

UNIVERSIDAD POLITÉCNICA DE MADRID
Escuela Técnica Superior de Ingenieros de Telecomunicación



**Passive Radar Techniques based on
Emerging Illuminators of Opportunity
and Software-Defined Radio**

DOCTORAL THESIS

Submitted for the degree of Doctor by:

Rodrigo Blázquez García
Máster Universitario en Ingeniería de Telecomunicación

Madrid, 2024



UNIVERSIDAD POLITÉCNICA DE MADRID
Escuela Técnica Superior de Ingenieros de Telecomunicación

Doctoral Degree in Electronic Systems Engineering

**Passive Radar Techniques based on
Emerging Illuminators of Opportunity
and Software-Defined Radio**

DOCTORAL THESIS

Submitted for the degree of Doctor by:

Rodrigo Blázquez García

Máster Universitario en Ingeniería de Telecomunicación

Under the supervision of:

Dr. Mateo Burgos García

Dr. Diego Cristallini

Madrid, 2024

Title: Passive Radar Techniques based on Emerging Illuminators of Opportunity and Software-Defined Radio

Author: Rodrigo Blázquez García

Doctoral Programme: Electronic Systems Engineering

Thesis Supervision:

Dr. Mateo Burgos García, Catedrático del Departamento de Señales, Sistemas y Radiocomunicaciones, Universidad Politécnica de Madrid (Supervisor)

Dr. Diego Cristallini, Group Leader of Passive Covert Radar, Fraunhofer Institute for High Frequency Physics and Radar Techniques

External Reviewers:

Thesis Defense Committee:

Thesis Defense Date:

This thesis has been partially supported by the grant FPU15/01253 of the *Ministerio de Educación de España*, the projects EC2014-53815-R and TEC2017-87061-C3-1-R of the *Ministerio de Economía y Competitividad de España*, and the project E/E810/NC005/MF006 of the *Wehrtechnische Dienststelle* (WTD) 81.

A mis abuelos

A mis padres

A mi hermana

A Raquel

"There was once a little man called Niggle, who had a long journey to make."

"He was the sort of painter who can paint leaves better than trees. He used to spend a long time on a single leaf, trying to catch its shape, and its sheen, and the glistening of dewdrops on its edges. Yet he wanted to paint a whole tree, with all of its leaves in the same style, and all of them different."

"Before him stood the Tree, his Tree, finished. If you could say that of a Tree that was alive, its leaves opening, its branches growing and bending in the wind [...]."

Extracts from *Leaf by Niggle*, J.R.R. Tolkien

Acknowledgement

I need to express my most sincere gratitude to all the people who have accompanied and helped me during this longer than expected journey. I am so lucky to have met you all.

Mateo, thank you very much for taking the risk of calling me and letting me collaborate in your projects when I didn't even know what the Fourier transform was. Thank you for everything I have learned from you. If it wasn't for you, this thesis would not exist and my career would probably have been different.

Diego, infinite thanks for giving me the opportunity to come to Fraunhofer FHR and to be part of your group in an exceptional research environment with exciting and motivating projects. Thank you for all the support, discussions, and technical ideas that have helped me to improve and advance in the work presented here.

From my time at the UPM, I would like to thank all the professors and colleagues of the Microwave and Radar group, and especially to Luis, Carlos (x2), Marta (x2), Federico, Mario, Clara, Dani, Elías, Mu, Randy, Álvaro, Fernando, Alba, Juan, Alejandro (x2), Lourdes, Alberto, Javier (x2), José Ignacio, Félix, Joseto, Pablo, Gorka, Víctor, Jordi, Carmen, and Jesús. It is exceptional how much I have learned from all of you and the great atmosphere.

I would also like to thank the entire former department of Passive Radar and Anti-Jamming Techniques of Fraunhofer FHR and other colleagues for having welcomed me and for all the support I have received during these last years, including for the measurement campaigns: Smarty, Philipp, Viktor, Iole, Stefan, Dominik, Thomas, Vichet, Ruben, Wolli, David, Tobi, Miguel, Emil, Torsten, Johen, Matthias, Stephan, Marion, Daniel... To Ferran and Angel, thank you for all the mutual support along this path. To David, thank you for sharing your experiences with me and for all the technical, but also off-topic, discussions. To Theressa, Gusti and their family, thank you for the happiness that you transmit.

The good things of this thesis are also yours.

My thanks to all the reviewers of this thesis for their esteemed time spent in suggesting ideas and improvements that have enhanced the work here presented. Besides, I would like to thank all the institutions that have funded this work, the passive radar community for making this field of knowledge motivating and dynamic, and to the UPM and Fraunhofer FHR for providing the research environment that has made this work possible.

Finally, I don't have enough words to thank my family, friends, Raquel and her family for their endless support and understanding even in the distance. *Os quiero.*

Abstract

The deployment of novel wireless communication systems, such as the new generations of mobile communications (i.e. Long-Term Evolution -LTE- and 5G) or the low-Earth orbit (LEO) communication satellite constellations (e.g. Starlink or OneWeb), offers new possibilities for the development of passive radars with enhanced capabilities using those transmissions as illumination of opportunity. For this reason, this thesis is focused on the analysis, development and experimental validation of passive radar techniques that enable the exploitation of these two emerging illuminators: (i) the LTE mobile communication system whose main application is envisioned in urban or semi-urban areas, and (ii) the novel broadband communication LEO satellite constellations such as Starlink or OneWeb, which are considered of great interest for applications in remote areas. Besides, as an enabling technology to develop and validate passive radar prototypes, the novel commercial-off-the-shelf (COTS) software-defined radio (SRD) devices have been considered.

In order to overcome some current challenges in critical infrastructure surveillance, the potential usage of downlink LTE signals have been analysed, including the estimation of achievable capabilities, the experimental characterization of the LTE signals for passive radar applications, and the design of a system architecture and signal processing.

The validation of the developed LTE-based passive radar and the proposed adaptive techniques based on the use of digital arrays implemented by SDR devices with multiple coherent channels has been performed in field tests with a drone as a cooperative target. The achieved results show the feasibility to detect a small-size drone at a range of up to 250 m from the receiver. However, limitations have been also observed in terms of the continuous availability of the signal in different frequency channels, depending on the transmission of user payload, and the requirement to optimize the considered geometry in order to avoid blind zones. Since the proposed architecture is considered scalable, these limitations and the improvement of target localization and tracking capabilities could be addressed in the future by resorting to a multistatic configuration exploiting several LTE transmitters, given the typically dense network, or deploying multiple receiving nodes.

Regarding the exploitation of the novel broadband communication LEO satellites with global and persistent coverage for passive radar applications, the performed analyses demonstrate the technical feasibility and the promising achievable capabilities compared to other satellite-based illuminators of opportunity such as Digital Video Broadcasting-Satellite or the Global Navigation Satellite Systems. Besides, the developed architecture and systems have been validated in two field tests focused, respectively, in the measurement of scattered signals from clutter or static elements of the monitored area, and of scattered signals of a medium-sized drone as a cooperative moving target. The achieved results, which could be considered preliminary in the sense that are expected to be improved by applying more advanced signal processing techniques based, for example, on motion compensation or by selecting a reference satellite that optimizes the bistatic geometry, already demonstrate the feasibility to detect distinctive elements of the monitored area or a medium-sized drone at a range of at least 150 m using a 30 degree-beamwidth antenna for the surveillance channel.

Therefore, the results obtained in this thesis open new possibilities and enable emerging techniques in the context of multistatic surveillance applications in urban environments based on passive radar nodes exploiting mobile communication signals, and of persistent remote area or infrastructure monitoring, for example, for avalanche detection, deploying ground-based receivers that exploit the novel broadband communication LEO satellites.

Resumen

El despliegue de nuevos sistemas de comunicaciones inalámbricas, como las nuevas generaciones de comunicaciones móviles (Long-Term Evolution -LTE- y 5G) o las constelaciones de satélites de comunicaciones en órbita terrestre baja (LEO) (como OneWeb o Starlink), ofrecen nuevas posibilidades para el desarrollo de radares pasivos con capacidades mejoradas empleando dichas transmisiones como iluminadores de oportunidad. Por ello, esta tesis se centra en el análisis, desarrollo y validación experimental de técnicas de radar pasivo que permiten el uso de estos iluminadores emergentes: (i) el sistema de comunicaciones móviles LTE para aplicaciones en zonas urbanas o semiurbanas, y (ii) los nuevos satélites LEO de comunicaciones de banda ancha, de gran interés para aplicaciones en zonas remotas. Además, como tecnología habilitadora para desarrollar y validar prototipos de radares pasivos, se han considerado los nuevos dispositivos comerciales de radio definida por software (SDR).

Con el objetivo de abordar los retos actuales en la vigilancia de infraestructuras, se ha analizado el uso de las señales del enlace descendente del sistema LTE, incluyendo la estimación de las capacidades potenciales, la caracterización experimental de dichas señales para aplicaciones de radar pasivo y el diseño de una arquitectura de sistema y del procesado de señal.

Para la validación del sistema desarrollado basado en LTE y de las técnicas adaptativas propuestas centradas en el uso de un array digital implementado mediante dispositivos SDR con múltiples canales, se han realizado pruebas de campo con un dron como blanco cooperativo. Los resultados muestran la capacidad de detectar drones de pequeño tamaño a una distancia de hasta 250 m del receptor. Sin embargo, también se han observado limitaciones en términos de la disponibilidad continua de la señal en diferentes canales de frecuencia, dependiente de la transmisión de datos de usuario, y la necesidad de optimizar la geometría del sistema para evitar zonas ciegas. Dado que la arquitectura propuesta se considera escalable, estas limitaciones y la mejora de la localización y seguimiento de blancos podrían abordarse recurriendo a una configuración multiestática que explote varios transmisores LTE o desplegando múltiples nodos receptores.

En cuanto al empleo de los nuevos satélites de comunicaciones LEO con cobertura global y persistente para aplicaciones de radar pasivo, los análisis realizados demuestran su viabilidad técnica y mejores capacidades potenciales en comparación con otros iluminadores satelitales, como el sistema de difusión de vídeo digital por satélite o los sistemas globales de navegación por satélite. Además, los sistemas desarrollados han sido validados en dos pruebas de campo centradas, respectivamente, en la medida de señales reflejadas por clutter o elementos estáticos del área monitorizada, y de señales reflejadas por un dron de tamaño medio como blanco móvil cooperativo. Los resultados obtenidos, que podrían considerarse preliminares en el sentido de que podrían mejorarse aplicando técnicas más avanzadas de procesado de señal basadas, por ejemplo, en la compensación de movimiento o seleccionando adaptativamente el satélite de referencia que optimice la geometría biestática, demuestran la viabilidad para detectar elementos característicos del área monitorizada o un dron de tamaño medio a un alcance de al menos 150 m del receptor utilizando una antena de 30 grados de ancho de haz para el canal de vigilancia.

Los resultados de esta tesis abren nuevas posibilidades y habilitan técnicas emergentes en aplicaciones de vigilancia multiestática para entornos urbanos basadas en nodos radar pasivos que explotan las señales de comunicaciones móviles, y de monitorización persistente de áreas remotas, por ejemplo, para la detección de avalanchas, desplegando receptores terrestres que explotan las señales transmitidas por las nuevas constelaciones LEO de comunicaciones de banda ancha.

Contents

Acknowledgement	ii
Abstract	iii
Resumen	v
List of Figures	xi
List of Tables	xix
Acronyms and Abbreviations	xx
I INTRODUCTION	1
1 Introduction	3
1.1 Urban and critical infrastructure surveillance: LTE-based passive radar . . .	6
1.2 Remote area surveillance: Broadband communication LEO satellite-based passive radar	9
1.3 Objectives and organization of the Thesis	10
1.3.1 Objectives	10
1.3.2 Thesis organization	11
1.4 List of publications	12
1.5 Supervised MSc and BSc theses	15
2 Passive Radar: Principles and Concepts	17
2.1 Passive radar architectures and geometry	18
2.1.1 Passive radar architectures	18
2.1.2 Bistatic geometry	21

2.1.3	Bistatic radar equation	23
2.1.4	Signal model and ambiguity function	25
2.2	Passive radar processing	28
2.2.1	Digital beamforming	30
2.2.2	DSI and clutter removal	32
2.2.3	Range compression and Doppler processing	33
II	LONG-TERM EVOLUTION-BASED PASSIVE RADAR	37
3	LTE-Based Passive Radar System: Analysis, Design and Developments	39
3.1	Motivation of high-speed railways surveillance	40
3.2	Analysis of LTE as illumination of opportunity	42
3.2.1	LTE-R specifications and downlink waveform	42
3.2.2	Self ambiguity function analysis of downlink LTE signals	45
3.3	LTE-R based passive radar system design	49
3.3.1	Hardware architecture	49
3.3.2	Signal processing and multistatic data fusion	53
3.4	Estimation of covered area and simulation results	55
4	LTE-Based Passive Radar System: Experimental Validation	61
4.1	Description of the measurement scenario	61
4.1.1	LTE base station	62
4.1.2	Passive radar receiver	63
4.1.3	Cooperative target	64
4.2	Scenario analysis	65
4.3	Received signal analysis	69
4.4	Target detection results	72
4.5	Conclusions	81

III BROADBAND COMMUNICATION LEO SATELLITE-BASED PASSIVE RADAR

85

5 Broadband Communication LEO Satellite-Based Passive Radar System: Analysis, Design and Developments	87
5.1 Overview of emerging satellite-based illuminators of opportunity	88
5.2 Starlink and OneWeb satellite constellations	92
5.3 Passive radar system architecture	97
5.4 Experimental passive radar prototypes	101
5.5.1 Maximum detection performance and range resolution	105
5.5.2 Required tracking antenna azimuth and elevation rate	109
5.5.3 Estimated accuracy of satellite position predictions	110
5.5.4 Range and Doppler migration effects	113
5.5.5 SAR and polarimetric modes	115
5.6 Experimental signal characterization for passive radar applications	122
5.6.1 Starlink signals	122
5.6.2 OneWeb signals	127
6 Broadband Communication LEO Satellite-Based Passive Radar: Experimental Validation	133
6.1 Area monitoring measurements	134
6.1.1 Measurement description	134
6.1.2 Measurement results	138
6.2 Drone detection measurements	162
6.3 Conclusions	164
IV CONCLUSIONS	167
7 Conclusions and Future Work	169
7.1 Conclusions	169

7.2 Future research lines	171
Bibliography	173

List of Figures

1.1	Application scenarios of LTE and LEO satellite constellations as illuminators of opportunity	5
1.2	Single-node passive radar architecture based on downlink LTE signals for drone detection in urban environments	8
1.3	Block diagram of passive radar signal and data processing based on the range-Doppler cross-correlation	8
2.1	Passive radar system architectures	20
2.2	Bistatic geometry	21
2.3	Dynamic 3D bistatic/multistatic geometry for passive radar simulation . . .	25
2.4	Normalized spectrum of user downlink channels	26
2.5	Comparison of simulated and measured Astra 19.2°E signals	27
2.6	AF of a simulated Astra 19.2° signal	29
2.7	Common passive radar processing chain	30
2.8	Batches algorithm	34
2.9	Keystone Transform for first-order motion compensation	36
3.1	Diagram of the proposed LTE-R based passive multistatic radar approach. .	41
3.2	Frame structure of downlink LTE-R signals	44
3.3	Reconstruction processing of downlink LTE signal	44
3.4	Receiving setup used for LTE signal characterization	45
3.5	Normalized power spectrum of a measured 10 MHz-channel downlink LTE signal at the 800 MHz band	46

