variance approaches.

error even in closely placed sources with a reduction of almost half of the error given by the other spatial-based methods. All spatial-based methods give an error estimation of less than 2° for greater delay spread. On the other hand, beamforming presents worse performance even at higher angular spread. Because of its data-independent property, the classical beamforming, Delay And Sum (DAS) used in this part of the work, suffers from lower resolution. This is also because of the lower number of antenna elements being used. Having a wider main lobe (associated with fewer antenna elements) results in a poorer angular resolution. This explains the lower performance of the technique to accurately differentiate between arriving signals, where the best accuracy achieved is no lower than 2° estimation error.

Evaluating the performance of the power-based techniques like IAA, SAMV, and SAMV-SML, it is observed from the results obtained that they generate higher resolution sparse spatial estimates for the coherent sources. However, even though they reduce the smearing effect, the resolution provided is not high enough to separate the two closely spaced sources at lower SNR.

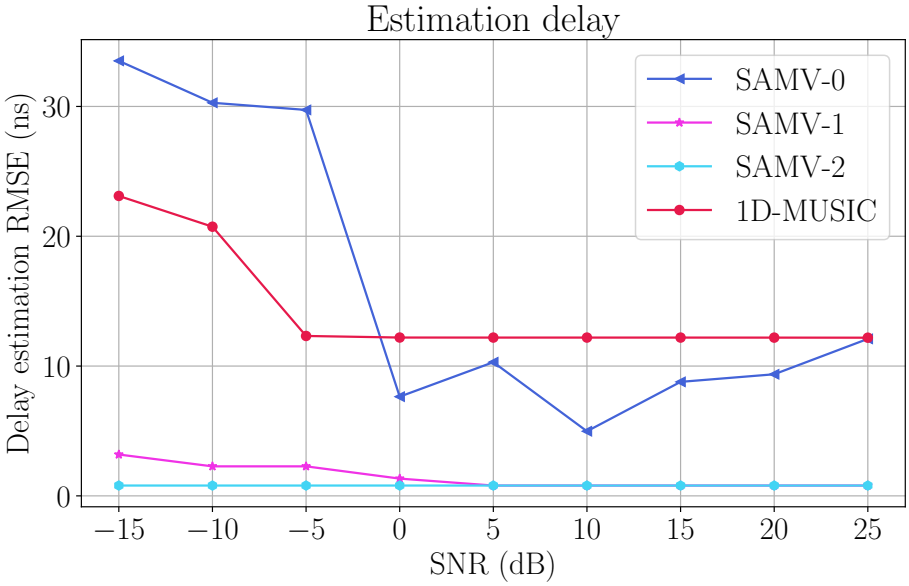


Figure 6.23: Time delay error estimation.

In general, the sparse techniques have a better performance compared to the IAA techniques. By comparing these techniques, it is seen that the difference between IAA with its counterpart SAMV methods is the way of estimating the power matrix. In IAA, the power estimates are done by adding up the signal magnitude. For the case of sparse methods, the power matrix is computed as proportional to the square estimates at the previous iteration for the case of SAMV-0, proportional to the square of Capon power for the case of SAMV-1, and a combination of the power estimates at previous iteration and the standard Capon power estimates for the case of SAMV-2. This approach makes the covariance matrix of IAA suffer from matrix singularity when only a few elements of the signal powers are non-zero, i.e., the noise-free case. IAA performs better at higher SNR starting from 5 dB and needs a higher number of snapshots. For the sparse methods, due to the combination of power estimates, SAMV-2 achieves better resolution. Moreover, knowing that the resolution of the power-based sparse techniques is limited by the fineness of the direction scanning grid, the "grid-limit-free" SAMV-SML approaches have superior resolution and provide the most accurate estimates below 1°. They are also more robust to practical difficulties, such as the insufficient number of snapshots, and provide grid-independent asymptotically efficient estimates without any additional grid refinement postprocessing. From the results, it is seen that the SAMV-0 approach does not work in excessively low SNR. All the sources can be accurately resolved when they have adequately high SNR. SAMV-2 provides better results even in low SNR and with very close-placed sources, by giving an angle error estimation up to 20° lower. In conditions of long angular spread and high SNR SAMV-1 and SAMV-2 are very similar in accuracy. SAMV-1 and IAA are equivalent at high SNR.

For the case of delay estimation, two methods are used: 1D MUSIC and the SAMV sparse methods. The latter have been modified to enable the time delay estimation as explained in Section 6.3. The results show a better resolution for the case of SAMV-1 and SAMV-2 even in extensive low SNR conditions. For both cases, MUSIC and SAMV-1 and SAMV-2, at high SNR, the accuracy reaches a limit of resolution. The latter method lowers the delay error estimation by one order of magnitude.

6.7 Experimental results on angle estimation accuracy

To evaluate the proposed receiver and the feasibility of the calibration for the angle estimation accuracy, indoor and outdoor experiments were performed by transmitting an uplink 5G signal. The indoor experiment is carried out in an empty laboratory room of the office building and the outdoor experiment in an open space in the backyard, both at the Autonomous University of Barcelona, Spain. For the indoor experiment, the In-Situ calibration data (see the calibration process in Section 6.5.2.1) are considered and the calibration data obtained from the anechoic chamber process described in Section 6.5.2.2 are considered for the outdoor experiments. In this section, the experimental hardware and software setup are first presented. Then, the experimental results are analyzed.

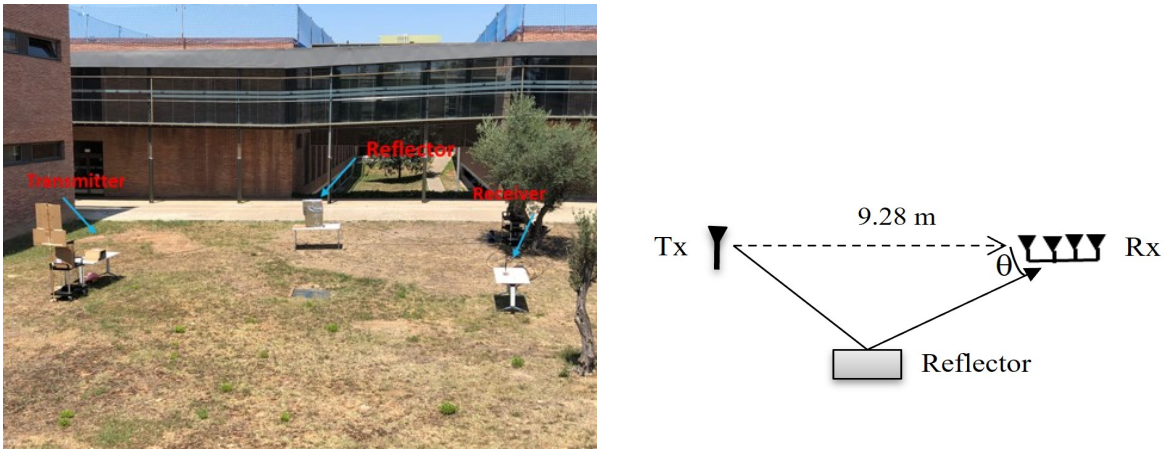
6.7.1 Experimental hardware and software setup

The setup and parameter configurations for the indoor experiment are maintained the same as the In-Situ calibration described in Section 6.5.2.1. Similar to the calibration process, for the indoor experiment, the array manifold at the receiver side is swiveled so that different angles of arrival are obtained (from $-90°$ to $-90°$ with a step size of $5°$). The experiment is carried out under LoS conditions.