3.6	Received constellation for the Physical Downlink Shared Channel (PDSCH) of LTE after channel equalization	46
3.7	Normalized range-Doppler AF of a reconstructed 10 MHz-channel downlink LTE signal	47
3.8	AF zero-Doppler cut and zero-range cut of a reconstructed downlink LTE signal	48
3.9	Acquisition of a 50 ms-LTE signal with 20 MHz channel bandwidth	50
3.10	Normalized range-Doppler AF of a received 20 MHz-channel downlink LTE signal	51
3.11	Geometrical deployment of the suggested passive multistatic radar system . .	52
3.12	Hardware architecture of the passive multistatic radar system	52
3.13	Block diagram of the signal processing applied in each receiving node of the passive multistatic radar system	54
3.14	Reference and surveillance synthesized beams of the receiver node 1	55
3.15	Estimation of the covered area by the passive multistatic radar system for the detection of cars, pedestrians and small drones	56
3.16	SNR in dB for the receiver 1 of a small drone with 0.1m^2 RCS when using the reference signal of the eNodeB 1 and the reference signal of the eNodeB 2 . .	58
3.17	Range-Doppler cross-correlation function between the LTE reference signal and a simulated surveillance channel applying or not DSI and multipath cancellation	60
4.1	Measurement campaign scenario	62
4.2	Estimated EIRP of the considered LTE base station as a function of the azimuth angle	63
4.3	Configuration of the antennas connected to the USRP-2945 forming a non-calibrated non-uniform linear array	64
4.4	Cooperative target and conducted flights during the measurements.	65
4.5	Estimated target SNR and target-to-direct signal power ratio for the LTE channel centered at 930 MHz with 10 MHz bandwidth	67
4.6	Estimated target SNR and target-to-direct signal power ratio for the LTE channel centered at 1870 MHz with 20 MHz bandwidth.	68

4.7	Analysis of the bistatic geometry: Bistatic range, Doppler frequency and bistatic angle	69
4.8	Received IQ signal on channel 1 and spectra of the received signals on the four channels for an LTE channel centered at 930.1 MHz with 10 MHz bandwidth	70
4.9	Received IQ signal on channel 1 and spectra of the received signals on the four channels for an LTE channel centered at 1869.9 MHz with 20 MHz bandwidth	71
4.10	Histograms of the digitised voltage values for the considered acquisitions intervals of the frequency channels at 930 MHz and 1870 MHz	72
4.11	Range-Doppler maps computed as the autocorrelation of the signals recorded by channel 1 for recordings of the 930 MHz and the 1870 MHz LTE channels during a flight of the drone	73
4.12	Range-Doppler maps for several time intervals computed as the autocorrelation of the signals recorded by channel 1 for the 1870 MHz LTE channel	74
4.13	Proposed signal processing for the computation of the range-Doppler maps based on adaptive digital beamforming	75
4.14	Range-Doppler maps applying the proposed adaptive digital beamforming and both the digital beamforming and ECA for a recordings of the 930 MHz and 1870 MHz-LTE channels during a flight of the drone	78
4.15	Sequence of range-Doppler maps obtained for the 930 MHz-LTE channel measurements during a flight of the drone	79
4.16	System geometry showing the directions of arrival of the drone signals and of the direct signal from the LTE transmitter	80
5.1	Number of satellite launches promoted by commercial, governmental and academic/non-profit institutions	89
5.2	Starlink and OneWeb planned satellite constellations	93
5.3	Percentage of time as a function of the number of visible satellites for the OneWeb and Starlink planned constellations	94
5.4	Bidirectional links for broadband LEO communication satellites	95
5.5	Frequency plan of Starlink and OneWeb communication satellites	95

5.6	Illuminating spot beam patterns of a Starlink satellite	96
5.7	Illuminating spot beam patterns of a OneWeb satellite	96
5.8	Proposed passive radar system architecture for target detection applications	97
5.9	Diagram with computation steps to estimate satellite azimuth, elevation and skew in the antenna-body coordinate system from TLE data	98
5.10	Diagrams of the considered local Earth-fixed coordinate system at the position of the antenna and of the body-fixed antenna coordinate system	99
5.11	Proposed passive radar system architecture for imaging application including multiple surveillance channels	101
5.12	SABBIA 2.0 front-end block diagram for one of channel	102
5.13	Rack of SABBIA 2.0 passive radar system	102
5.14	Portable 8U 19" rack including the USRP X310, reference signal generation, power supply and recording and control computer	103
5.15	Block diagram of the developed system based on a COTS SDR	103
5.16	Antenna module options for LEO satellite signal acquisition	105
5.17	Exemplary spectra of received signals with the USRP X310-based system and Kymeta antennas	106
5.18	Estimated SNR for ground targets of different radar cross sections (RCS) considering two antenna configurations of the surveillance channel (high-gain narrow beam and low-gain wide beam)	107
5.19	Spot beam footprints dB for two positions of a Starlink satellite	109
5.20	Achievable range resolution on Earth surface and iso-range contours for two positions of a Starlink satellite	110
5.21	Analysis of a near-zenith pass of a Starlink satellite	111
5.22	Box plots of satellite position propagation errors in RTC coordinates for the STARLINK-1007 satellite based on historical analysis of TLE data and using SGP4 propagation method	112
5.23	Bistatic range and Doppler migration of a stationary ground target as a function of its position for an integration time of 1 s and a near-zenith Starlink satellite position	114

5.37 Normalized autocorrelation computed with a CPI of 80 ms of a pulsed transmission from a Starlink satellite	128
5.38 Normalized spectrogram of a received signal from a OneWeb satellite	129
5.39 Normalized range-Doppler ambiguity function computed using 100 ms CPI from a received OneWeb user-downlink signal	130
6.1 Satellite view of Erpeler Ley showing the deployment location of the passive radar system and the sector with visibility over the Rhine valley	134
6.2 View of the Rhine valley in the direction of the surveillance channels during the measurements	135
6.3 Antenna setups used for the measurement campaign	135
6.4 Figure of the trial location showing the antennas and the recording system SABBIA 2.0	136
6.5 Figure of the trial location showing the view across the Rhein valley	137
6.6 Figure of the trial location showing the reference Kymeta antenna and the view across the Rhein valley	138
6.7 Approximate estimation of the instantaneous footprint of the surveillance Kymeta and horn antennas	139
6.8 Sky plot of the tracked satellites during the measurements with signal reception	140
6.9 Spectrograms of the signals recorded for 113 s with a center frequency of 11.2 GHz during a pass of the STARLINK-3943 satellite	141
6.10 Azimuth and elevation of satellites being tracked by the reference Kymeta antenna	142
6.11 Sky plot of the satellite passes and projection over an Earth map of the satellites crossing the cone defined by an elevation higher than 40° during the considered measurement	143
6.12 Averaged amplitude level along time in both digitised frequency channels for the four considered antennas	143
6.13 Spectrogram of the central 1 MHz-band of the upper frequency channel for the received signals with the reference Kymeta and horn antennas	146

6.14 Spectrum at the center of the upper frequency channel of the received signal by the reference Kymeta antenna at several recording times	146
6.15 Automatic pilot detections and estimated Doppler frequency for the tracked satellites over the spectrogram computed for the received signals with the reference Kymeta antenna	147
6.16 Range-Doppler map obtained by cross-correlating the reference signal received by the Kymeta antenna tracking a Starlink satellite and the surveillance signal received by a horn antenna using a CPI of 3 s	149
6.17 Zoom of the range-Doppler map in which clutter scattered signals are observed with low SNR	149
6.18 Spectrograms of the signals recorded during 162 s for a center frequency of 11.2 GHz with the four channels during a pass of the ONEWEB-0446 satellite.	150
6.19 Azimuth and elevation of the ONEWEB-0446 satellite being tracked by the reference Kymeta antenna during the considered recording	150
6.20 Sky plot of the satellite passes and projection over an Earth map of the satellites crossing the cone defined by an elevation higher than 40° during the considered measurement	151
6.21 Averaged amplitude level along time in both digitised frequency channels for the four considered antennas	152
6.22 Range-Doppler map computed with a 0.54 s CPI by cross-correlating the reference OneWeb signal received with the Kymeta antenna and the surveillance signal received with the horn antenna	153
6.23 Bistatic range, bistatic Doppler frequency and bistatic Doppler frequency rate for the monitored area	154
6.24 Iso-range and iso-Doppler curves over an altitude map of the monitored area	155
6.25 Surface points in line of sight from a grid spanning a ±45° azimuth sector around the antenna pointing direction	156
6.26 Projection of LOS points inside the surveillance antenna beamwidth over the computed range-Doppler map	157
6.27 Projection of surface points onto the range-Doppler domain	157

6.28 Range-Doppler map projected onto a geographic coordinate system around the receiver location	158
6.29 Range-Doppler map projected onto a geographic coordinate system around the receiver location and compared with a satellite image from Google Earth . .	159
6.30 Range-Doppler map computed with a 0.54 s CPI by cross-correlating the reference signal received with the Kymeta antenna and the surveillance signal received with the horn antenna for a later time	160
6.31 Max-hold over the range-Doppler maps with CPI 0.54 s computed during 8.7 s for the considered OneWeb acquisition	161
6.32 Measurement scenario to validate the target detection capabilities	162
6.33 Drone detection results: Range-Doppler map with a CPI of 0.36 s and non-coherent integration of range-Doppler maps with CPI 0.36 s computed during 3 seconds	163

List of Tables

1.1	Drone detection and classification technologies	7
3.1	LTE-R System Parameters	43
3.2	Parameters used for the estimation of the covered area	56
4.1	Frequency bands assigned to the considered LTE base station.	62
4.2	Transmitter, receiver and target parameters used in the estimation of target SNR, target-to-direct signal power ratio and direct signal SNR.	66
5.1	Main characteristics of Starlink constellation, LEO SAR constellations, TerraSAR-X and GNSS constellations	91
5.2	Starlink and OneWeb constellation parameters	93
5.3	System parameters considered for the power budget analysis.	106
6.1	Main properties of the considered antenna setups.	135
6.2	Position and tilting (relative to zenith) of the surveillance antennas.	137

Acronyms and Abbreviations

ADC Analog-to-Digital Converter

AF Ambiguity Function

AGC Automatic Gain Control

CA-CFAR Cell-Averaging Constant False Alarm Rate

CCF Cross-Correlation Function

CFAR Constant False Alarm Rate

CHAD Doppler Channel Detector

COTS Commercial Off-The-Shelf

CPI Coherent Processing Interval

DAB Digital Audio Broadcasting

DC Direct Current

DoA Direction of Arrival

DSI Direct Signal Interference

DVB-T Digital Video Broadcasting-Terrestrial

DVB-S Digital Video Broadcasting-Satellite

ECA Extensive Cancellation Algorithm

ECA-B Extensive Cancellation Algorithm-Batches

ECEF Earth-Centered Earth-Fixed

ECI Earth-Centered Inertial

EIRP Equivalent Isotropic Radiation Power

EKF Extended Kalman Filter

ENU East, North, Up

EOP Earth Orientation Parameters

ERTMS European Rail Traffic Management System

ETSIT Escuela Técnica Superior de Ingenieros de Telecomunicación

FCC Federal Communications Commission

FDD Frequency Division Duplex

FFT Fast Fourier Transform

FHR Fraunhofer Institute for High Frequency Physics and Radar Techniques

FM Frequency Modulation

FOV Field-of-View

FPGA Field Programmable Gate Array

FSR Forward Scattering Radar

FSS Fixed-Satellite Service

GEO Geosynchronous Equatorial Orbit

GMTI Ground Moving Target Indicator

GNSS Global Navigation Satellite System

GPS Global Positioning System

GSM Global System for Mobile communications

GSM-R Global System for Mobile communications-Railway

HSR High-Speed Railways

IF Intermediate Frequency

IFFT Inverse Fast Fourier Transform

IMU Inertial Measurement Unit

ISAC Integrated Sensing and Communication

IQ In-phase, Quadrature

JCAS Joint Communication and Sensing

KT Keystone Transform

LEO Low-Earth Orbit

LHCP Left-Handed Circular Polarization

LNB Low-Noise Block

LOS Line-of-Sight

LS Least Squares

LTE Long-Term Evolution

LTE-R Long-Term Evolution-Railway

MIMO Multiple-Input Multiple-Output

- MRC** Maximum Ration Combining
- MVDR** Minimum Variance Distortionless Response
- NVMe** Non-Volatile Memory Express
- OFDM** Orthogonal Frequency-Division Multiplexing
- PCIe** Peripheral Component Interconnect Express
- P_d** Probability of Detection
- PDSCH** Physical Downlink Shared Channel
- P_{fa}** Probability of False Alarm
- PNT** Positioning, Navigation and Timing
- PRI** Pulse Repetition Interval
- PSS** Primary Synchronization Signal
- QAM** Quadrature Amplitude Modulation
- QPSK** Quadrature Phase-Shift Keying
- RCS** Radar Cross Section
- RF** Radio Frequency
- RHCP** Right-Handed Circular Polarization
- RS** Reference Signals
- RTC** Radial, Transverse, Cross-Track
- SC-FDMA** Single-Carrier Frequency Division Multiple Access
- SC-TDM** Single-Carrier Time Division Multiplexing
- SDP4** Simplified Deep Space Perturbations Model 4
- SDR** Software-Defined Radio
- SGP4** Simplified General Perturbations Model 4
- SINR** Signal-to-Interference-plus-Noise Ratio
- SIR** Signal-to-Interference Ratio
- SNR** Signal-to-Noise Ratio
- SPCS** Space Control Squadron
- SSD** Solid-State Drive
- SSS** Secondary Synchronization Signal

STAP Space-Time Adaptive Processing

TBD Track-Before-Detect

TLE Two Line Elements

TMC Target Motion Compensation

ULA Uniform Linear Array

UPM Universidad Politécnica de Madrid

UTC Coordinated Universal Time

WGS84 World Geodetic System 84

WiFi Wireless-Fidelity

ZF Zero-Forcing

Part I

INTRODUCTION

Chapter 1

Introduction

The development and deployment of novel wireless communication systems, such as the new generations of mobile communication systems (i.e. Long-Term Evolution -LTE- and 5G) [Dah16] or Fixed-Satellite Services (FSS) based on low-Earth orbit (LEO) satellite constellations [Su19], offers new possibilities for the development of passive radars [Gri22; Mal19] with enhanced capabilities using those transmissions as illumination of opportunity. In addition, these communication systems are commonly based on the deployment of a dense transmitter network (ground-based or space-borne) and, therefore, they might be suitable to implement a multistatic radar architecture with multiple transmitters and receivers that improve robustness, spatial diversity and three-dimensional target localization [Che98; OHa18; Ngu19] in order to overcome some of the current challenges in critical infrastructure surveillance, such as the detection and tracking of drones or other targets with low detectability, both in urban and remote areas.

In contrast to conventional monostatic radars, passive radars exploit existing broadcast and communication signals, usually called illumination of opportunity, in order to sense the environment and detect and track targets. Therefore, since they do not require a dedicated transmitter, passive radars usually present a lower cost. They do not need licensing or spectrum allocation and are based on the efficient reuse of the already congested electromagnetic spectrum. Since the location of the receiver is covert, it is more complex to deploy effective

countermeasures such as jamming against them [Gri05]. In addition, bistatic and forward scattering geometries usually provide enhanced detection of stealth targets [Gri22; Sub11].

However, the non-cooperative transmissions used as illumination of opportunity in passive radars are not optimized for radar usage. For this reason, the suitability of these waveforms should be analysed, for example by means of the ambiguity function [Bak05] in order to determine their associated resolution and sidelobe level properties and, in digital systems, the possible occurrence of ambiguities due to the pilot, signal and frame structure that may impact on the performance of the passive radar. The analysis of the transmitted waveforms is also required to propose an optimal signal processing that allows the detection of weak moving targets masked by the direct signal interference (DSI) or multipath (i.e. static clutter) components [Col09].

In this regard, novel digital communication systems present additional system complexity and adaptive capabilities, such as the use of digital beamforming [Li04], MIMO (multiple-input multiple-output) techniques [Li10] such as spatial diversity and spatial multiplexing [Loz10], adaptive coding and modulation [Bis10], spread-spectrum or Orthogonal Frequency-Division Multiplexing (OFDM) modulations [Sch05], or total transmitted power and effective bandwidth depending on the propagation channel properties and network load [Gho10], that may pose new challenges in their usage as illumination of opportunity and associated passive radar signal processing compared to previously developed passive radars based on both analogue or digital broadcast, communication and radionavigation systems such as Frequency Modulation (FM) radio [Col13], Digital Audio Broadcasting (DAB) [Sch17], Digital Video Broadcasting-Terrestrial (DVB-T) [Pal12; Con12], Wireless-Fidelity (WiFi) [Col12], Digital Video Broadcasting-Satellite (DVB-S) [Umm20] or Global Positioning System (GPS) [Ma18], among others.

Therefore, the potential usage of downlink LTE signals and of LEO FSS signals as emerging illuminations of opportunity to develop passive radars mainly aimed for urban and remote area surveillance, respectively, has been researched in this doctoral thesis including the design, simulation, implementation and experimental validation of the systems and their associated signal processing. Both communication systems offer important properties as illumination of

opportunity for high-resolution passive radars, but their typical deployment and operation makes them suitable for complementary application scenarios, as shown in Figure 1.1. LTE systems are typically available in urban or semi-urban areas, while the global and persistent coverage of the novel LEO satellite constellations enables their exploitation especially in remote areas (i.e. rural, mountainous, oceanic or poles) where terrestrial communications infrastructures do not provide coverage.

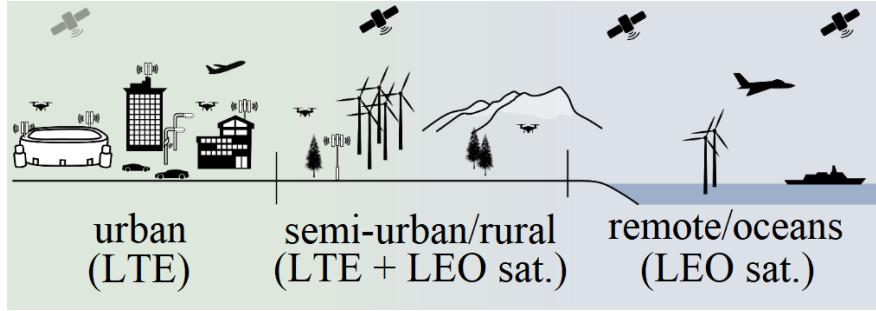


Figure 1.1: Complementary application scenarios of LTE mobile communication system and LEO satellite constellations as illuminators of opportunity for passive radar applications.

For this reason, the analysis and validation of the proposed LTE-based passive radar system has been focused on the surveillance application of critical infrastructure, specifically of high-speed rail networks, against emerging threats due to the negligent or malicious use of drones. On the other hand, the analysis and validation of the proposed passive radar based on broadband communication LEO satellite constellations have also addressed the surveillance and monitoring of remote areas, including the measurement of scattered signals from clutter, opening new possibilities for novel remote sensing applications such as avalanche detection [OHa20].

Although passive radar systems typically require more stringent receiver requirements than communications systems, advances in software-defined radio (SDR) devices in recent years have enabled the development and prototyping of flexible and modular passive radars. The availability of commercial off-the-shelf (COTS) SDR equipment [Ulv10; Cha18; Gom18] with enhanced capabilities, particularly with respect to its instantaneous bandwidth, dynamic range, number of coherent channels and noise figure, has raised the interest in validating this technology for the development of passive radar systems [Ber10] with multiple channels [Pet15], operating in multiple bands [Jęd22] or based on digital array techniques [Alm23;

Núñ23]. These advances and the reduction of costs have also promoted the development of multistatic or netted passive radar systems [Gen20a] that exploit spatial diversity to improve target detection, localization and tracking [Bea22; Cha14]. For these reasons, this thesis has made use of this SDR technology as a key element in the development and validation of the proposed systems and techniques.

1.1 Urban and critical infrastructure surveillance: LTE-based passive radar

Recently, the exponential increase in the use of consumer drones has exposed the need to develop novel surveillance systems against the malicious or negligent use of these platforms [Jac19]. These surveillance systems, commonly referred to as anti-drone systems, must perform three fundamental functions: detection, classification and threat neutralization [Shi18].

To detect and classify small drones, surveillance systems based on various technologies, described in Table 1.1, have been suggested [Shi18]. In open scenarios, such as isolated critical infrastructures or airports, one of the most efficient solutions is the integrated use of active medium-range high-resolution ground radars [dQue19], also based on Multiple-Input Multiple-Output techniques [Kla16], for target detection with optical sensors or micro-Doppler analysis [Gar19] for threat classification. However, as these systems require a direct line of sight to the target, they are not completely suitable for urban environments, where buildings greatly limit their range. Moreover, their high cost hampers the deployment of sensor networks to overcome these line-of-sight blocking problems. Besides, active radars require transmission licenses which may be limited in certain application scenarios, e.g. around critical infrastructure such as airports.

Novel approaches of the state-of-the-art are based on the fusion of multiple sensing sources and technologies [Sva22], including passive radars [Jov18; Jov21]. Besides, multiple experimental passive radar systems based on different illuminations of opportunity such as DVB-T [Fan18; Mar20; del19], DVB-S [Sei22] or WiFi [Mar17], among others, with bistatic,

Table 1.1: Drone detection and classification technologies

<i>Technology</i>	<i>Measuring principle</i>	<i>Challenges</i>
Acoustic sensors [Cas08]	Microphone arrays that detect sound emissions from drones and estimate their direction of arrival	<ul style="list-style-type: none"> - Limited range - Affected by other noise sources - Not suitable for fixed-wing drone detection
Optical sensors [Mül17; Kan20]	Visible light or infrared surveillance cameras that detect drones by image processing	<ul style="list-style-type: none"> - Affected by weather and light conditions - For long ranges, they require a narrow field of view (FOV) that limits the volumetric scanning speed
Radio frequency monitoring [Ngu16]	Detection and angle of arrival estimation of radio frequency emissions from the drone or its associated remote control	<ul style="list-style-type: none"> - Not suitable for autonomous drones without communication links - Several sensor nodes are required for localization
Active ground radars [Och17]	Monostatic mid-range radars that detect the reflection of the transmitted signal on the targets	<ul style="list-style-type: none"> - Only suitable for open areas (e.g. isolated critical infrastructures or airports) - High cost

multistatic [Lü19] or forward-scattering [Raj20] configurations have been developed in the last years for drone detection applications.

As shown in the exemplary single-node architecture of Figure 1.2, most of these works, which are based on digital transmissions, have highlighted the importance of receiving the transmitted signals (i.e. direct signal) with a sufficient signal-to-noise ratio (SNR) and without multipath components, or of reconstructing it by demodulation and remodulation, in order to achieve a higher Direct Signal Interference (DSI) and multipath cancellation in the surveillance channel when applying a common passive radar signal processing (Figure 1.3) [Lom12]. In this way, weak targets with low Radar Cross-Sections (RCS), such as drones, can be detected, which would otherwise remain covered by the sidelobes caused by the DSI and multipath components in the range-Doppler maps.

In addition to the approaches and results of this thesis, multiple works have been also presented based on the exploitation of mobile communication systems such as Global System

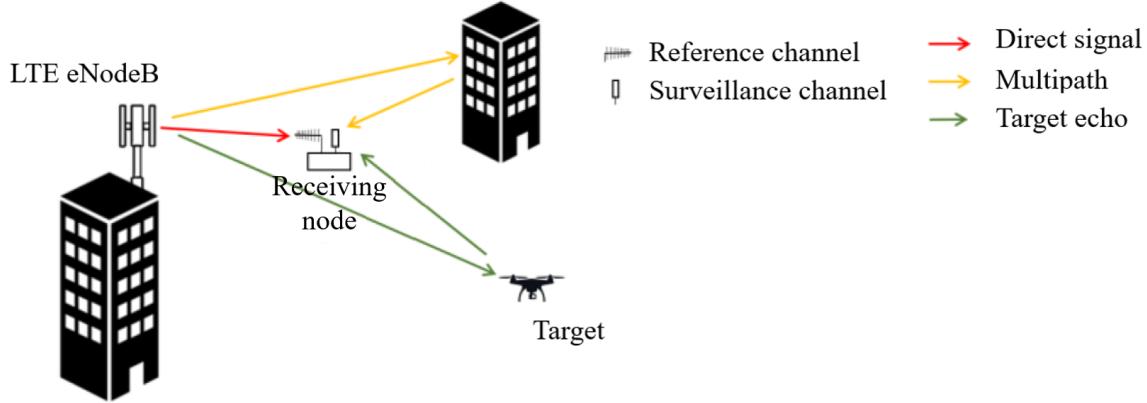


Figure 1.2: Exemplary single-node passive radar architecture based on downlink LTE signals transmitted by base stations (i.e. evolved Node B –eNodeB–) for drone detection in urban environments. The main received signal components in the reference and surveillance channels are also shown.

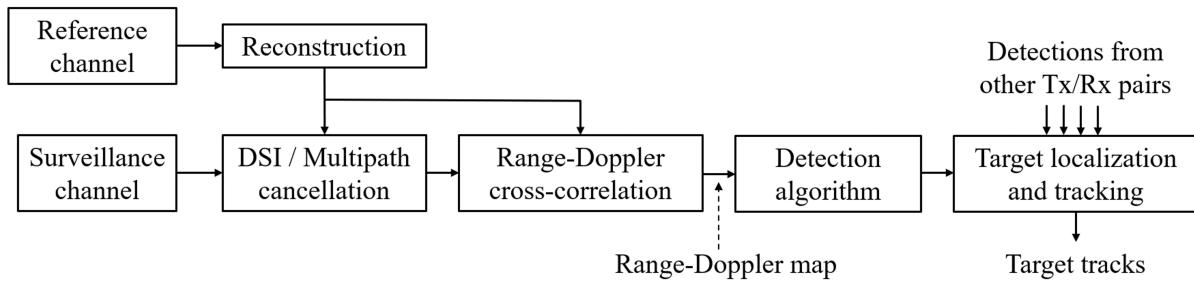


Figure 1.3: Common passive radar signal and data processing based on the range-Doppler cross-correlation between the reference and the surveillance signals.

for Mobile Communications (GSM) [Tan05; Kno20] and LTE [Gen20b; Tay23], and most recently the emerging 5G and 6G systems [Mak22; Sam21; Abr23; Ksi23; Lin22; Bar19].

In this context, the contributions of this thesis are the analysis, development and validation of a scalable passive radar architecture based on LTE downlink signals and multi-channel COTS SDR devices for the surveillance of critical infrastructures, specifically high-speed railway networks, against drone threats. Besides, to address the main limitation for the detection of low RCS targets even at closed ranges due to DSI or main multipath components, the use of adaptive digital beamforming techniques which do not require the calibration of the array has been proposed and experimentally validated.

1.2 Remote area surveillance: Broadband communication LEO satellite-based passive radar

In the last few years, several companies have applied to the US Federal Communications Commission (FCC) for broadcast licenses to operate global internet services using LEO satellite constellations [Del19]. Among others, Starlink, OneWeb, Telesat or Project Kuiper have planned and started to deploy dense networks of LEO satellite constellations to globally and persistently offer FSS and broadband internet access. Starlink, in particular, with a satellite launching rate never seen before, has almost fully deployed its planned first-phase constellation composed of 4,425 satellites in 83 orbital planes, including both polar and non-polar orbits, and has recently started to launch satellites of its second-phase constellation in order to provide low-latency high-speed internet access mainly aimed for rural or remote areas [Spa16].

The frequency bands used for these services are in the Ku- and Ka-bands for the user and gateway links, respectively. In addition, the effective radiated power (ERP), bandwidth and lower propagation attenuation of these satellite signals, compared to GPS or geosynchronous DVB-S satellites, represent very attractive characteristics for passive radar applications [Say19].

Passive radar systems using space-based transmitters have gained attention in the last years given their relevant capabilities in terms of [Cri18]: (i) global illumination of the Earth surface including remote areas and oceans, (ii) permanent surveillance in all-weather and light conditions, (iii) redundancy of the illumination due to the dense constellation, and (iv) robustness against natural disasters or physical attacks. Several passive radar systems based on transmissions from DVB-S/DVB-S2 [Pis20], Global Navigation Satellite Systems (GNSS) [Ma17], Synthetic Aperture Radars (SAR) [Beh15; Bár15] or communication satellites such as Iridium [Dan17] have been developed and experimentally validated for target detection [San20] and imaging [Pis19] applications. However, the novel possibilities and advantages that offer the emerging broadband communication LEO satellite constellations such as Starlink or OneWeb, in addition to their recent availability, have increased the interest in investigating

techniques to opportunistically exploit their signals in the context of passive radar [Blá22a; Gom22b; Blá22b; Gom23a; Blá23a; Gom23b; Blá23b; Blá23c] and Positioning, Navigation and Timing (PNT) [Nei21a; Nei23; Jar23] applications.

For these reasons, the exploitation of user-downlink signals from Starlink and OneWeb satellites as illumination of opportunity for passive radar applications has been considered in this thesis, contributing to the theoretical analysis, architecture design, system development, and experimental validation of this emerging but promising technology.

1.3 Objectives and organization of the Thesis

1.3.1 Objectives

This thesis is focused on the analysis, development and experimental validation of passive radar techniques that enable the exploitation of two emerging illuminators of opportunity: (i) the LTE mobile communication system whose main application is envisioned in urban or semi-urban areas, and (ii) the novel broadband communication LEO satellite constellations such as Starlink or OneWeb, which are considered of great interest for applications in remote areas. Besides, as an enabling technology to develop and validate passive radar system prototypes the novel COTS SRD devices have been considered.

The main objectives addressed by this thesis are as follows:

- Theoretically analyse the characteristics of the LTE and LEO communication satellite systems and estimate of the achievable capabilities by exploiting their user-downlink signals as illumination of opportunity for passive radar applications, in order to show the technical feasibility.
- Experimentally characterize the user-downlink LTE and LEO communication satellite signals for passive radar applications in terms of the evaluation of their ambiguity function.

- Design and develop the associate passive radar system architecture, with focus on the use of COTS SDR devices, and signal processing in order to enable the exploitation of the considered illuminations of opportunity.
- Experimentally validate the use of LTE and LEO communication satellite user-downlink signals as illuminators of opportunity for passive radar application by performing field trials with cooperative targets, and assess their limitations based on the obtained results.

1.3.2 Thesis organization

This doctoral thesis is divided in four parts devoted, respectively, to: (i) the introduction and presentation of basic principles and concepts; (ii) the analyses and results associated to the LTE-based passive radar; (iii) the analyses and results associated to the broadband communication LEO satellite-based passive radar; and (iv) conclusions.

A brief description of each chapter is presented below:

- Part I: Introduction
 - **Chapter 1:** This chapter introduces this doctoral thesis by explaining its motivation in the context of the current state-of-the-art, and stating the main objectives and achieved novel contributions.
 - **Chapter 2:** This chapter describes the basic concepts of the passive radar techniques on which the development of this thesis is based.
- Part II: LTE-based passive radar
 - **Chapter 3:** This chapter presents firstly an introduction to the concept of exploiting the LTE user-downlink signals as illumination of opportunity for passive radar applications with focus on the surveillance of critical infrastructures such as high-speed railway networks. Afterwards, it describes the considered system architecture and, in order to demonstrate its technical feasibility, shows the results of the performed theoretical analyses and the experimental characterization of the LTE signals for passive radar in terms of their ambiguity function.

- **Chapter 4:** In this chapter, the description and experimental results of a measurement campaign using the developed LTE-based passive radar system for drone target detection are presented, experimentally validating the presented techniques and assessing their limitations.
- Part III: Broadband communication LEO satellite-based passive radar
 - **Chapter 5:** This chapter presents an introduction to the novel broadband communication LEO satellite constellations, analysing their characteristics in the context of passive radar applications. The theoretical results of achievable capabilities and the experimental characterization of user-downlink signals transmitted by these satellites show the technical feasibility and promising capabilities of exploiting them as illumination of opportunity. The description of the developed passive radar systems that enable the validation of the proposed techniques is also included in this chapter.
 - **Chapter 6:** This chapter describes the field tests performed to experimentally validate the use of these LEO satellite signals and presents the results obtained in the context of: (i) measurements of scattered signals from clutter or static elements of the monitored area, and (ii) target detection using a medium-sized drone as cooperative target.
- Part IV: Conclusions
 - **Chapter 7:** This chapter presents the main conclusions of this thesis and, based on the achieved results, sets a roadmap of relevant topics for further research.