For the outdoor experiment two different set-ups are realized: one with no-multipath where the transmitter and receiver are in LoS conditions, and one in the presence of multipath where a reflector is placed in two different positions (one forming a $45°$ angle of arrival placed in between the TX and RX as depicted in Figure 6.24 and the other forming $30°$ placed near the TX side in a distance of 4 m away). The transmitter and receiver are placed within a distance of 9.28 m (see Figure 6.24). The same setup is used for the case of no-multipath, where the presence of the reflector is removed. For the first setup, with no multipath, the linear array composed of 4 elements at the receiver side is swiveled so that different angles of arrival are obtained (from $-60°$ to $-60°$ with a step size of $10°$. For the case of multipath, the angle of arrival of the TX is maintained fixed at $0°$, and the reflector body is moved in the proper positions to form the decided angle of arrival. With this experiment, the exploration of the accuracy achieved from the estimation methods proposed in this chapter of the angle of arrival estimation coming from the reflector is performed. This experiment can be considered as a first step to open the path for the localization and/or sensing problem.

Since the experimental scenarios for both indoor and outdoor involve movement and targets in the horizontal plane (azimuth), the vertical plane (elevation) variations are expected to be minimal. Moreover, ULA is typically sensitive to variations in the azimuth angle. The presence of only four elements in the ULA, limit the ability to accurately estimating both azimuth and elevation angles simultaneously. Nevertheless, since elevation variations are minimal, the accuracy gain from considering elevation angles tends to be marginal. The angular spread in the elevation dimension is typically an order of magnitude lower than in the azimuth dimension. Because of all the above-mentioned reasons, the angle measurements of these experiments will be focused only on the azimuth angle.

In both scenarios, the SRS signal is transmitted periodically every 1 millisecond during 2 sec from the single antenna port of USRP-Tx N310. The system parameters used are a carrier



(a) Environmental Layout.

(b) Experimental Setup.

Figure 6.24: Setup of an outdoor experiment for AoA estimation in the presence of a reflection forming a 45° angle of arrival. Note that, for an experiment where the reflector forms a 30° angle of arrival, it is placed near the TX side. For the scenario without multipath, i.e., the TX and RX are in LoS conditions, the reflector is removed and the rest of the setup has remained the same.

frequency of 2.4875 GHz, transmission gain of 65 dB, and a sampling rate of 30.72 Msps, corresponding to 25 MHz bandwidth. For the experimental part, omnidirectional monopole antennas are used for both TX and RX. The single transmitter antenna is mounted directly on one of the transmission channels of the TX-N310, while on the receiver's side, the antennas are mounted in a platform with a separation of $\lambda/2$ between elements of the antenna. To improve the resolution ability, in the presence of interference, the correction is undertaken by choosing only the subcarriers that do not contain the interference after the demodulation of the waveform as explained in 6.5.2.1. For these experiments, an interference at a center frequency of 2.479 GHz with a 2 MHz bandwidth has been detected. Note that this interference is the same as the one detected during the In-Situ calibration process. The samples are recorded using LabVIEW. For the outdoor experiments, 3 tests for each case are considered with a duration of 2 seconds each. The recorded samples were processed with Matlab offline.

6.7.2 Indoor experimental results

Multipath effects manifest in the propagation delay of a reference signal at each subcarrier k as a phase shift $\sum_{r=1}^{R} \alpha^r \cdot e^{-j2\pi k \Delta f \tau^r}$. Here, τ^r represents the propagation delay of the r-th path, R is the total number of propagation paths, and α^k denotes the absolute amplitude of the k-th signal. Severe multipath conditions give rise to a propagation delay impact of 5.3° across successive subcarriers. This has been computed by considering 2 paths, a frequency spacing of 15 kHz and a propagation delay of 1 sample corresponding to 9.7656 m. For incident angles positioned between the test angles, an interpolation within the range of array modeling errors (computed during antenna error calibration) was executed. These inaccuracies have a direct impact on the precision of the AoA estimation, as evidenced by the results presented in Figure 6.25.

Results depicted in 6.25 show a significant improvement in AoA estimation accuracy with a maximum of 46.74% when applying only the RF channel error corrections. The large improvement in the accuracy of AoA estimation shows the high phase offset that the received RF

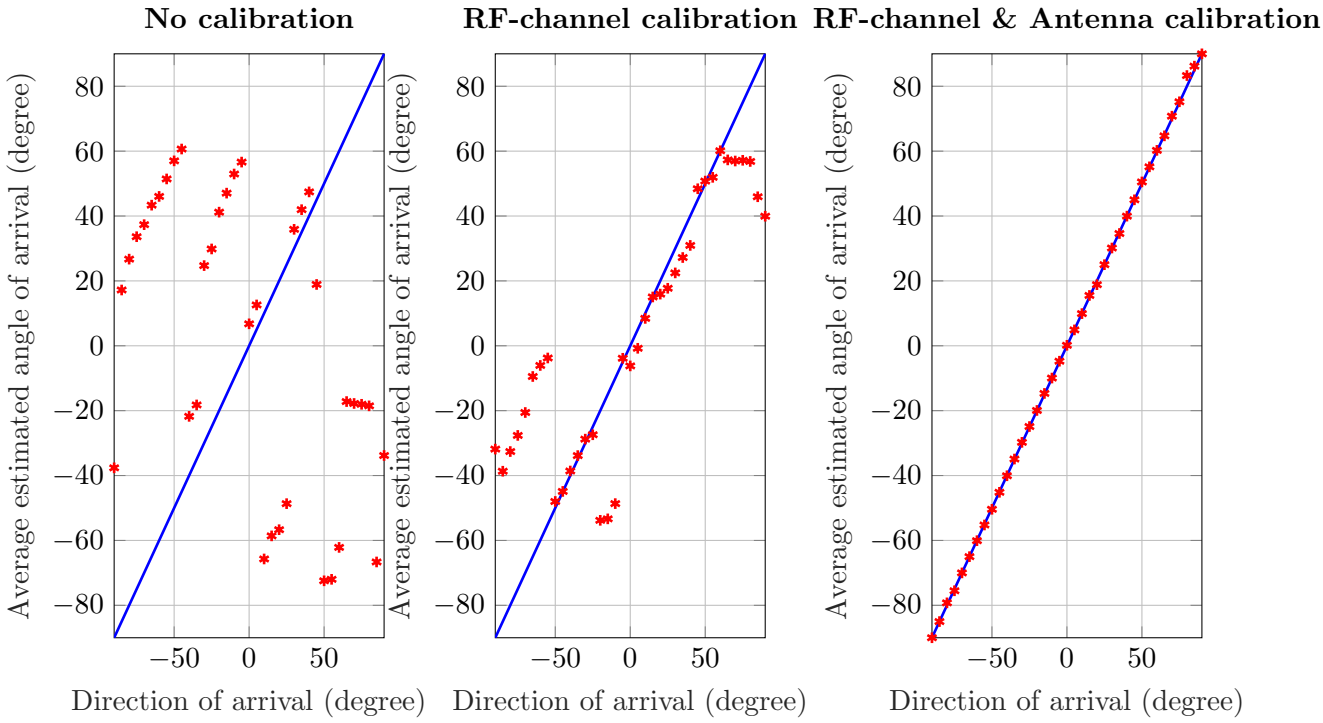


Figure 6.25: Estimation angle of arrival accuracy using In-Situ calibration in indoor environment.