1.4 List of publications

During the development of this thesis, the obtained results and conclusions have been presented in a book chapter and in the following journals, conferences and workshops:

International journals:

- R. Blázquez-García, D. Cristallini, M. Ummenhofer, V. Seidel, J. Heckenbach, and D. O'Hagan, "Capabilities and challenges of passive radar systems based on broadband low-Earth orbit communication satellites," *IET Radar, Sonar and Navigation*, 2023.
- R. Blázquez-García, J. Casamayón-Antón, and M. Burgos-García, "LTE-based passive multistatic radar for high-speed railway network surveillance: design and preliminary results," *International Journal of Microwave and Wireless Technologies*, vol 11.5-6, pp. 482–489, 2019.

National journals:

- R. Blázquez-García, D. Cristallini, and D. O'Hagan, "Megakonstellationen als Wegbereiter für globale und dauerhafte Erdbeobachtung," *ITG-News (VDE)*, vol. 1/2023, pp. 16–18, 2023.

International conferences:

- M. Ummenhofer, V. Seidel, J. Heckenbach, R. Blázquez-García, and D. Cristallini, "First results of DVB-S based passive polarimetric measurements of micro-Doppler signatures from a helicopter," *IEEE International Radar Conference*, 2023.
- R. Blázquez-García, D. Cristallini, M. Ummenhofer, V. Seidel, J. Heckenbach, and Daniel O'Hagan, "Multichannel passive radar demonstrator based on Starlink satellite signals for persistent bistatic SAR interferometry", *2023 IEEE International Geoscience and Remote Sensing Symposium (IGARSS)*, 2023.
- R. Blázquez-García, D. Cristallini, M. Ummenhofer, V. Seidel, J. Heckenbach, and D. O'Hagan, "Experimental comparison of Starlink and OneWeb signals for passive radar", *2023 IEEE Radar Conference (RadarConf)*, 2023. IEEE Michael C. Wicks Radar Student Travel Grant.
- D. Cristallini, R. Blázquez-García, and D. O'Hagan, "K-space signal occupancy of Starlink signals and its applications in passive radar imaging", *2023 IEEE Radar Conference (RadarConf)*, 2023.

- R. Blázquez-García, D. Cristallini, V. Seidel, J. Heckenbach, A. Slavov, and D. O'Hagan, "Experimental acquisition of Starlink satellite transmissions for passive radar applications", *IET Radar Conference*, 2022.
- R. Blázquez-García, M. Ummenhofer, D. Cristallini, and D. O'Hagan, "Passive radar architecture based on broadband LEO communication satellite constellations", *2022 IEEE Radar Conference (RadarConf)*, 2022
- R. Blázquez-García, J. Casamayón-Antón, and M. Burgos-García, "LTE-R based passive multistatic radar for high-speed railway network surveillance," *2018 European Radar Conference (EuRAD)*, 2018.

International workshops:

- R. Blázquez-García, P. Gomez-Del-Hoyo, D. Cristallini, P. Samczyński, M. Ummenhofer, M. Khyzhniak, V. Seidel, J. Heckenbach, and D. O'Hagan, "Starlink and OneWeb satellite constellations as emerging illuminators for passive radar applications," *Multistatics and Passive Radar Focus Days*, 2023.
- R. Blázquez-García, "Passive radar techniques based on broadband communication LEO satellite constellations," in Workshop on Applications for Advanced Passive Radar Systems, *2023 European Radar Conference (EuRAD)*, 2023.
- R. Blázquez-García, "Passive radar techniques based on broadband communication LEO satellite constellations," in Workshop on Applications for Advanced Passive Radar Systems, *2022 European Radar Conference (EuRAD)*, 2022.

National conferences:

- R. Blázquez García, L. Muñoz Miguel, and M. Burgos García, "Red de sensores radar pasivos para detección de drones en entornos urbanos," *XXXIV Simposium Nacional de la Unión Científica Internacional de Radio (URSI)*, 2019.
- R. Blázquez García, J. Casamayón Antón, and M. Burgos García, "Nuevo concepto de radares pasivos multiestáticos basados en LTE-R para vigilancia de líneas ferroviarias

de alta velocidad,” *VI Congreso Nacional de I+D en Defensa y Seguridad (DESEi+d)*, 2018.

- R. Blázquez García, J. Casamayón Antón, and M. Burgos García, “On the use of LTE-R signals for passive multistatic radar,” *XXXIII Simposium Nacional de la Unión Científica Internacional de Radio (URSI)*, 2018.
- A. Barbero Rodríguez, R. Blázquez García, A. Fernández Cruza, M. Insua Feito, and M. Burgos García, “Análisis de viabilidad de despliegues anti-dron basados en tecnologías de última generación,” *V Congreso Nacional de I+D en Defensa y Seguridad (DESEi+d)*, 2017.

Book chapter:

- D. Cristallini, D. O’Hagan, T. Weyland, and R. Blázquez-García, “Outlook on future trends,” in *Passive Radar on Moving Platforms* (Eds. D. O’Hagan and D. Cristallini): The Institution of Engineering and Technology, 2023, pp. 291–312.

1.5 Supervised MSc and BSc theses

During the development of this thesis, the following MSc and BSc theses have been supervised:

MSc Theses:

- A. Delgado Fernández, *Análisis y desarrollo de técnicas basadas en medidas inerciales para la mejora de las capacidades de teledetección en sensores electro-ópticos embarcados*, 2021.
- H. Cuevas Esteban, *Diseño de un sistema de vigilancia costera y salvamento marítimo basado en la cooperación entre plataformas autónomas aéreas y navales*, 2018. Isdefe I+D+i “Antonio Torres” Award.

BSc Theses:

- Á. Cerrada Ramírez, *Análisis y modelado de sistemas de estabilización de sensores electro-ópticos embarcados en vehículos aéreos no tripulados*, 2020. Award “Cátedra de Defensa y Seguridad de la Red Horizontes” Isdefe-UPM.
- A. Delgado Fernández, *Desarrollos de algoritmos para la detección de objetos ópticamente camuflados utilizando cámaras hiperespectrales embarcadas*, 2019. Award “Cátedra Ingeniero General D. Antonio Remón Zarco del Valle” UPM-CESEDEN. Finalist Isdefe I+D+i “Antonio Torres” Award.
- D. Conde Párraga, *Desarrollo de un sistema de clasificación automática de modulaciones empleando equipos de radio definida por software*, 2019.
- C. González Alcalá, *Desarrollo de algoritmos para la detección y clasificación de blancos marítimos en imágenes SAR satelitales*, 2019.
- M. Dávila Requena, *Desarrollo de una herramienta para el análisis de sensores radar embarcados en misiones ISTAR*, 2018.
- B. Gómez Cifuentes, *Desarrollo de una herramienta de análisis de sensores ópticos embarcados para misiones ISTAR*, 2018.
- A. Fernández Cruza, *Diseño de un despliegue para la detección, identificación y neutralización de amenazas basadas en vehículos aéreos no tripulados*, 2017

Chapter 2

Passive Radar: Principles and Concepts

In contrast to conventional radar systems (i.e. active radars), a passive radar does not transmit a dedicated electromagnetic signal optimised for sensing applications but exploits signals transmitted by other systems, generally broadcast or communications systems (e.g. FM radio [Col13], DBV-T [Pal12], WiFi [Col12], mobile communications systems [Kno20], DVB-S [Pis20], etc.), but also transmitted by jammers [NAT20] or active radars [Kus13]. For this reason, the signals used by passive radars are commonly known as illumination of opportunity and they are inherently bistatic radar systems since the receiver is not co-located with the transmitter. Furthermore, this bistatic configuration can be considered scalable to multistatic passive radar systems (i.e. multiple transmitter-receiver pairs), considering multiple transmitters of opportunity or deploying multiple spatially distributed receiving nodes.

In general, passive radars present important advantages in terms of lower cost, covert operation, no need for frequency allocation and efficient reuse of the electromagnetic spectrum which make them relevant systems for surveillance and monitoring applications in both civilian [Par] and military fields [Hen]. However, the exploitation of non-cooperative transmissions, which are not optimized for radar applications, usually requires two coherent receiving channels

to separately receive the reference signals and the target scattered signals. Besides, it poses challenges associated with measurement ambiguities (i.e. ghost targets due to the signal structure), and the high level of direct signal interference resulting in demanding dynamic range requirements and possible masking of weak targets. Therefore, system architectures and signal processing for passive radars are required to address these challenges.

This chapter describes common system architectures and signal processing techniques that have been proposed for passive radars, including the key concepts and principles of this technology that will be referred to throughout the rest of this thesis, in which the novel use of both a terrestrial illuminator of opportunity, i.e. LTE downlink signals, and a satellite-based illuminator of opportunity, i.e. the user downlink signals of the emerging broadband communication LEO satellite constellations (e.g. Starlink or OneWeb), has been analysed and experimentally validated.

2.1 Passive radar architectures and geometry

2.1.1 Passive radar architectures

Common passive radar operation requires a copy of the signal transmitted by the illuminator of opportunity, usually called reference or direct signal, in order to perform a coherent integration of the surveillance signals received from the area of interest and detect the time-delayed and Doppler-shifted signals scattered by the targets. Since the reference signal should ideally have a high SNR and not contain multipath components, while the received power of the direct signal in the surveillance channel should be ideally low to avoid masking of weak targets and demanding dynamic range requirements, the system architecture of passive radars is commonly composed of two directional antennas pointed respectively to the transmitter of opportunity and to the area of interest, as shown in Figure 2.1(a). Recent developments and advances in coherent multichannel receivers have enabled the implementation of passive radar architectures based on digital arrays, as shown in Figure 2.1(b). Although this architecture presents more demanding dynamic range requirements, since both the direct and target scattered signals are simultaneously received by each array element, the capability to synthesize multiple receiving

beams by digital beamforming has advantages in terms of flexibility, adaptability, persistence and direction of arrival (DoA) estimation [Núñ23; Alm23]. Besides, when the illumination of opportunity is a digitally modulated signal, it can be reconstructed by demodulation and subsequent remodulation in order to get a noise-free reference signal without multipath components even when the direct signal is received through the antenna sidelobes, enabling the single-channel passive radar architecture [Fan18] shown in Figure 2.1(c).

Although direct signal interference (DSI) in the surveillance channels is also cancelled by signal processing techniques, to minimize it, the transmitter of opportunity is usually selected in a direction that differs from the area of interest. However, to detect targets in the area around the baseline between the transmitter and receiver, Forward Scattering Radar (FSR) techniques can be applied [Col20], which potentially achieve better target detectability, even of stealth targets, because the RCS is typically enhanced in the forward scattering direction.

Passive radar architectures can be extended to consider multiple spatially distributed transmitter of opportunity or receiving nodes in order to realize a multistatic radar system with improved target detection and localization capabilities due to the spatial diversity [Che98].

Furthermore, the current congestion of the electromagnetic spectrum and the increasing demands on sensing capabilities to improve efficiency and autonomy in multiple application scenarios have recently accelerated the convergence between communications and sensing, and raised the interest in the so-called Joint Communication and Sensing (JCAS) or Integrated Sensing and Communication (ISAC) techniques [Bar21]. However, in contrast to the common operation of passive radars, these approaches assume a certain degree of cooperation and control of the transmitted signals to jointly optimize the communication and radar capabilities and may also consider monostatic geometries with the receiver co-located with the transmitter.

The capabilities of passive radar systems can be analysed based on the associated bistatic geometry, the bistatic radar equation (to estimate the maximum detection range) and the ambiguity function of the considered signals of opportunity (to evaluate their suitability for radar applications). These concepts are described in detail in the following subsections and are used throughout this thesis to evaluate the achievable capabilities of the proposed systems.

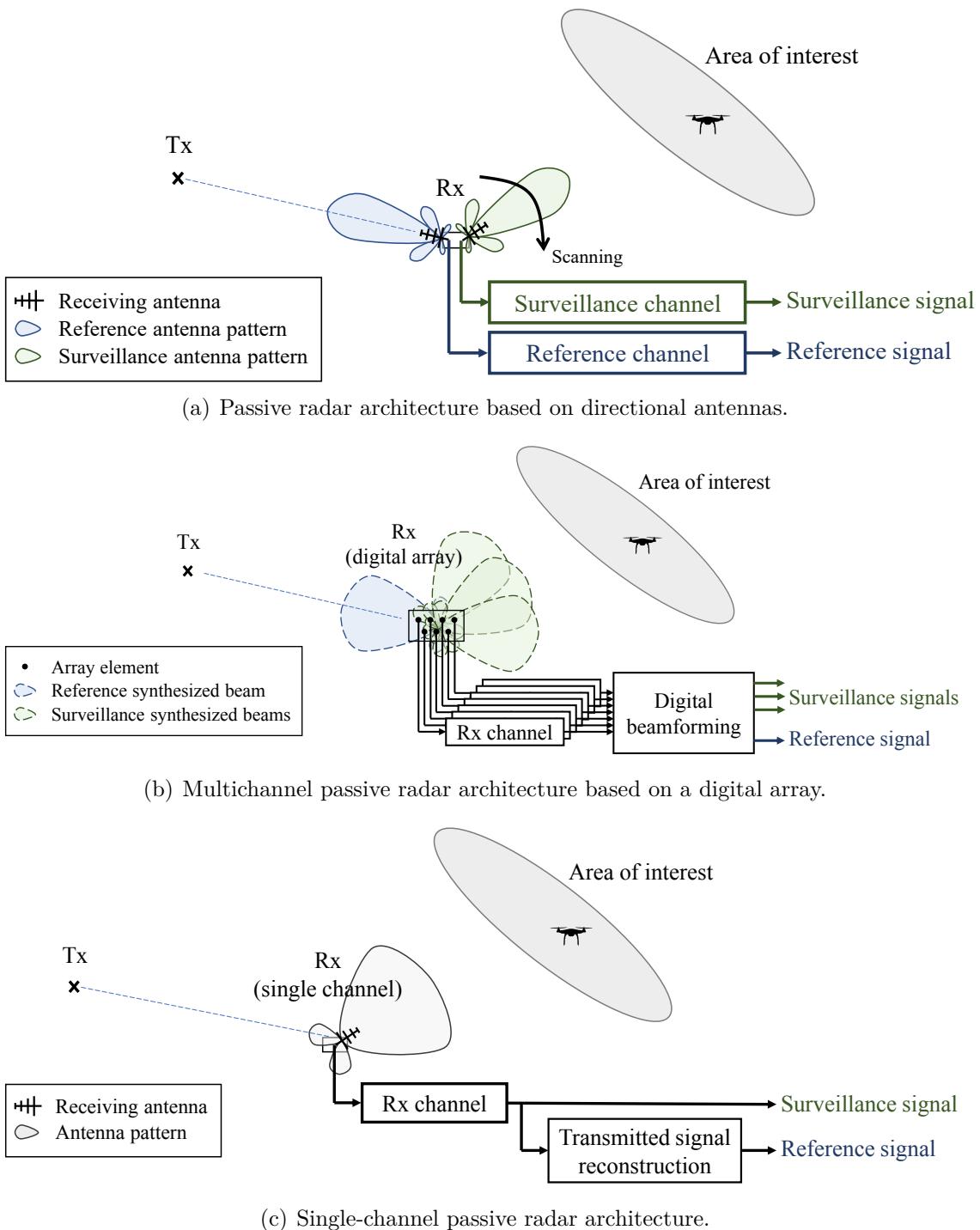


Figure 2.1: Passive radar system architectures.

2.1.2 Bistatic geometry

The bistatic geometry is defined based on the spatially distributed positions of the transmitter (Tx), receiver (Rx) and target (Tgt) as simplified in Figure 2.2 for a two dimensional representation.