channels apply and therefore a severe degradation on the angle of arrival is faced. Moreover, an additional reduction of error estimation of maximum 25.9% is noted when the antenna error correction is applied, especially in cases close to the end-fire array where unsatisfactory performance is expected. The maximum error estimation deviation reaches ±17.32 degrees and it reduces up to less than one degree (±0.58) when applying the full calibration corrections estimated during In-Situ calibration. These results show the importance of the calibration process enabling the stability and accuracy of the AoA estimation since the measured antenna array manifold severely deviates from the nominal manifold. Therefore, the In-Situ measurements cause an improvement of the incident angles as they capture the real array responses more precisely by using the post-established in-field measurements.

Table 6.6: AoA estimation performance

Calibration Method		No calibration	RF channel calibration	RF channel & antenna error calibration
rmse_AoA_estimate (º)	max	151.64	58.16	3.35
	min	5.9	0.07	0.007
std_estimation_error (º)	max	17.32	14.58	0.58
	min	0.04	0.02	0.003

6.7.3 Outdoor experimental results

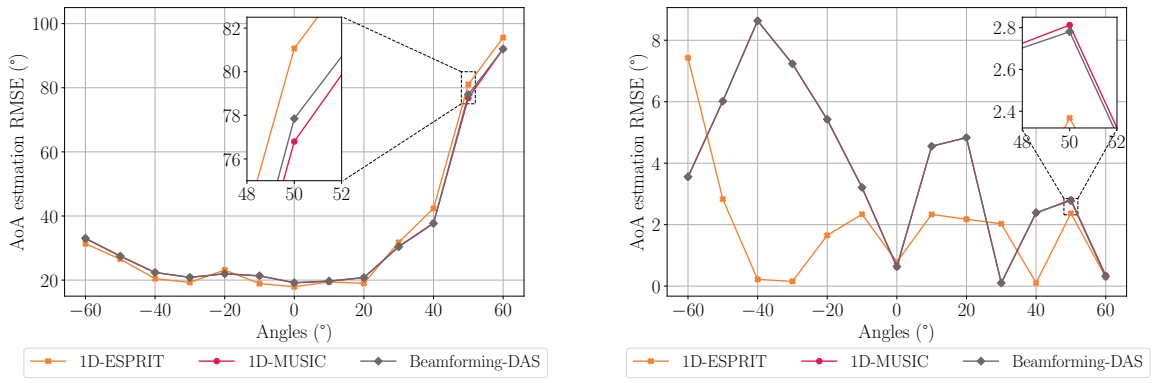
As already stated, the distance (d) between the TX and RX is set to 9.28 m (see Figure 6.24). This distance should be based on the requirement that the electromagnetic field in the area of the received antenna array must contain only components present in the far field of the transmit antenna ($d \longrightarrow \infty$). The distance for this experiment was limited by the available surface and having into account that the phase deviation ξ concerning a planar wave increases toward the

edge of the antenna, at a frequency of 2.4875 GHz, a 1.3° of additional phase deviation is present. The phase deviation at the edge of the array antenna aperture (width A) is computed using the following formula:

$$\xi \sim= \frac{\pi A^2}{4d\lambda}, \tag{6.44}$$

where A is the antenna aperture, d is the distance between the TX and RX, and λ is the wavelength.

Since the number of incoming signals is not known in practice, the Minimum Descriptive Length (MDL) criterion is used to estimate it. Figure 6.26 shows the results obtained during experimentation in a non-multipath scenario. Conventional subspace-based techniques such as MUSIC and ESPRIT, as well as classical beamforming, are used to perform angular estimation. The angle estimation error reduces four times when calibration is used showing the feasibility and the great impact of caliration in angle measurements. Moreover, the results show that the angle error estimation reduces as we go near 0°. On the other hand, for angles near the end-fire position of the antenna array, the error increases. MUSIC and beamforming give similar performance in terms of estimation accuracy for all angles, with MUSIC given an 0.05° reduction in the error estimation. A maximum of $\sim 8.6°$ and a minimum of $\sim 0.1°$ angle error estimation is achieved by this method. The average error estimation is $\sim 3.8°$. Both methods are consistent in their estimation of all considered snapshots with a standard deviation of $\sim 2.6°$.



(a) No calibration.

(b) Calibration.

Figure 6.26: RMSE angle estimation in LoS conditions.

Figure 6.27 shows the results obtained from the experiment in the presence of multipath. The RMSE angle estimation is separated into three tests that correspond to different data streams captured, where the conditions are maintained the same. Based on the MDL approach, the number of incoming signals is 3. Additionally, it might happen that the number of incoming signals is incorrectly estimated by the MDL method. This may lead to the appearance of spurious (or false) angular estimates.

Considering 3 incoming signal means that, having an array composed of 4 elements, the MUSIC reduces to the Pisarenko method, where the angle will be estimated as the angular position of the roots. In this case, we will not have the problem of separating the "signal roots" from the "noise roots". Moreover, apart from the computational simplicity, Pisarenko can have a relatively poor statistical accuracy. However, in the case of our scenario, it can distinguish the presence of the two expected signals from different paths.

For the case of reflection with an AoA 30°, the results show promising high performance where the accuracy of AoA estimation is below 4° for all the techniques considered, except beamforming that gives a high error estimation. The effectiveness of beamforming techniques depends on the width of the main lobe in the array's beam pattern and its ability to distinguish between sources at different angles. A ULA with 4 elements typically has a relatively wide main lobe, and the resolution may not be high enough to distinguish sources close to each other in angle. Therefore, the worst performance of the beamforming techniques can be because the secondary lobes of the response corresponding to the direct signal can move the position of the maximum of the reflection lobe.

The lowest angle error is obtained by MUSIC with an error below 1.5°. IAA, SAMV-1, and SAMV2-SML give similar resolution with an angle error below 3°. SAMV0-SML and SAMV1-SML have the same angular accuracy. Apart from beamforming, 1D ESPRIT (both LS and TLS approach) gives the worst estimation with a maximum angle error of 3.9°.

For the case of reflection with an AoA 45° the maximum angle error estimation computed is 8.9°. Even in this case, MUSIC presents a better resolution (the last two tests). Here, the performance of beamforming has improved with an averaged angle error of $\sim 4°$. IAA and SAMV-1 have given very similar results with an error estimation of 6.47° on average. SAMV-SML techniques give the highest estimation error compared to the rest of the methods. This is because the output of SAMV-2 is taken as an input to the algorithm and the results obtained here show that these methods have the worst performance.