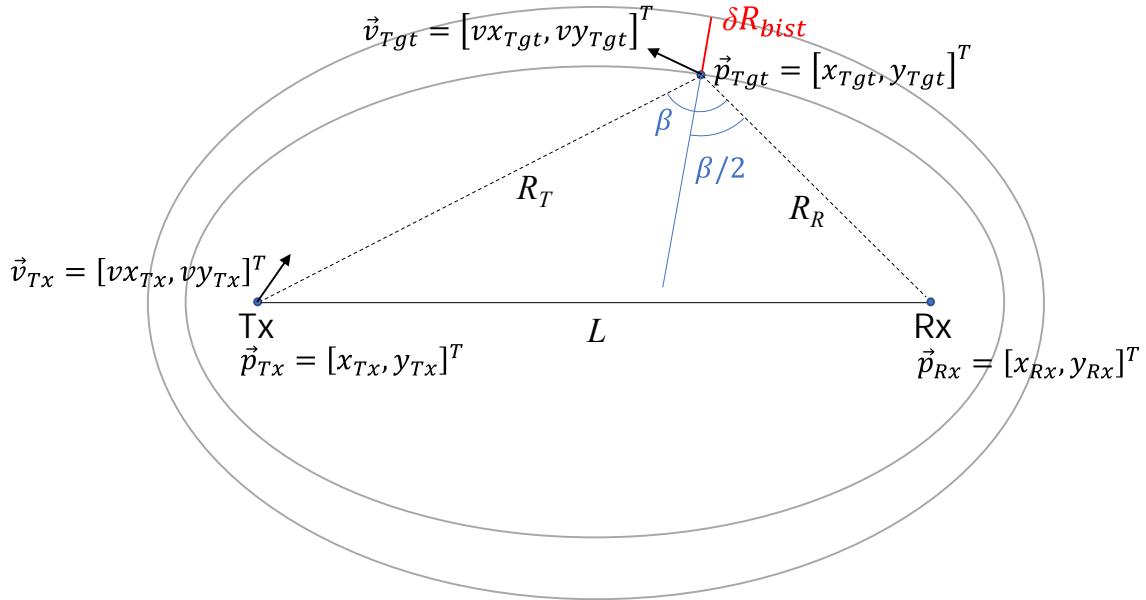


Figure 2.2: Simplified two-dimensional bistatic geometry composed of a transmitter (Tx), a stationary receiver (Rx) and a target (Tgt).

The bistatic range R_{bist} can be defined by:

$$R_{bist} = R_T + R_R - L \quad (2.1)$$

where R_T is the transmitter-target distance, R_R is the target-receiver distance and L is the baseline distance between the transmitter and the receiver, which are given by:

$$R_T = \|\vec{p}_{Tgt} - \vec{p}_{Tx}\| \quad (2.2)$$

$$R_R = \|\vec{p}_{Rx} - \vec{p}_{Tgt}\| \quad (2.3)$$

$$L = \|\vec{p}_{Rx} - \vec{p}_{Tx}\| \quad (2.4)$$

In the simplified two-dimensional representation, a specific bistatic range defines an ellipse, usually called iso-range curve, with foci on the transmitter and receiver and a semi-major axis given by $a = \frac{R_T + R_R}{2}$, whose points present the same bistatic range. Similarly, in the three-dimensional space, a bistatic range gives rise to an ellipsoid.

On the other hand, assuming a stationary receiver, the bistatic velocity v_{bist} of a target can be defined by:

$$v_{bist} = (\vec{v}_{Tx} - \vec{v}_{Tgt}) \frac{\vec{p}_{Tgt} - \vec{p}_{Tx}}{\|\vec{p}_{Tgt} - \vec{p}_{Tx}\|} + \vec{v}_{Tgt} \frac{\vec{p}_{Rx} - \vec{p}_{Tgt}}{\|\vec{p}_{Rx} - \vec{p}_{Tgt}\|} - \vec{v}_{Tx} \frac{\vec{p}_{Rx} - \vec{p}_{Tx}}{\|\vec{p}_{Rx} - \vec{p}_{Tx}\|} \quad (2.5)$$

The bistatic range and velocity of a target give rise, respectively, to a time difference of arrival $\Delta\tau$ (i.e. time delay) and a frequency difference of arrival Δf_D (i.e. Doppler frequency shift) between the received target scattered signal (tgt) and the direct signal (DS), given by:

$$\Delta\tau = \tau^{(tgt)} - \tau^{(DS)} = \frac{R_{bist}}{c_0} \quad (2.6)$$

$$\Delta f_D = f_D^{(tgt)} - f_D^{(DS)} = -\frac{f_T}{c_0} \frac{dR_{bist}}{dt} = \frac{v_{bist}}{c_0} f_T \quad (2.7)$$

where c_0 is the speed of light and f_T is the center frequency of the transmitted signal.

The bistatic angle β varying between 0 and 180° is defined as the angle between the target-transmitter and target-receiver directions, given by:

$$\beta = \arccos \left\{ \frac{\vec{p}_{Tx} - \vec{p}_{Tgt}}{\|\vec{p}_{Tx} - \vec{p}_{Tgt}\|} \cdot \frac{\vec{p}_{Rx} - \vec{p}_{Tgt}}{\|\vec{p}_{Rx} - \vec{p}_{Tgt}\|} \right\} \quad (2.8)$$

while $\beta/2$ is often referred to as the bistatic bisector. When the bistatic angle is close to zero, the geometry is considered to be pseudo-monostatic, while when it is close to 180° , a forward scattering geometry is observed.

Similarly to monostatic radars, the achievable range and Doppler resolutions are related to the transmitted bandwidth B and coherent processing interval (CPI) T_{CPI} , respectively. However, as shown in Figure 2.2 with the two concentric ellipses, the bistatic range resolution

also depends on the position of the target and its associated bistatic angle. Therefore, for bistatic radar systems, the achievable bistatic range and Doppler resolutions (δR and δf_D) can be approximated by:

$$\delta R_{bist} \approx \frac{c_0}{2B \cos(\beta/2)} \quad (2.9)$$

$$\delta f_D \approx \frac{1}{T_{CPI}} \quad (2.10)$$

The bistatic range and Doppler resolutions taking into account the specific characteristics of the considered signals can also be estimated from the main peak width of the signal ambiguity function, which is defined below.

2.1.3 Bistatic radar equation

The target detection capabilities of passive radar systems can be estimated by the bistatic radar equation, which is based on a power budget analysis adapted to the considered bistatic geometry. For example, it allows to estimate the maximum detection range based on the minimum required SNR to detect targets with an assumed RCS fluctuation model and specific probabilities of detection and false alarm.

The target SNR after ideal coherent integration (i.e. integration gain $T_{CPI} \cdot B$) given by the bistatic radar equation depends on its distances to the transmitter (R_T) and the receiver (R_R), its RCS (σ) and the considered characteristics of the transmitter and receiver [Mar23b; Bro13]:

$$SNR = \frac{P_T G_T(tgt) F_T}{4\pi R_T^2} \frac{\lambda^2 G_R(tgt)}{4\pi} \frac{\sigma F_R}{4\pi R_R^2 k T_0 F} \frac{T_{CPI}}{L_S} \frac{1}{k T_0 F} \quad (2.11)$$

where P_T is the averaged transmitted power, $G_T(tgt)$ is the transmitter antenna gain in the direction of the target, F_T is the transmitter-target propagation factor, λ is the wavelength associated to the center frequency of the transmitted signal, $G_R(tgt)$ is the receiver surveillance

antenna gain in the direction of the target, F_R is the target-receiver propagation factor, k is the Boltzmann's constant, T_0 is the reference noise temperature (290 K), F is the receiver noise factor and L_S is a loss term to include additional system losses. If a free space propagation model is considered for both transmitter-target and target-receiver paths, the propagation factors F_T and F_R are assumed to be 1.

In certain passive radar scenarios, especially when the transmitter is close to the receiver, the limiting factor may not be the thermal noise but the required dynamic margin or the correlation sidelobes of the residual direct signal interference [Mar23b]. Since in the surveillance channels, both the direct signal interference with power P_{DS} and the target scattered signal with power P_{Tgt} are received, the dynamic margin of the receiver should be greater than:

$$\text{Dynamic margin} > \frac{P_{DS}}{P_{Tgt}} = \frac{R_T^2}{G_T(tgt)F_T} \frac{4\pi}{G_R(tgt)} \frac{R_R^2}{\sigma F_R} \frac{G_T(rx)F_{TR}G_R(tx)}{L^2} \quad (2.12)$$

where $G_T(rx)$ is the transmitter antenna gain in the direction of the receiver, $G_R(tx)$ is the receiver surveillance antenna gain in the direction of the transmitter, F_{TR} is the transmitter-receiver propagation factor and L is the baseline length.

In addition, the correlation sidelobes of the residual direct signal interference can mask the targets and, therefore, a signal-to-interference ratio (SIR) can be evaluated taking into account that those sidelobes are reduced with respect to the direct signal level by a factor γ which also takes into account the DSI cancellation stage of the signal processing [Mar23b]:

$$SIR = \frac{P_{Tgt}\gamma}{P_{DS}} = \frac{G_T(tgt)F_T}{R_T^2} \frac{G_R(tgt)}{4\pi} \frac{\sigma F_R}{R_R^2} \frac{L^2\gamma}{G_T(rx)F_{TR}G_R(tx)} \quad (2.13)$$

In general, since the illuminations of opportunity are not optimised for radar applications, their autocorrelation sidelobes are typically a more limiting factor than the potential sidelobes induced by the receiving phase noise in the target and clutter responses. However, a high receiver phase noise could limit clutter suppression of clutter cancellation techniques applied in the signal processing [Hen23].

2.1.4 Signal model and ambiguity function

In order to evaluate the proposed techniques for LTE-based and LEO satellite-based passive radars, a signal level simulator with the following characteristics has been developed:

- Simulation of static transmitters and receivers, but also of a dynamic 3D bistatic/multistatic scenario as shown in Figure 2.3 that considers the current trajectories and dynamics of one or multiple LEO satellites based on their orbital data.

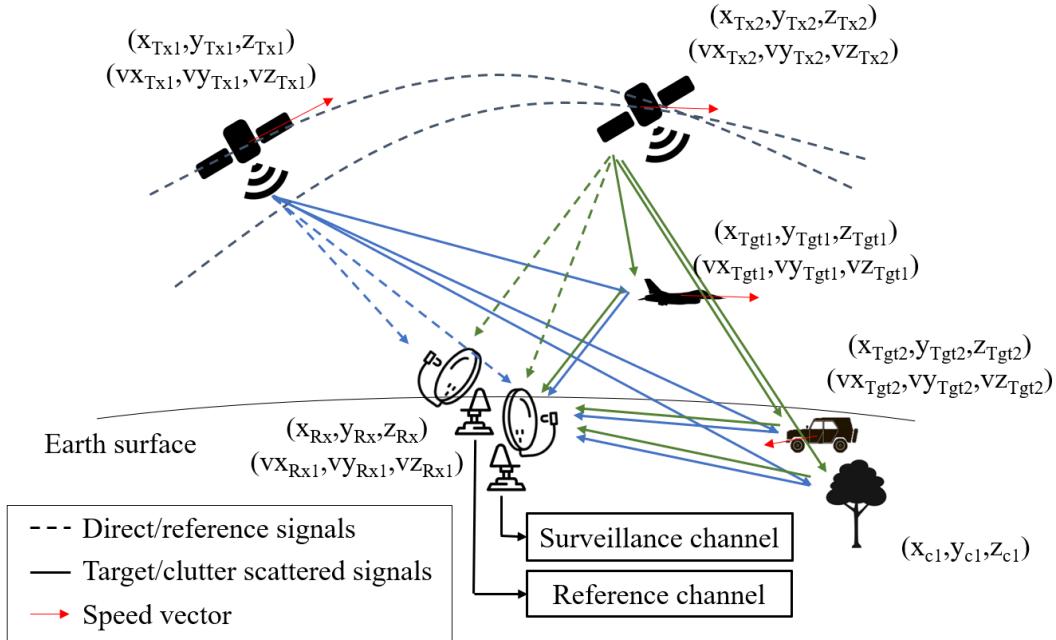


Figure 2.3: Considered dynamic 3D bistatic/multistatic geometry for LEO satellite-based passive radar simulation, including the position, i.e. (x, y, z) , and velocity, i.e. (vx, vy, vz) , of the different scenario elements, i.e. transmitters (Tx), receivers (Rx), targets (Tgt) and clutter (c).

- Simulation of the characteristic waveforms transmitted by the considered LTE base stations (i.e. physical layer based on OFDM modulation with pilot and synchronization signals defined by the standard) and by LEO satellites (i.e. OFDM signals for Starlink and single carrier signals for OneWeb). For this purpose, the signal properties based on the LTE standard or estimated based on the experimental characterization for the communication LEO satellites have been taken into account. As an example, Figure 2.4 shows the spectrum of simulated single carrier signals for the multiple frequency

channels of broadband communication LEO satellites. Besides, the signal simulation has been also extended to include other signals of opportunity such as DVB-S transmissions, as shown in Figure 2.5 which includes a comparison between a simulated and a measured multi-transponder DVB-S signal.

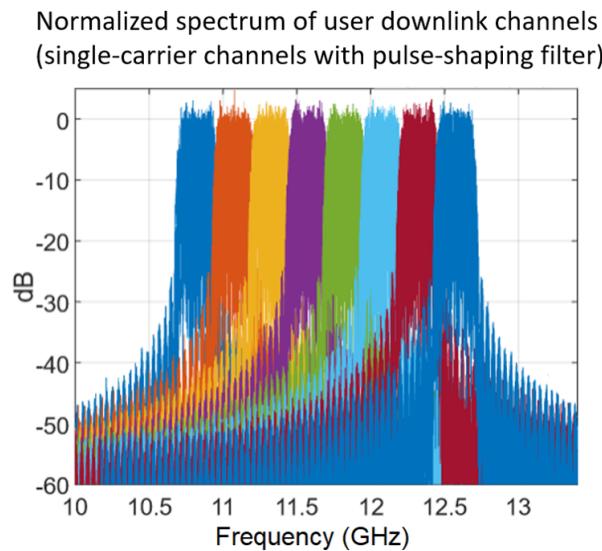
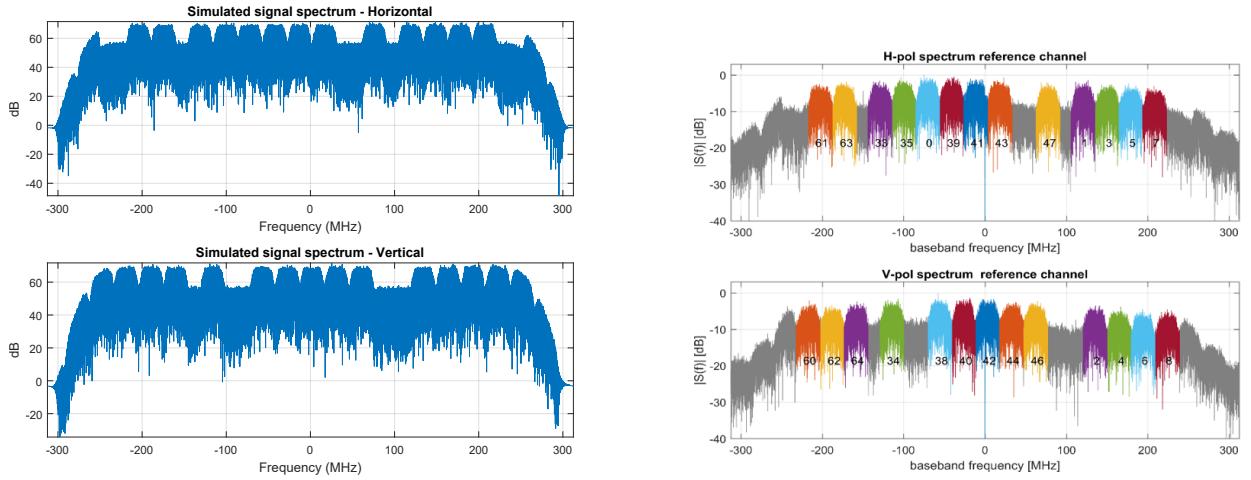


Figure 2.4: Normalized spectrum of user downlink channels (single-carrier signals with pulse-shaping filter simulating the waveform type transmitted by OneWeb satellites).