Overall, the estimation for the second case is worse than the first case. This can be derived from using aluminum foil to build the reflection body. Knowing that the foil has different diffuse properties (the bright side lower diffuse % and the matte side a higher diffuse %), it was decided to go with the bright side. However, the scatter of the arriving signal depends also on the direction of the signal. Some show more scatters than another angle. These limitations, as well as some residuals that remained during the calibration part have contributed to the degradation of the results. A summarized table of the performance of each method for both cases is presented below (see 6.7, 6.8). Because of the bad performance of angle estimation evaluated through simulations, the power-based method SAMV-0 is not considered for both scenarios: reflection at 30° and 45°. The simulation results showed that this method is not stable and only worked for high SNR. The angle error estimation obtained was above 15° and therefore it was decided to not be considered in the analysis.

Table 6.7: Table with AoA estimation averages and standard deviation for estimation of the reflection angle at 30°.

Method	Test1	Test2	Test3
Beamforming - DAS	42.313 ± 0.100	42.268 ± 0.100	42.360 ± 0.082
1D- MUSIC	31.267 ± 0.938	32.322 ± 0.938	31.670 ± 1.282
IAA	31.990 ± 0.234	33.180 ± 0.234	33.270 ± 0.134
LS- ESPRIT	32.635 ± 1.114	33.941 ± 1.114	31.667 ± 1.328
TLS- ESPRIT	32.635 ± 1.114	33.941 ± 1.114	31.667 ± 1.328
SAMV-1	32.015 ± 0.222	33.195 ± 0.222	33.270 ± 0.134
SAMV-2	32.503 ± 0.137	33.688 ± 0.137	33.620 ± 0.128
SAMV0-SML	33.100 ± 0.182	34.601 ± 0.182	34.310 ± 0.205
SAMV1-SML	33.100 ± 0.182	34.601 ± 0.182	34.310 ± 0.205
SAMV2-SML	32.037 ± 0.135	33.327 ± 0.135	33.190 ± 0.105

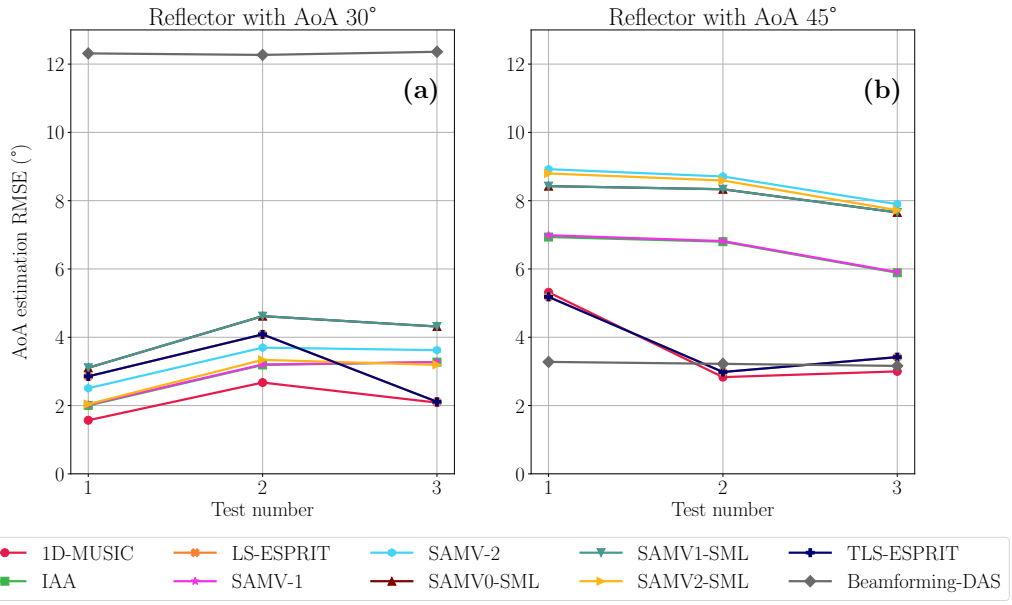


Figure 6.27: Evaluating the accuracy of the angle of arrival estimation in the presence of multipath.

Table 6.8: Table with AoA estimation averages and standard deviation for estimation of the reflection angle at 45°.

Method	Test1	Test2	Test3
Beamforming-DAS	48.277 ± 0.099	48.220 ± 0.099	48.160 ± 0.082
1D- MUSIC	49.938 ± 1.995	47.410 ± 1.995	47.750 ± 1.231
IAA	51.928 ± 0.326	51.790 ± 0.326	50.880 ± 0.327
LS- ESPRIT	49.941 ± 1.585	47.648 ± 1.585	48.281 ± 0.984
TLS-ESPRIT	49.941 ± 1.585	47.648 ± 1.585	48.281 ± 0.984
SAMV-1	51.979 ± 0.343	51.810 ± 0.343	50.900 ± 0.321
SAMV-2	53.918 ± 0.278	53.702 ± 0.278	52.890 ± 0.328
SAMV0-SML	53.423 ± 0.231	53.329 ± 0.231	52.653 ± 0.235
SAMV1-SML	53.423 ± 0.231	53.329 ± 0.231	52.653 ± 0.235
SAMV2-SML	53.792 ± 0.289	53.585 ± 0.289	52.715 ± 0.329

6.8 Conclusions

In this work, we have demonstrated the potential of 5G signals for indoor and outdoor observable estimation for positioning. It was investigated the array modeling errors and proposed the design of an efficient receiver to calibrate the errors and provide Time of Arrival (ToA) and AoA estimates. Note that, for the experimental part only the AoA estimation was considered. Different techniques were proposed to deal with the presence of coherent sources and provide an accurate angular estimation. The evaluation is done in conditions of multipath and interference in signal propagation. The results show a significant improvement in AoA estimation accuracy because of calibration. The calibration process fully exploits the bandwidth resources provided by the 5G signal to resolve the presence of interference in the measurement data. We believe this is an important step to provide high-precision AoA estimation and therefore leading to an accurate positioning location. Moreover, it is proposed a scalable solution to calibrate universal hardware and antenna arrays.

Conclusions and future work

This chapter summarizes the main conclusions of the work conducted in this dissertation and provides several recommendations for future research in this field.

Conclusions

This thesis has contributed to the topic of 5G positioning by exploring time and angle-based positioning techniques to improve localization accuracy in demanding environments. Through this work, we contributed to the understanding of the potential and limitations inherent in 5G positioning. Possible advancements in the domain of 5G positioning for various use cases are evaluated, by addressing key challenges and exploring innovative techniques. The overarching objectives, outlined at the beginning of this work, have been systematically addressed and fulfilled.