- Simulation of range and Doppler migration effects by considering the following signal model that takes into account the scenario dynamics during the integration time, not resorting to a stationary approximation (i.e. constant range and Doppler frequency during the integration time). For this purpose, reference and surveillance signals ($s_{ref}(t)$ and $s_{surv}(t)$) are simulated as a superposition of several components (direct signal, targets, multipath/clutter and noise) with variable delay and Doppler frequency during the integration time, as shown in Equations 2.14 and 2.15:



(a) Spectrum of simulated Astra 19.2°E downlink signals at 11.095 GHz with a sampling rate of 625 MHz and a radio frequency bandwidth of 500 MHz

(b) Spectrum of captured Astra 19.2°E downlink signals at 11.095 GHz and a sampling rate of 625 MHz. Overlay numbers indicate associated transponder IDs (reproduced from [Umm23]).

Figure 2.5: Comparison of simulated and measured Astra 19.2°E signals at 11.095 GHz.

$$s_{ref}(t) = a^{(DS_{ref})} \cdot d(t - \tau^{(DS_{ref})}(t)) \cdot e^{j2\pi \int_0^t f_D^{(DS_{ref})}(t) dt} + \sum_{n=1}^{N_{mp}} a_n^{(mp_{ref})} \cdot d(t - \tau_n^{(mp_{ref})}(t)) \cdot e^{j2\pi \int_0^t f_D^{(mp_{ref})}(t) dt} + n_{ref}(t) \quad (2.14)$$

$$s_{surv}(t) = a^{(DS_{surv})} \cdot d(t - \tau^{(DS_{surv})}(t)) \cdot e^{j2\pi \int_0^t f_D^{(DS_{surv})}(t) dt} + \sum_{n=1}^{N_{mp}} a_n^{(mp_{surv})} \cdot d(t - \tau_n^{(mp_{surv})}(t)) \cdot e^{j2\pi \int_0^t f_D^{(mp_{surv})}(t) dt} + \sum_{k=1}^{N_{tgt}} a_k^{(tgt)}(t) \cdot d(t - \tau_k^{(tgt)}(t)) \cdot e^{j2\pi \int_0^t f_D^{(tgt)}(t) dt} + n_{surv}(t) \quad (2.15)$$

where a , τ and f_D represents the complex amplitude, the time-dependent delay and the time-dependent Doppler frequency, respectively, of the direct signal (DS), the multipath/clutter components (mp) and the targets (tgt) in the reference (ref) or surveillance ($surv$) channels. Complex additive white Gaussian noise ($n_{ref}(t)$ and $n_{surv}(t)$) is also considered based on the noise figure of the receivers. No target signals

are considered in the reference channel given the typical pointing of a directional reference antenna towards the transmitter of opportunity, spatially separated from the surveillance area.

Independent channels without co-channel interference are typically simulated for the reference signals, but co-channel interference and superposition of scattered signals from different LTE based stations or LEO satellites could be also considered.

In this way, apart from evaluating signal processing techniques with simulated data for the considered scenarios, the computation of the ambiguity function of simulated signals can be performed, which allows to assess the properties of the signals in terms of resolution and sidelobe levels. This ambiguity function (AF) is given by the square magnitude of the output of the matched filter representing the point target response depending on the time delay and Doppler frequency [Gri22]. Therefore, the range-Doppler AF $\chi(\tau, f_d)$ of a signal of opportunity $s(t)$ of duration T_{CPI} is given by [Bak05]:

$$\chi(\tau, f_d) = \left| \int_{-\infty}^{\infty} s(t) \cdot s^*(t - \tau) \cdot e^{-j2\pi f_d t} \cdot dt \right|^2 \quad (2.16)$$

where τ is the time delay and f_d is the Doppler frequency. As an example, Figure 2.6 represents the computed AF for the simulated horizontally polarized DVB-S signal of Figure 2.5(a), showing high range sidelobe levels due to the multi-transponder transmission with spectrum notches between frequency channels.

2.2 Passive radar processing

In order to compute the so-called range-Doppler maps from which the targets can be detected, estimating their associated bistatic range and Doppler frequency, and tracked based on a time sequence of detections, several processing steps are usually perform in passive radar systems from the reference and surveillance signals. Figure 2.7 shows a common processing chain for a passive radar architecture based on a receiving digital array, in which firstly the reference and surveillance signals are extracted by means of digital beamforming techniques. As said before, for digital modulated signals, the reference signal can be reconstructed in order to

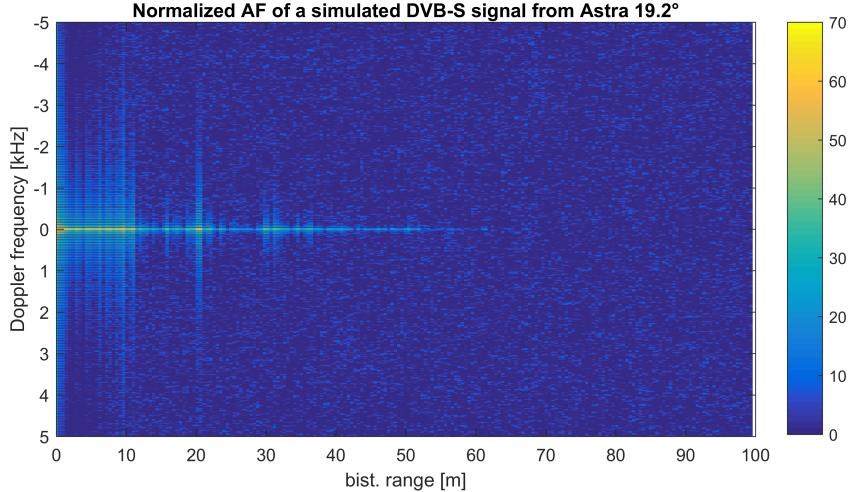


Figure 2.6: AF normalized to the averaged noise floor level of a simulated horizontally polarized Astra 19.2° signal centered at 11.095 GHz with 625 MS/s sampling frequency and 500 MHz radio frequency bandwidth, considering a coherent integration interval of 25 ms.

ideally get a noise-free copy of the transmitted signal without multipath components. In order to suppress the direct signal interference and clutter components in the surveillance signals, DSI cancellation algorithms, such as the Extensive Cancellation Algorithm (ECA), are applied, which are usually based on subtracting time-delayed replicas of the reference signal. Afterwards, the range-Doppler maps can be computed by cross-correlating the reference and surveillance signals in batches (i.e. range compression) and a subsequent Doppler processing to coherently integrate them during the CPI. This cross-correlation and Doppler processing approximately implements a matched filter, but also mismatched filtering techniques can be applied, for example, to suppress ambiguities such as the reciprocal filter, or motion compensation techniques to cope with range and Doppler migration effects during the CPI. Automatic target detection algorithms are performed over the range-Doppler maps, and the sequence of detections are used to track and localize targets, possibly fusing detections from other transmitter-receiver pairs in a multistatic system.

The main processing steps which are used in the development of this thesis are further describe below, i.e. digital beamforming, DSI and clutter cancellation and range-Doppler map computation based on batch cross-correlation and Doppler processing.

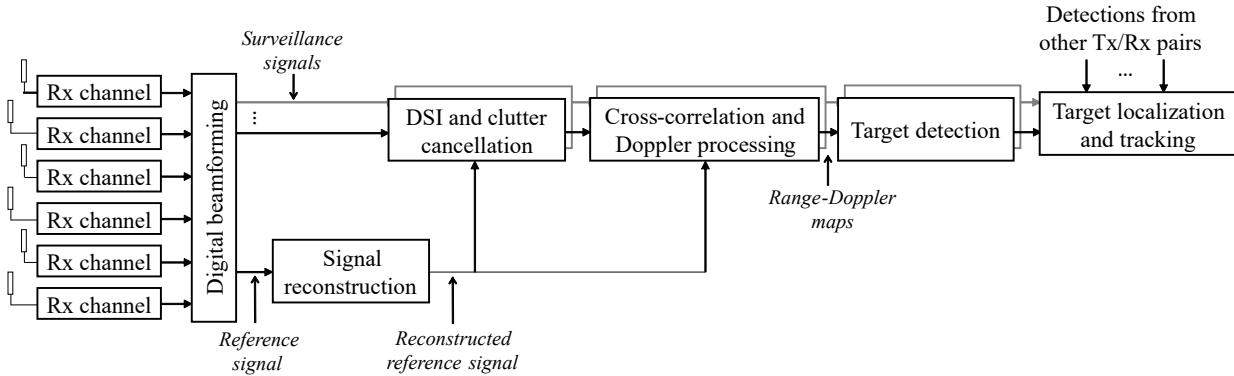


Figure 2.7: Common passive radar processing chain with a receiving digital array.

2.2.1 Digital beamforming

The use of a digital array implemented with multiple receiving channels allows the application of digital beamforming techniques by linearly combining the received signals in order to: synthesize multiple simultaneous antenna beams; adapt the antenna beams based on optimization methods for example to maximize target signal-to-interference-plus-noise ratio (SINR) by spatial filtering [Van02; Núñ23]; or estimate the target direction-of-arrival (DoA) [Alm23].

The output of the beamformer $y[n]$ for the n -th time sample is given by the linear combination defined by the beamforming vector \mathbf{w} of the signals received by the array channels stacked in the vector $\mathbf{s}[n]$:

$$y[n] = \mathbf{w}^H \mathbf{s}[n] \quad (2.17)$$

Based on the calibrated array response, the beamforming vector can be designed to implement antenna patterns with desired properties, for example, maximizing the gain in a specific direction while having nulls in other directions, depending on the degrees of freedom of the digital array. Naturally, several beamformers can be simultaneously applied with different desired characteristics.

Adaptive techniques to maximize SNR or SINR have been developed usually based on estimating a sample spatial covariance matrix. Many of these techniques, such as Maximum Ratio Combining (MRC), Minimum Variance Distortionless Response (MVDR) or Zero-

Forcing (ZF) [Núñ23] also require the accurate calibration of the array response. Besides, some adaptive beamforming techniques require the spatial covariance matrix to contain only the interference components in order to avoid the suppression of target signals, making the estimation of this covariance matrix difficult [Pal14].

To avoid these requirements for array calibration and estimation of the interference covariance matrix, in this thesis, simple beamforming techniques which maximize or minimize the output power of the beamformer subject to the beamformer vectors (i.e. \mathbf{w}_{max} or \mathbf{w}_{min}) being a unit vector have been used:

- Output power maximization:

$$\begin{aligned} & \max_{\mathbf{w}_{max}} \mathbf{w}_{max}^H \mathbf{S} \mathbf{w}_{max} \\ & \text{s.t. } \mathbf{w}_{max}^H \mathbf{w}_{max} = 1 \end{aligned} \quad (2.18)$$

- Output power minimization:

$$\begin{aligned} & \min_{\mathbf{w}_{min}} \mathbf{w}_{min}^H \mathbf{S} \mathbf{w}_{min} \\ & \text{s.t. } \mathbf{w}_{min}^H \mathbf{w}_{min} = 1 \end{aligned} \quad (2.19)$$

where the sample spatial covariance matrix \mathbf{S} of the received signals is estimated in each CPI (composed of N samples) by:

$$\mathbf{S} = \frac{1}{N-1} \sum_{n=0}^{N-1} (\mathbf{s}[n] - \bar{\mathbf{s}})(\mathbf{s}[n] - \bar{\mathbf{s}})^H \quad (2.20)$$

where $\bar{\mathbf{s}}$ is the sample mean vector:

$$\bar{\mathbf{s}} = \frac{1}{N} \sum_{n=0}^{N-1} \mathbf{s}[n] \quad (2.21)$$

2.2.2 DSI and clutter removal

Surveillance signals, in addition to containing the target scatter signals, present clutter or multipath components and direct signal interference, whose correlation sidelobes can prevent the detection of weak targets. Therefore, even when the direct signal is received partially suppressed through the sidelobes of the surveillance antenna or beam, a direct signal and clutter cancellation algorithm is usually applied, such as the Extensive Cancellation Algorithm (ECA) [Col09].

The ECA algorithm is based on a Least Square (LS) approach by projecting the surveillance signal onto the orthogonal subspace to the disturbance subspace (i.e. DSI and clutter components). With the assumption that the main multipath components are potentially present in the first K range bins, the aim of the ECA algorithm is to minimize the residual power after disturbance cancellation:

$$\min_{\alpha} \|\mathbf{s}_{surv} - \mathbf{X}\alpha\|^2 \quad (2.22)$$

where \mathbf{s}_{surv} is the vector form of the surveillance signal with N samples, i.e.:

$$\mathbf{s}_{surv} = [s_{surv}[0], s_{surv}[1], \dots, s_{surv}[N-1]]^T \quad (2.23)$$

and \mathbf{X} is the basis matrix of the disturbance subspace which, considering DSI and multipath components (i.e. static clutter), can be defined by:

$$\mathbf{X} = \mathbf{B}\mathbf{S}_{ref} \quad (2.24)$$

where \mathbf{B} is an incidence matrix that selects the last N rows of a matrix composed of K time-shifted replicas of the reference signal:

$$\mathbf{S}_{ref} = [\mathbf{s}_{ref}, \mathbf{D}\mathbf{s}_{ref}, \mathbf{D}^2\mathbf{s}_{ref}, \dots, \mathbf{D}^{K-1}\mathbf{s}_{ref}] \quad (2.25)$$

being \mathbf{D} a delay matrix that shifts the signal by one time sample and \mathbf{s}_{ref} the vector form of the reference signal with $N + R - 1$ samples:

$$\mathbf{s}_{ref} = [s_{ref}[-R + 1], \dots, s_{ref}[0], \dots, s_{ref}[N - 1]]^T \quad (2.26)$$

where $R - 1$ is the number additional reference signal samples to achieve the integration of N samples over an extent of R delay bins in the cross-correlation processing.

The solution of the considered minimization problem is given by:

$$\boldsymbol{\alpha} = (\mathbf{X}^H \mathbf{X})^{-1} \mathbf{X}^H \mathbf{s}_{surv} \quad (2.27)$$

Therefore, the surveillance signal \mathbf{s}_{ECA} after DSI and clutter cancellation can be obtained by:

$$\mathbf{s}_{ECA} = \mathbf{s}_{surv} - \mathbf{X}\boldsymbol{\alpha} = \left[\mathbf{I}_N - \mathbf{X}(\mathbf{X}^H \mathbf{X})^{-1} \mathbf{X}^H \right] \mathbf{s}_{surv} \quad (2.28)$$

where \mathbf{I}_N is the $N \times N$ identity matrix. The ECA algorithm can also consider Doppler-shifted replicas of the reference signal in the disturbance subspace in order to additionally suppress non-zero-Doppler clutter components. Besides, efficient implementations of this algorithm have been proposed such as the ECA batches (ECA-B) [Col09; Lom12; Col16].