Chapter 1 highlighted the significance of reference signals in 5G New Radio (NR), emphasizing their crucial role in supporting positioning services. Their adaptability and flexibility make them invaluable tools in the 5G positioning. In Chapter 2 a simulation platform was proposed, which allowed us to perform software simulations using models and configurations that are fully representative of real use cases and user environments. Through the methodology proposed in the simulation platform, we evaluated the 5G positioning performance in different environments and configurations, as presented in Chapter 3. Standalone and hybrid techniques were explored that laid a robust foundation for assessing positioning capabilities in challenging scenarios. The integration of 5G network density has been a critical factor for positioning accuracy to achieve the target set by the 5G standard, i.e., a positioning error $<$ 10m (80% of User Equipment (UE)) for outdoor scenarios. Additionally, an analysis of positioning capabilities in scenarios crucial for two challenging use cases: Internet of Things (IoT) and autonomous cars was performed. The results have shown that, for the case of IoT scenarios, where narrowband cellular technologies are prevalent, extended coverage areas lead to lower network density. This, in turn, results in Non Line of Sight (NLoS) scenarios, introducing multipath effects that are challenging to mitigate due to the narrow bandwidth available. The standard techniques implemented like Cell IDentity (CID) and Uplink Time Difference of Arrival (UTDoA) have shown minimal power consumption, which is an important factor for low-energy IoT applications. However, their accuracy is primarily dependent on the coverage area of the connected base station. Round Trip Time (RTT) techniques, on the other hand, have provided better accuracy but they come at the cost of additional UE power consumption. For the case of autonomous cars, the time and angle-based standalone techniques have offered a promising avenue to improve the accuracy of vehicle localization with a positioning error $<$ 10m in conditions of no synchronization error and

$<$ 30m with maximum synchronization error. The advanced physical features of 5G networks, such as optimized waveforms, wide bandwidth, cmWave technology, and high-density networks, make them well-suited for positioning purposes.

In Chapter 4 we addressed the challenge of maintaining position integrity in urban cellular network positioning systems. We proposed an algorithm, centered on excluding base stations affected by NLoS conditions. The algorithm demonstrated notable advantages, offering a promising avenue to improve accuracy in challenging urban scenarios. An even better accuracy was achieved when incorporating a hybrid method composed of time and angle-based techniques. These findings were presented in Chapter 5, where we proposed the use of array antennas in combination with time-delay-based positioning method to enhance accuracy in deep urban environments. The hybrid method provided an improvement of 27.5% in positioning accuracy compared to the accuracy provided by time-based and angle-based methods used alone. In addition, the use of the Base Station (BS) detection and exclusion method, proposed in Chapter 4, allowed us to identify and remove abnormal measurements from BS affected by NLoS and synchronization error. The method managed to remove the malicious BS in the majority of cases. The maximum horizontal position error was reduced by 40% compared to UTDoA solution and 18.15% compared to the hybrid case without the BS exclusion mechanism. This improvement overtook the performance achieved by RTT, which relaxes the constrained positioning problem, i.e., the presence of synchronization error.

Finally, in Chapter 6 we proposed an experimental platform that allows to bridge the gap between simulation and real-world. This was done through a reproducible methodology of customized setup based on Software-Defined Radio (SDR). The methodology allows the transmission and reception of an uplink signal from one UE to a BS, equipped with an antenna array to estimate its angle of arrival. We provided insights and a systematic approach for conducting theoretical and experimental 5G localization studies through an accurate and robust Angle of Arrival (AoA) estimation process for 5G networks. The methodology consisted of several steps such as calibration (Radio Frequency (RF) channel error calibration and antenna error calibration), synchronization (a time delay and frequency offset estimation) and data processing (data extraction) to finally provide the AoA estimation. We have demonstrated the potential of 5G signals for indoor and outdoor observable estimation, explored array modeling errors, and proposed efficient receiver design for calibration, enabling accurate AoA estimation. The results showcase a significant improvement in AoA estimation accuracy compared to the case without calibration, particularly in the presence of multipath and interference. Overall, the angle estimation obtained following our methodology appears to be very accurate. When no multipath is presented, a maximum of $\sim 8.6°$ and a minimum of $\sim 0.1°$ angle error estimation is achieved by using conventional methods. The average error estimation is $\sim 3.8°$. The methods are consistent in their estimation of all considered snapshots with a standard deviation of $\sim 2.6°$. In the presence of multipath, when using conventional methods, the lowest angle error obtained is below $2°$ and the highest angle error is $12.3°$. To improve the angle estimation we explored more modern and complex AoA estimation. The lowest angle error achieved is below $2°$ and the highest below $8.9°$. Both methods, conventional and unconventional, showcase a scalable solution for real-world applications, underscoring the practical impact of the research.

In summary, the collective insights from these chapters underscore the transformative potential of 5G positioning technologies. From improving simulation methodologies to addressing

real-world challenges in urban environments, this research has paved the way for more accurate and reliable positioning solutions. The proposed hybrid algorithms, exclusion methods, the use of angular measurements, the evaluation of signal parameter estimation algorithms, and calibration techniques exhibit potential for real-world applications, emphasizing the practical utility of the research outcomes. We have also helped to bridge the gap between simulation and practical deployment. This thesis not only has contributed valuable insights to the research community but also has offered practical solutions with real impact on the evolution of 5G positioning. We believe that this work is a step forward in unlocking the full potential of 5G localization, setting the stage for a new era of precise and reliable positioning in diverse and challenging scenarios.

Future Work

As we conclude this thesis, it is important to highlight potential future research lines to advance further the work done. Some of the proposed future works are as follows:

1. Further exploration into the integration of emerging technologies, such as machine learning and artificial intelligence, could enhance the robustness of 5G positioning algorithms

2. Continued real-world validations and optimizations will be crucial for bridging the gap between simulation and practical deployment.

3. A number of issues remain in terms of integrity in an urban environment. This promising topic is waiting for innovations. Considering all the complexities of the urban integrity monitoring mentioned in 4, we have the following perspectives:

    - Error modeling in urban environments is still an important aspect to be conquered, especially the characterization of the local effects, which can contribute to integrity monitoring;
    - The proper way to remove the constraint assumption in the classic Receiver Autonomous Integrity Monitoring (RAIM) approach with a low computational cost should be fully addressed in the future. If this can be achieved, the implementation can be facilitated;
    - Improvement of the existing urban integrity algorithms is necessary in terms of the trade-off between the size of the protection level and the criterion of integrity. And other new algorithms can be developed based on the combination of current methods.
    - The integrity specifications for different urban applications should be developed and tested. For this, the methodology used in the aviation domain can be partly taken.

4. While the measurements taken during array calibration may be subject to errors, such as sensor noise, reflections from the anechoic chamber, imperfections in the positioner, cabling-induced attenuations and phase-drifts, and proximity effects between the antenna array and probe (i.e., not in far-field). To ensure accurate array processing, these errors need to be corrected. Approaches to reduce these errors occurring during array calibration measurements can be further investigated.

5. Extend research to include three-dimensional (3D) positioning capabilities, especially in urban environments with complex vertical structures. Understanding and addressing challenges related to vertical positioning could open new applications in areas like augmented reality and drone navigation.

6. Conduct extensive real-world deployment studies to validate and refine the proposed algorithms and techniques. Emphasize testing in diverse environments, including smart cities, industrial settings, and rural areas, to ensure the robustness and generalizability of the solutions.

7. In addressing challenges like sensitivity to blockages, severe path loss, and inadequate coverage in cellular systems, Reflective Intelligent Surfaces (RIS) emerges as a key technology for fostering a smart radio environment in future-generation applications. RIS is poised to play a pivotal role in the evolution of "6G communication networks," offering the potential to enhance network performance by creating a controllable radio ecosystem. The integration of RIS into cellular systems for positioning should be investigated to overcome limitations of traditional systems.

Bibliography

[1] Y. Lu, P. Richter, and E. S. Lohan, "Opportunities and challenges in the industrial internet of things based on 5g positioning," in *2018 8th International Conference on Localization and GNSS (ICL-GNSS)*. IEEE, 2018, pp. 1–6.