2.2.3 Range compression and Doppler processing

In order to efficiently implement an approximate matched filtering processing based on the computation of the two-dimensional (i.e. delay and Doppler shift) cross-correlation function between the reference and surveillance signals, approaches based on the Fast Fourier Transform (FFT) have been proposed. A common method is the batches algorithm [Mos15], depicted in Figure 2.8, which performs the range compression over subsequent signal batches by the cross-correlation function implemented with FFT and, afterwards, a Doppler processing

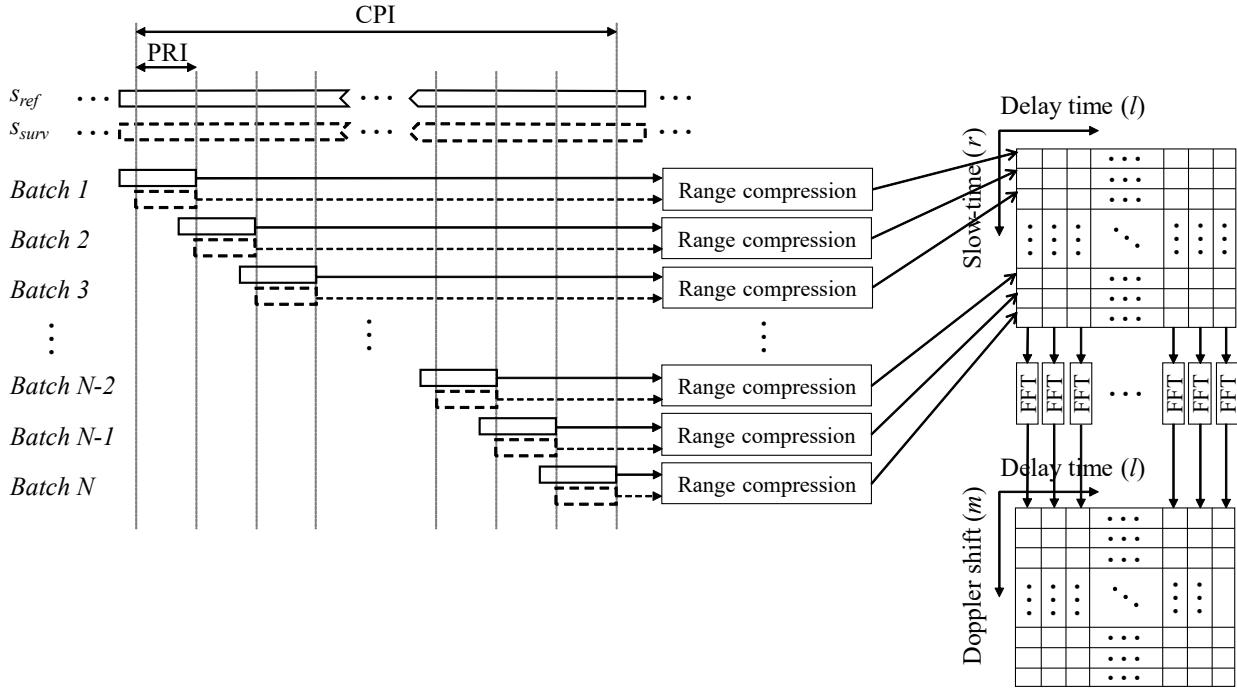


Figure 2.8: Batches algorithm to compute the delay-Doppler cross-correlation function.

coherently integrating the batches during the CPI by applying FFTs over the slow time domain.

The signal segmentation in batches of duration PRI, i.e. Pulse Repetition Interval for its analogy to pulse radar processing, takes into account additional samples of the reference signal in order to allow an integration along the PRI interval over a certain extent of delay bins. To compute the delay time-slow time matrix ($CCF(l, r)$), the range compression based on the cross-correlation function (CCF) between the reference and surveillance signal batches can be efficiently implemented in the Fourier domain applying zero padding in time-domain in order to discard circularly correlated samples [Mar23b]:

$$CCF(l, r) = IFFT \left[S_{surv}[k] S_{ref}^*[k] \right] \quad (2.29)$$

where $S_{surv}[k]$ and $S_{ref}[k]$ are given by:

$$S_{surv}[k] = FFT [s_{surv} [n]] \quad (2.30)$$

$$S_{ref}[k] = FFT [s_{ref} [n]] \quad (2.31)$$

being $FFT[\cdot]$ and $IFFT[\cdot]$ the Fast Fourier Transform and the Inverse Fast Fourier Transform, respectively. Afterwards, Doppler processing can be applied by performing a FFT over the slow-time domain for each delay bin in order to obtain the delay time-Doppler shift matrix ($CCF(l, m)$):

$$CCF(l, m) = FFT [CCF(l, r)] \quad (2.32)$$

which is also the so-called range-Doppler map given the relationship between delay and bistatic range.

The selection of shorter batch lengths (i.e. PRI) limits the operating bistatic range of the system and increases the computational load. However, longer batches lead to increased SNR losses and Doppler ambiguities, especially for fast targets, due to the considered approximation of constant phase during the PRI and the sampling in the slow-time domain. Therefore, PRI selection should take into account both the maximum bistatic range of the area of interest and the maximum expected Doppler frequency of the targets.

Depending on the characteristics and internal structure of the considered signals of opportunity, high correlation sidelobes and ambiguities may appear in the range-Doppler map, as evaluated by the ambiguity function. Therefore, mismatched filtering techniques have also been developed to reduce sidelobes and avoid masking of weak targets, such as the reciprocal filter [Mar23a] or the Doppler Channel Detector (CHAD) [Gas16] for OFDM signals, which also enable the application of Space-Time Adaptive Processing (STAP) [Woj18; Bla23b] and other clutter cancellation approaches [Qui23] by removing the content-dependent variability of the ambiguity function.

Besides, if the bistatic range or Doppler frequency of a target changes during the CPI more than the bistatic range or Doppler resolution, the target response is spread over several resolution cells reducing the coherent integration gain. These range and Doppler migration effects can be addressed by applying Target Motion Compensation (TMC) or Track-Before-Detect (TBD) techniques [San20] in order to effectively increase the coherent integration time. These techniques are usually based on assumptions or approximations of target dynamic

models and are often computationally expensive, especially when high-order dynamics are compensated and the parameter search space is multidimensional.

A common TMC technique to compensate for the range migration induced by a constant bistatic velocity, i.e. first-order motion compensation, is the Keystone Transform (KT) [Pig17]. For this purpose, KT is applied in the fast-time Fourier-transform domain (i.e. before the IFFT of the range compression in the previously described batches algorithm) by rescaling the slow time r to \bar{r} for each fast-time frequency $f[p]$:

$$\bar{r} = \frac{f_T + f[p]}{f_T} r \quad -\frac{N_B - 1}{2} \leq r \leq \frac{N_B - 1}{2} \quad (2.33)$$

where f_T is the center transmitting frequency, p is the fast-time frequency index, and N_B is the number of batches during the CPI, which is considered to be an odd number. In order to apply the IFFT along the fast-time frequency, a rectangular grid in the region of support is needed and, therefore, the original fast-time frequency domain should be actually interpolated at $r = \frac{f_T}{f_T + f[p]} \bar{r}$ with $-\frac{N_B - 1}{2} \leq \bar{r} \leq \frac{N_B - 1}{2}$, as schematically shown in Figure 2.9.

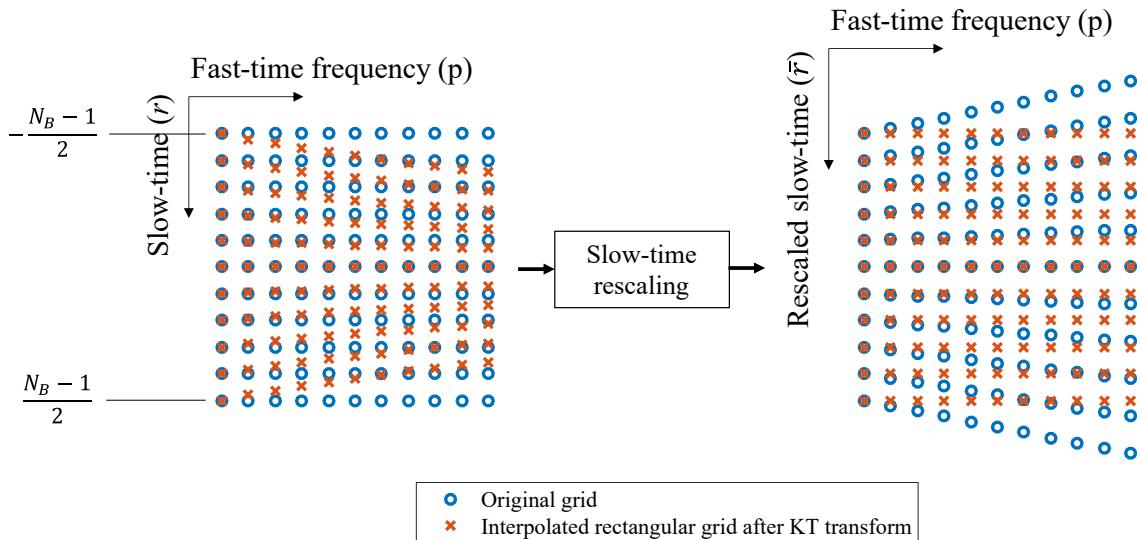


Figure 2.9: Keystone Transform for first-order motion compensation.

Apart from the conventional sinc interpolation, which is used in this thesis when first-order TMC is applied, other resampling techniques using a chirp-z-transform [Sha16] or Lagrange polynomial interpolation [Pig17] have been proposed to reduce the computational load of the KT algorithm.

Part II

LONG-TERM EVOLUTION-BASED PASSIVE RADAR

Chapter 3

LTE-Based Passive Radar System: Analysis, Design and Developments

This chapter presents the design of a passive radar system based on the use of Long-Term Evolution (LTE) downlink signals as illumination of opportunity, addressing the perimeter surveillance of high-speed railway networks as an application scenario. Taking into account the specifications and standard of the LTE system, the ambiguity function of measured downlink signals is analysed in terms of the range and Doppler resolutions and ambiguity and sidelobe levels. The deployment of the proposed passive radar is flexible and scalable, and it is based on multichannel software defined radio (SDR) receivers that obtain the reference and surveillance signals by means of digital beamforming. The signal processing and data fusion are based, respectively, on the delay-Doppler cross-correlation with the reconstructed reference signals and a two-stage tracking at sensor and central level. Finally, the performance of the proposed system is estimated in terms of its maximum detection range and simulation results of the detection of moving targets are presented, demonstrating its technical feasibility for the short-range detection of small drones.

3.1 Motivation of high-speed railways surveillance

In the recent years, several European, North-American and Asian countries are becoming more interested in the development and expansion of their high-speed railways (HSR) networks, which have been prioritized by several governments as the motor of their local economy [Hen17]. However, trains designed to travel at speeds up to 400 km/h open new technological challenges in terms of safety and security.

In one hand, since HSR networks are considered critical infrastructures, the surveillance of the railway perimeter is a high priority requirement for avoiding uncontrolled intrusions that may endanger the security. Besides, it has been recently exposed the necessity of developing new perimeter surveillance systems that deal with the negligent or malicious usage of consumer drones. Current systems are based on fence sensor monitoring [Ind], detecting impacts of objects and jumps over the fence, surveillance cameras [FLI], or active radars [Adv] that autonomously monitor, detect and alert operators of moving objects in protected areas. Nevertheless, these surveillance systems show certain limitations in HSR scenarios: fence sensors cannot detect aerial vehicles such as drones; surveillance cameras are severely affected by weather and light conditions, and, due to their narrow field of view to achieve long-range detection, they usually require an excessive time to cover the whole volume under surveillance, not suitable for the detection of high-dynamic targets; and mid-range active radars are not appropriate for large longitudinal areas because the deployment of several devices along the rails would entail a considerably high cost.

On the other hand, an accurate system for train and railway monitoring is needed to avoid accidents and to optimize the use of the infrastructure. For this reason, the installation of the European Rail Traffic Management System (ERTMS) is currently mandatory in European HSR, but further research should be carried out to develop robust systems that provide the railway managers with real-time information about the tracks and to detect possible obstacles on the rail. To that end, the integration of a Ku-band radar on the head of the trains has been proposed in [Liu17], but this does not provide a persistent situational awareness along the tracks.

3.1. MOTIVATION OF HIGH-SPEED RAILWAYS SURVEILLANCE

The mobile communication systems deployed in railway scenarios based on the LTE standard are commonly referred to as LTE-Railway (LTE-R) systems [He16]. By exploiting the downlink LTE-R signal as illumination of opportunity in a multistatic passive radar configuration, the proposed solution attempts to address the aforementioned challenges for the surveillance and monitoring tasks of HSR networks.

As schematically shown in Figure 3.1, the receiving nodes of the sensor network can be implemented by using Commercial Off-The-Shelf (COTS) SDR devices, considerably reducing the deployment cost of the system, which in turn makes use of the already deployed LTE-R infrastructure. Besides, this system does not need spectrum allocation, does not interfere with other communication systems and is easily scalable.

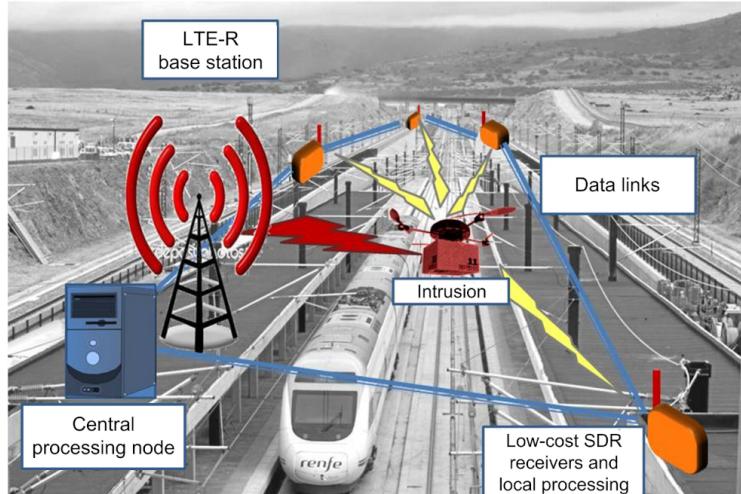


Figure 3.1: Diagram of the proposed LTE-R based passive multistatic radar approach: SDR nodes deployed along the railway receive the LTE-R reference signal and its reflections on the targets, apart from other multipath components. The target detections performed locally in each receiving node are sent to a central processing node where data fusion and target tracking can be performed.

A passive radar system for train monitoring exploiting the Global System for Mobile communications-Railway (GSM-R) has been presented in [Che16]. However, the novelty of the proposed system is the use of passive multistatic radar techniques based on LTE-R signals to provide surveillance and monitoring services to HSR scenarios. The design, experimental signal analysis and simulated target detection results are presented in this chapter, while the Chapter 4 shows the results of the experimental validation for drone detection using a single LTE-based passive radar node.

3.2 Analysis of LTE as illumination of opportunity

3.2.1 LTE-R specifications and downlink waveform

Due to the limited capacity and capabilities of GSM-R and in view of the performance and maturity level of LTE, LTE-R started to be deployed as the standard mobile communication system for HSR, accomplishing new operational needs, being compatible with the standard 4G LTE network, and coexisting with GSM-R [He16]. While the 5G standard for high-mobility scenarios is planned to be expanded along the railway networks over the next few years [Noh20], the deployed LTE network is expected to remain operational, as GSM coverage has typically been maintained.

The LTE variant for railway scenarios (i.e. LTE-R) is based on the LTE standard and it uses a subset of the LTE parameters in order to guarantee the specific requirements of HSR scenarios in terms of mobility, reliability and capacity. In this way, LTE-R systems have a linear coverage along the track instead of cellular deployment and, preferably, uses modulations with low-order constellations and lower frequency bands in order to maintain a low symbol error rate, extend coverage and reduce handovers. LTE-R network achieves not only the safe operation of trains, but also enables more advanced railway services than GSM, complying with the following operational needs: high-speed movements up to 500 km/h, broadband wireless transmission for real-time video, low latency up to 500 ms, network reliability and availability and quality of service [Son16]. In order to attain all these requirements, the system parameters of LTE-R are listed in Table 3.1.

Uplink LTE-R is based on single-carrier frequency division multiple access (SC-FDMA), whereas downlink LTE-R signals use orthogonal frequency division multiplexing (OFDM) with 15 kHz subcarrier spacing, while each subcarrier is modulated using quadrature phase-shift keying (QPSK) or 16-quadrature amplitude modulation (16-QAM).

Based on the physical layer of the LTE standard [Eur17], the frame structure of downlink LTE-R signals using frequency division duplex (FDD) and normal cyclic prefix is represented in Figure 3.2. In order to demodulate the transmitted signal, the physical layer includes two synchronization signals, the primary synchronization signal (PSS) and the secondary

Table 3.1: LTE-R System Parameters

<i>Parameter</i>	<i>Specification</i>
Frequency	700 MHz, 800 MHz, 1.8 GHz, 2.6 GHz
Bandwidth	1.4 - 20 MHz
Modulation	QPSK/16-QAM
Multiple access scheme	OFDM/SC-FDMA (Downlink/Uplink)
Cell range	4-12 km
Cell configuration	Linear coverage
Peak data rate	50/10 Mbps (Downlink/Uplink)
Mobility	Max. 500 km/h

synchronization signal (SSS), which are transmitted twice in each frame, and reference signals (RS), which are used for channel estimation and equalization. The frame structure of the downlink LTE-R signal with the insertion of cyclic prefixes in guard intervals and pilot subcarriers give rise to ambiguities when applying the range-Doppler cross correlation processing in passive radars, which may compromise their performance by masking real targets or causing false alarms. For this reason, since communication signals are not optimized for radar use, it is important to analyse the suitability of downlink LTE-R signals as illumination of opportunity for passive radar by means of the ambiguity function [Eve15].