[2] Z. B. Tariq, D. M. Cheema, M. Z. Kamran, and I. H. Naqvi, "Non-gps positioning systems: A survey," *ACM Computing Surveys (CSUR)*, vol. 50, no. 4, pp. 1–34, 2017.

[3] R. F. Brena, J. P. García-Vázquez, C. E. Galván-Tejada, D. Muñoz-Rodriguez, C. Vargas-Rosales, J. Fangmeyer *et al.*, "Evolution of indoor positioning technologies: A survey," *Journal of Sensors*, vol. 2017, 2017.

[4] F. Mogyorósi, P. Revisnyei, A. Pasić, Z. Papp, I. Törös, P. Varga, and A. Pasić, "Positioning in 5g and 6g networks—a survey," *Sensors*, vol. 22, no. 13, p. 4757, 2022.

[5] J. A. del Peral-Rosado, R. Raulefs, J. A. López-Salcedo, and G. Seco-Granados, "Survey of cellular mobile radio localization methods: From 1G to 5G," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 2, pp. 1124–1148, 2018.

[6] J. A. del Peral-Rosado, J. A. López-Salcedo, G. Seco-Granados, F. Zanier, and M. Crisci, "Achievable localization accuracy of the positioning reference signal of 3GPP LTE," in *Proc. International Conference on Localization and GNSS (ICL-GNSS)*, 2012, pp. 1–6.

[7] J. A. Del Peral-Rosado, R. E. I. Castillo, J. Mıguez-Sánchez, M. Navarro-Gallardo, J. A. Garcıa-Molina, J. A. López-Salcedo, G. Seco-Granados, F. Zanier, and M. Crisci, "Performance analysis of hybrid gnss and lte localization in urban scenarios," in *2016 8th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*. IEEE, 2016, pp. 1–8.

[8] R. Keating, M. Säily, J. Hulkkonen, and J. Karjalainen, "Overview of positioning in 5g new radio," in *2019 16th International Symposium on Wireless Communication Systems (ISWCS)*. IEEE, 2019, pp. 320–324.

[9] I. Rahman, T. Chapman, M. A. Kazmi, and F. Ghasemzadeh, "Enabling the potential of 5g: Solutions to the technical challenges of the diverse 5g bands," *IEEE Wireless Communications*, vol. 27, no. 2, pp. 6–11, 2020.

[10] S. Bartoletti, L. Chiaraviglio, S. Fortes, T. E. Kennouche, G. Solmaz, G. Bernini, D. Giustiniano, J. Widmer, R. Barco, G. Siracusano *et al.*, "Location-based analytics in 5g and beyond," *IEEE Communications Magazine*, vol. 59, no. 7, pp. 38–43, 2021.

[11] R. Di Taranto, S. Muppirisetty, R. Raulefs, D. Slock, T. Svensson, and H. Wymeersch, "Location-aware communications for 5g networks: How location information can improve scalability, latency, and robustness of 5g," *IEEE Signal Processing Magazine*, vol. 31, no. 6, pp. 102–112, 2014.

[12] H. Wymeersch, G. Seco-Granados, G. Destino, D. Dardari, and F. Tufvesson, "5g mmwave positioning for vehicular networks," *IEEE Wireless Communications*, vol. 24, no. 6, pp. 80–86, 2017.

[13] S. Bartoletti, H. Wymeersch, T. Mach, O. Brunnegård, D. Giustiniano, P. Hammarberg, M. F. Keskin, J. O. Lacruz, S. M. Razavi, J. Rönnblom *et al.*, "Positioning and sensing for vehicular safety applications in 5g and beyond," *IEEE Communications Magazine*, vol. 59, no. 11, pp. 15–21, 2021.

[14] A. Nemra and N. Aouf, "Robust ins/gps sensor fusion for uav localization using sdre nonlinear filtering," *IEEE Sensors Journal*, vol. 10, no. 4, pp. 789–798, 2010.

[15] J. A. del Peral-Rosado, G. Granados, R. Raulefs, E. Leitinger, S. Grebien, T. Wilding, D. Dardari, E. Lohan, H. Wymeersch, J. Floch *et al.*, "Whitepaper on new localization methods for 5g wireless systems and the internet-of-things," in *White Paper of the COST Action CA15104 (IRACON).* COST Action CA15104, IRACON, 2018, pp. 1–27.

[16] F. Rinaldi, H.-L. Maattanen, J. Torsner, S. Pizzi, S. Andreev, A. Iera, Y. Koucheryavy, and G. Araniti, "Non-terrestrial networks in 5g & beyond: A survey," *IEEE access*, vol. 8, pp. 165 178–165 200, 2020.

[17] ETSI, "123 502 v15. 2.0 (jun. 2018),"5g," *Procedures for the 5G System (3GPP TS 23.502 version 15.2. 0 Release 15)," Jun*, 2018.

[18] 3GPP, "Study on nr positioning support, tr 38.855 v16.0," 2019.

[19] 3GPPRel.17, "Summary of Rel-17 Work Items, v.17.1," https://www.3gpp.org/specifications-technologies/releases/release-17, 2023, [Accessed on 4-Dec-2023].

[20] 3GPPRel.18, "System architecture for the 5G System (5GS), v.18.0," https://www.3gpp.org/specifications-technologies/releases/release-18, 2023, [Accessed on 4-Dec-2023].

[21] 3GPP, "Stage 2 functional specification of user equipment (UE) positioning in NG-RAN," Tech. Rep. TS 38.305, v15.5.0, Dec. 2019.

[22] J. A. Del Peral-Rosado, P. Nolle, S. M. Razavi, G. Lindmark, D. Shrestha, F. Gunnarsson, F. Kaltenberger, N. Sirola, O. Särkkä, J. Roström *et al.*, "Design considerations of dedicated and aerial 5g networks for enhanced positioning services," in *2022 10th Workshop on Satellite Navigation Technology (NAVITEC).* IEEE, 2022, pp. 1–12.

[23] S. Pal, "What's Inside Counts: How 6G Can Enable Ubiquitous, Reliable Indoor Location Services," https://www.6gworld.com/exclusives/whats-inside-counts-how-6g-can-enable-ubiquitous-reliable-indoor-location-services/, 2023, [Accessed on 1-Aug-2023].

[24] 3GPP, "Physical channels and modulation," *ETSI, TS138.211 V16.2.0*, vol. 5, pp. 1–135.

[25] J. A. del Peral-Rosado, O. Renaudin, C. Gentner, R. Raulefs, E. Dominguez-Tijero, A. Fernandez-Cabezas, F. Blazquez-Luengo, G. Cueto-Felgueroso, A. Chassaigne, D. Bartlett, F. Grec, L. Ries, R. Prieto-Cerdeira, J. A. Lopez-Salcedo, and G. Seco-Granados, "Physical-layer abstraction for hybrid gnss and 5g positioning evaluations," in *2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall)*, 2019, pp. 1–6.

[26] 3GPP, "Study on channel model for frequencies from 0.5 to 100 GHz,," Tech. Rep. TS 38.901, Re.14, Dec. 2017.

[27] 3GPP, "Lte, evolved universal terrestrial radio access (e-utra), physical channels and modulation," *ETSI TS136.211, V16.2.0*.

[28] 3GPP, "5G NR Physical layer procedures for control," *TS138.213 v15.7.0*, Oct. 2019.

[29] Alliance, "5g white paper," *Next generation mobile networks, white paper*, vol. 1, no. 2015, 2015.

[30] GSMA Assocation, "5G TDD Synchronisation, Guidelines and Recommendations for the Coexistence of TDD Networks in the 3.5 GHz Range," https://www.gsma.com/spectrum/wp-content/uploads/2020/04/3.5-GHz-5G-TDD-Synchronisation.pdf, 2023, [Accessed on 4-Oct-2023].

[31] 3GPP TR22.891, "Study on new services and markets technology enablers," 2016.

[32] 3GPP, "Tr 45.820 v13. 1.0,'cellular system support for ultra-low complexity and low throughput internet of things (ciot)'," 2015.

[33] W. Xu, M. Huang, C. Zhu, and A. Dammann, "Maximum likelihood toa and otdoa estimation with first arriving path detection for 3gpp lte system," *Transactions on Emerging Telecommunications Technologies*, vol. 27, no. 3, pp. 339–356, 2016.

[34] R1-1900236, "Performance evaluation for hybrid positioning based on gnss and nr," *3GPP, ESA, RAN1 AH-1901*, Taipei, Taiwan, 2019.

[35] K. Shamaei and Z. M. Kassas, "A joint TOA and DOA acquisition and tracking approach for positioning with LTE signals," *IEEE Transactions on Signal Processing*, vol. 69, pp. 2689–2705, 2021.

[36] B. Li, K. Zhao, and X. Shen, "Dilution of precision in positioning systems using both angle of arrival and time of arrival measurements," *IEEE Access*, vol. 8, pp. 192 506–192 516, 2020.

[37] R. Kaune, J. Hörst, and W. Koch, "Accuracy analysis for tdoa localization in sensor networks," in *14th international conference on information fusion*. IEEE, 2011, pp. 1–8.

[38] H. Xi, "Sensor selection for multiple sensor emitter location systems/xi hu, mark l. fowler," in *IEEE Aerospace Conference, Big Sky, Montana*, 2008, pp. 1–8.

[39] E. U. T. R. Access, "Base station (bs) radio transmission and reception," *3gpp ts*, vol. 36, p. V9, 2009.

[40] R1-1903021, "Evaluation results for rat-dependent positioning techniques," *3GPP TSG-RAN WG1 meeting Nr.96, Qualcomm*, Mar. 2019.

[41] R1-1901577, "Performance evaluations for nr positioning," *Huawei, HiSilicon*.

[42] R1-1901850, "Updated system level simulation results for nr positioning," *Nokia, Nokia Shanghai Bel*.

[43] 3GPP, "Study on nr positioning," Tech. Rep. TR 38.855, Rel. 16, March 2019.

[44] F. Mata, F. Grec, M. Azaola, F. Blázquez, A. Fernández, E. Dominguez, G. Cueto-Felgueroso, G. Seco-Granados, J. del Peral-Rosado, E. Staudinger *et al.*, "Preliminary field trials and simulations results on performance of hybrid positioning based on gnss and 5g signals," in *Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020)*, 2020, pp. 387–401.

[45] K. Shamaei and Z. M. Kassas, "LTE receiver design and multipath analysis for navigation in urban environments," *Navigation*, vol. 65, no. 4, pp. 655–675, 2018.

[46] R. Grover Brown, "A baseline GPS RAIM scheme and a note on the equivalence of three RAIM methods," *Navigation*, vol. 39, no. 3, pp. 301–316, 1992.

[47] B. W. Parkinson and P. Axelrad, "Autonomous GPS integrity monitoring using the pseudorange residual," *Navigation*, vol. 35, no. 2, pp. 255–274, 1988.

[48] R. M. Kalafus and G. Y. Chin, "Performance measures of receiver-autonomous gps integrity monitoring," in *Proceedings of the 1988 National Technical Meeting of the Institute of Navigation*, 1988, pp. 223–229.

[49] J. Blanch, T. Walter, P. Enge, Y. Lee, B. Pervan, M. Rippl, and A. Spletter, "Advanced raim user algorithm description: Integrity support message processing, fault detection, exclusion, and protection level calculation," in *Proceedings of the 25th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2012)*, 2012, pp. 2828–2849.

[50] J. A. del Peral-Rosado, J. Saloranta, G. Destino, J. A. López-Salcedo, and G. Seco-Granados, "Methodology for simulating 5g and gnss high-accuracy positioning," *Sensors*, vol. 18, no. 10, p. 3220, 2018.

[51] R. Grover Brown and G. Y. Chin, "Calculation of thresholds and protection radius using chi square methods-a geometric approach," *Navigation*, vol. V, pp. 155–179, 1997.

[52] J. De Heus, "Data-snooping in control networks," in *Proc. of Survey Control Networks, Meeting of the Study Group 5B*, 1982, pp. 211–224.

[53] M. Sturza, "Fault detection and isolation (FDI) techniques for guidance and control systems," *NATO AGARD Graph GCP/AG.314, Analysis, Design and Synthesis Methods for Guidance and Control Systems*, 1988.

[54] A. Brown and M. Sturza, "The effect of geometry on integrity monitoring performance," in *Proc. of the Institute of Navigation Annual Meeting*, 1990.

[55] 3GPP, "Study on positioning use cases, stage 1," Tech. Rep. TR 22.872, V16.1.0, Sept. 2019.

[56] B. Sun, B. Tan, W. Wang, and E. S. Lohan, "A comparative study of 3D UE positioning in 5G new radio with a single station," *Sensors*, vol. 21, no. 4, p. 1178, 2021.

[57] E. Y. Menta, N. Malm, R. Jäntti, K. Ruttik, M. Costa, and K. Leppänen, "On the performance of AoA–based localization in 5G ultra–dense networks," *IEEE Access*, vol. 7, pp. 33 870–33 880, 2019.

[58] GNUradio, "GNU Radio usage manual," https://wiki.gnuradio.org/index.php/Usage_Manual, 2023, [Accessed on 19-Jul-2023].

[59] M. S. Bartlett, "Periodogram analysis and continuous spectra," *Biometrika*, vol. 37, no. 1/2, pp. 1–16, 1950.

[60] R. O. Schmidt, *A signal subspace approach to multiple emitter location and spectral estimation*. Stanford University, 1982.

[61] R. Roy and T. Kailath, "Esprit-estimation of signal parameters via rotational invariance techniques," *IEEE Transactions on acoustics, speech, and signal processing*, vol. 37, no. 7, pp. 984–995, 1989.

[62] T. Yardibi, J. Li, P. Stoica, M. Xue, and A. B. Baggeroer, "Source localization and sensing: A nonparametric iterative adaptive approach based on weighted least squares," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 46, no. 1, pp. 425–443, 2010.

[63] H. Abeida, Q. Zhang, J. Li, and N. Merabtine, "Iterative sparse asymptotic minimum variance based approaches for array processing," *IEEE Transactions on Signal Processing*, vol. 61, no. 4, pp. 933–944, 2012.

[64] H. L. Van Trees, *Optimum array processing: Part IV of detection, estimation, and modulation theory*. John Wiley & Sons, 2002.

[65] P. Stoica, Z. Wang, and J. Li, "Robust capon beamforming," in *Conference Record of the Thirty-Sixth Asilomar Conference on Signals, Systems and Computers, 2002.*, vol. 1. IEEE, 2002, pp. 876–880.

[66] P. Stoica, P. Babu, and J. Li, "Spice: A sparse covariance-based estimation method for array processing," *IEEE Transactions on Signal Processing*, vol. 59, no. 2, pp. 629–638, 2010.

[67] P. Babu, P. Stoica, and J. Li, "New method of sparse parameter estimation in separable models and its use for spectral analysis of irregularly sampled data," *IEEE Transactions on Signal Processing*, vol. 59, no. 1, pp. 35–47, 2010.

[68] J. A. Nelder and R. Mead, "A simplex method for function minimization," *The computer journal*, vol. 7, no. 4, pp. 308–313, 1965.

[69] R. Pöhlmann, S. Zhang, E. Staudinger, S. Caizzone, A. Dammann, and P. A. Hoeher, "Bayesian in-situ calibration of multiport antennas for DoA estimation: Theory and measurements," *IEEE Access*, vol. 10, pp. 37 967–37 983, 2022.

[70] M.-C. Hua, C.-H. Hsu, W.-J. Liao, C.-C. Yao, T.-H. Yeh, and H.-C. Liu, "Direction-of-arrival estimator using array switching on software defined radio platform," in *2011 IEEE International Symposium on Antennas and Propagation (APSURSI)*. IEEE, 2011, pp. 2821–2824.

[71] M.-C. Hua, C.-H. Hsu, and H.-C. Liu, "Implementation of direction-of-arrival estimator on software defined radio platform," in *Proc. International Symposium on Communication Systems, Networks & Digital Signal Processing (CSNDSP)*. IEEE, 2012, pp. 1–4.

[72] M. Eberhardt, P. Eschlwech, and E. Biebl, "Investigations on antenna array calibration algorithms for direction-of-arrival estimation," *Advances in Radio Science*, vol. 14, pp. 181–190, 2016.

[73] J. Hershberger, T. Pratt, and R. Kossler, "Automated calibration of a dual-polarized SDR radar," in *Proc. IEEE Conference on Antenna Measurements & Applications (CAMA)*. IEEE, 2016, pp. 1–4.

[74] Y. Yang and R. S. Blum, "Phase synchronization for coherent MIMO radar: Algorithms and their analysis," *IEEE Transactions on Signal Processing*, vol. 59, no. 11, pp. 5538–5557, 2011.

[75] M. Krueckemeier, F. Schwartau, C. Monka-Ewe, and J. S. Technische, "Synchronization of multiple USRP SDRs for coherent receiver applications," in *Proc. International Conference on Software Defined Systems (SDS)*. IEEE, 2019, pp. 11–16.

[76] E. Research, "Ettus Research Knowledge Base: TwinRX Properties," https://files.ettus.com/manual/page_dboards.html#dboards_twinrx, 2023, [Accessed on 19-Jul-2023].

[77] Ettus Research, "Ettus Research Knowledge Base: USRP N300/N310," https://kb.ettus.com/N300/N310, 2023, [Accessed on 19-Jul-2023].

[78] N. Instruments, "Product documentation NI-2955," https://www.ni.com/docs/de-DE/bundle/usrp-2955-specs/page/specs.html, 2023, [Accessed on 19-Jul-2023].

[79] M. Viberg, M. Lanne, and A. Lundgren, "Calibration in array processing," in *Classical and Modern Direction-of-Arrival Estimation*. Elsevier, 2009, pp. 93–124.

[80] M. Jansson, A. L. Swindlehurst, and B. Ottersten, "Weighted subspace fitting for general array error models," *IEEE Transactions on Signal Processing*, vol. 46, no. 9, pp. 2484–2498, 1998.

[81] A. B. Gershman, "Robust adaptive beamforming in sensor arrays," *Int. J. Electron. Commun.*, vol. 53, pp. 305–314, 1999.

[82] I. J. Gupta, J. R. Baxter, S. W. Ellingson, H.-G. Park, H. S. Oh, and M. G. Kyeong, "An experimental study of antenna array calibration," *IEEE Transactions on antennas and propagation*, vol. 51, no. 3, pp. 664–667, 2003.

[83] E. Research, "USRP N210 software defined radio (SDR)." https://www.ettus.com/product/details/UN210-KIT, 2023, [Accessed on 19-Jul-2023].

[84] V. Technologies, "Valon 5009 Frequency Synthesizer," https://www.valonrf.com/frequency-synthesizer-6ghz.html, 2023, [Accessed on 19-Jul-2023].

[85] Y. Wang, L. Wang, J. Xie, M. Trinkle, and B. W.-H. Ng, "Doa estimation under mutual coupling of uniform linear arrays using sparse reconstruction," *IEEE Wireless Communications Letters*, vol. 8, no. 4, pp. 1004–1007, 2019.

[86] P. Heidenreich and A. M. Zoubir, "High-resolution direction finding of coherent sources in the presence of model errors using alternating projections," in *2009 IEEE/SP 15th Workshop on Statistical Signal Processing*. IEEE, 2009, pp. 521–524.

[87] S. M. Kay, *Fundamentals of statistical signal processing: estimation theory*. Prentice-Hall, Inc., 1993.

[88] C. Athaudage and K. Sathananthan, "Cramer-rao lower bound on frequency offset estimation error in ofdm systems with timing error feedback compensation," in *2005 5th International Conference on Information Communications & Signal Processing*. IEEE, 2005, pp. 1231–1235.

[89] R. Schmidt, "Multiple emitter location and signal parameter estimation," *IEEE transactions on antennas and propagation*, vol. 34, no. 3, pp. 276–280, 1986.

[90] M. Haardt and J. A. Nossek, "Unitary esprit: How to obtain increased estimation accuracy with a reduced computational burden," *IEEE transactions on signal processing*, vol. 43, no. 5, pp. 1232–1242, 1995.

[91] T.-J. Shan and T. Kailath, "Adaptive beamforming for coherent signals and interference," *IEEE Transactions on Acoustics, Speech, and Signal Processing*, vol. 33, no. 3, pp. 527–536, 1985.

[92] H. Krim and M. Viberg, "Two decades of array signal processing research: the parametric approach," *IEEE signal processing magazine*, vol. 13, no. 4, pp. 67–94, 1996.

[93] W. Roberts, P. Stoica, J. Li, T. Yardibi, and F. A. Sadjadi, "Iterative adaptive approaches to mimo radar imaging," *IEEE Journal of Selected Topics in Signal Processing*, vol. 4, no. 1, pp. 5–20, 2010.

[94] J.-P. Delmas, "Asymptotically minimum variance second-order estimation for noncircular signals with application to doa estimation," *IEEE Transactions on Signal Processing*, vol. 52, no. 5, pp. 1235–1241, 2004.

[95] D. Malioutov, M. Cetin, and A. S. Willsky, "A sparse signal reconstruction perspective for source localization with sensor arrays," *IEEE transactions on signal processing*, vol. 53, no. 8, pp. 3010–3022, 2005.