Besides, the usage of a digital signal allows to obtain a noise-free reference signal by demodulation and subsequent remodulation of the received direct signal transmitted by each LTE-R base station in order to improve the actual performance of the passive radar system. This reconstruction of the reference signal is based on the physical layer standard of LTE and it includes the processing steps displayed in Figure 3.3.

With the setup shown in Figure 3.4, consisting of a USRP N2945 SDR device and a directive antenna for the reference channel, LTE signals were acquired to perform an experimental characterization. Figure 3.5 shows the normalized power spectrum of a downlink LTE transmission. In this case, the transmitted signal is allocated in a 10 MHz-bandwidth channel

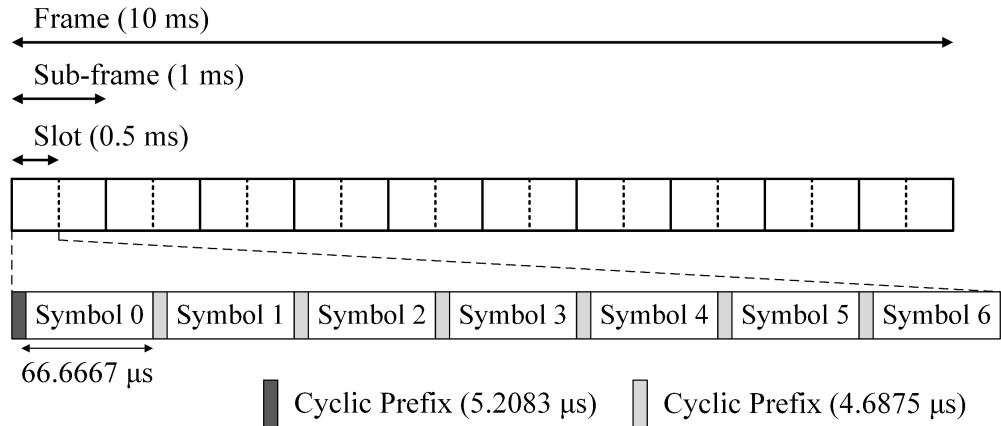


Figure 3.2: Frame structure of downlink LTE-R signals using FDD and normal cyclic prefix.

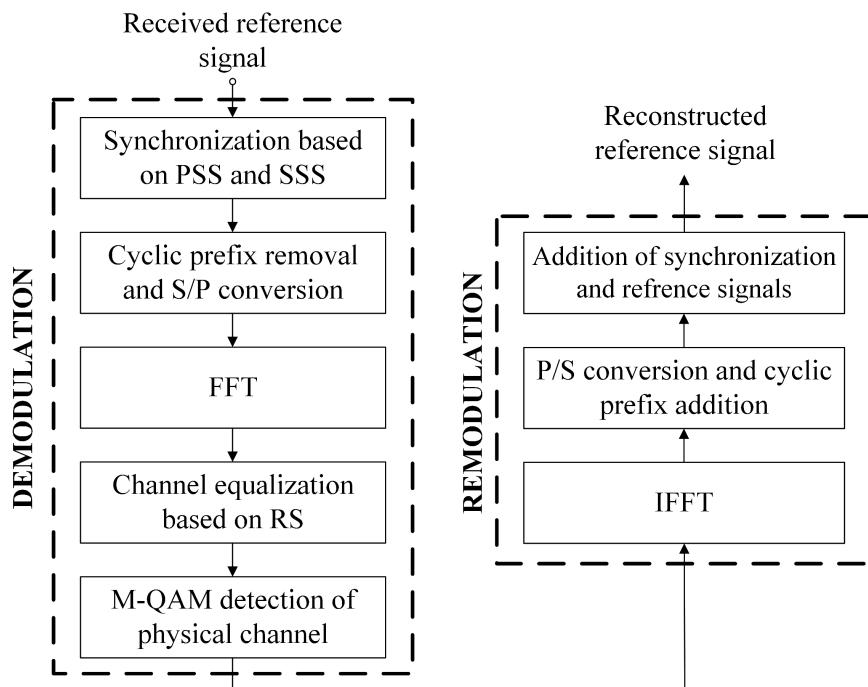


Figure 3.3: Reconstruction processing of downlink LTE signal based on demodulation and subsequent remodulation in order to obtain a noise-free reference signal for passive radar usage (PSS = primary synchronization signal; SSS = secondary synchronization signal; RS = reference signals; S/P = serial to parallel; P/S = parallel to serial; FFT = Fast Fourier Transform; IFFT = inverse FFT; M-QAM = M-ary quadrature amplitude modulation).

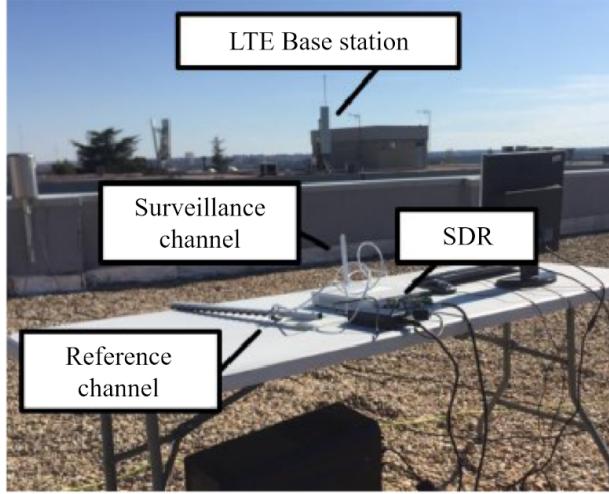


Figure 3.4: Receiving setup used for LTE signal characterization, composed of a USRP N2945 SDR device, a directive antenna for the reference channel, and preliminary an onmidirectional antenna for the surveillance channel.

at the 800 MHz band. However, the actual bandwidth of the signal does not occupy the whole channel due to the use of guard bands to avoid interfering the adjacent channels. When using downlink LTE signals as the illumination of opportunity, this bandwidth reduction decreases the bistatic range resolution of the passive radar system. Besides, the power spectrum of the received signal shows a ripple due to the frequency-dependent channel response, which should be equalized before demodulation by using the reference signals (RS) transmitted in the LTE frame.

As an example of the output of the demodulation processing, Figure 3.6 shows the constellation diagram for the Physical Downlink Shared Channel (PDSCH) of a measured downlink LTE signal after channel equalization. The 4-QAM detector, the subsequent remodulation of the physical layer channels and the addition of synchronization and reference signals based on LTE standard allows to ideally obtain a noise-free reference signal to be cross-correlated with the surveillance signals in the passive radar signal processing, described in Subsection 3.3.2.

3.2.2 Self ambiguity function analysis of downlink LTE signals

The bistatic range and Doppler resolution achievable by each receiving node of the multistatic system can be evaluated based on the main peak width of the self Ambiguity Function (AF)

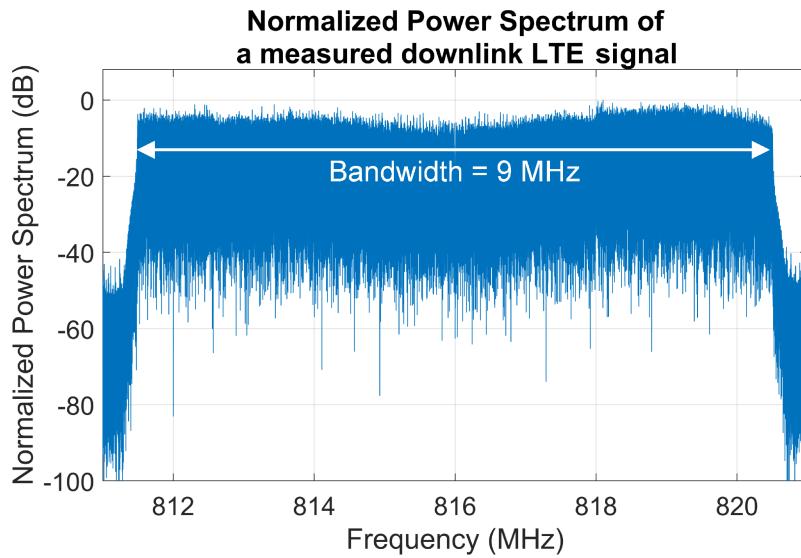


Figure 3.5: Normalized power spectrum of a measured 10 MHz-channel downlink LTE signal at the 800 MHz band.

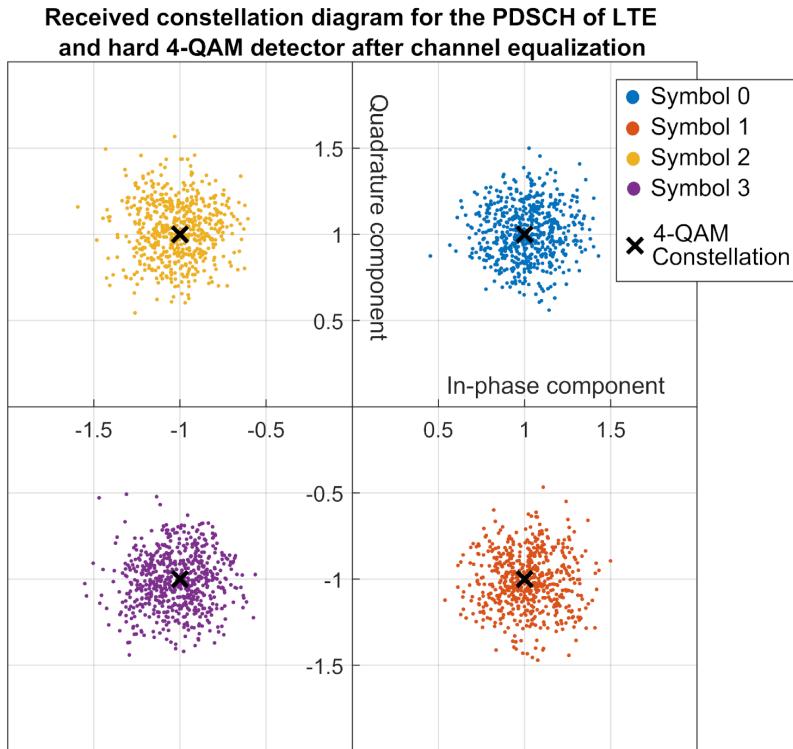


Figure 3.6: Received constellation for the Physical Downlink Shared Channel (PDSCH) of LTE after channel equalization. The colour of the points indicates the output of the hard 4-QAM detector.

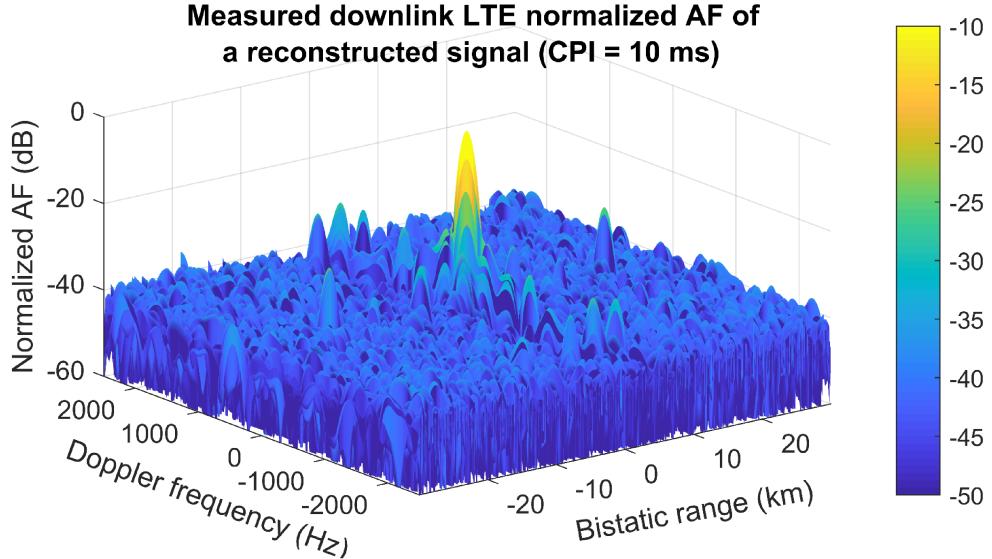


Figure 3.7: Normalized range-Doppler AF of a reconstructed 10 MHz-channel downlink LTE signal using a CPI of 10 ms and applying Hamming windows at frequency and time domain as a sidelobe reduction technique.

of the downlink LTE reference signals, which represents the output of the matched filter and is computed by the Equation 2.16. However, it should be noted that the actual bistatic range resolution is related to the bistatic geometry between the target and each transmitter-receiver pair [Bak05], as represented by the Equation 2.9.

Based on a received downlink 10 MHz-channel LTE signal, Figure 3.7 shows the range-Doppler AF computed after reference signal reconstruction using a coherent processing interval (CPI) of 10 ms. In order to reduce the sidelobe level, Hamming windows in the frequency and time domain have been applied. The obtained AF presents a near-thumbtack shape suitable for passive radar usage, but it shows several ambiguities due to the structure of the downlink LTE signal. In order to analyse the bistatic range and Doppler resolution and the sidelobe level of downlink LTE signals as illuminators of opportunity, the zero-Doppler cut and the zero-range cut of the computed AF for different CPIs are represented in Figure 3.8, respectively.

As it can be observed in the zero-Doppler cut, the bistatic range width of the AF main peak from the reconstructed downlink LTE signal is approximately 48 m for all the considered CPIs, which is in agreement with its approximate 9 MHz bandwidth and the resolution decrease due to the Hamming windowing [Har78]. Besides, the floor level is decreased when increasing

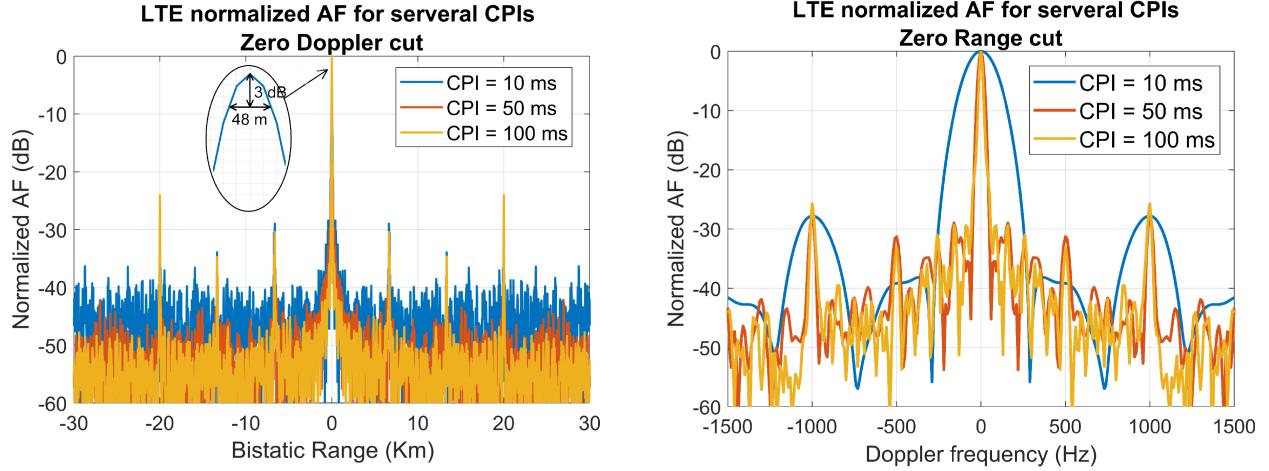


Figure 3.8: AF zero-Doppler cut (left) and zero-range cut (right) of a reconstructed downlink LTE signal using different CPIs.

the CPI as it is expected due to the compression gain given by the product of the bandwidth and the CPI. However, a high range ambiguity appears at 20 km of bistatic range due to the cyclic prefix of the OFDM modulation. This ambiguity is related to the $66.7 \mu\text{s}$ useful symbol time (T_u) of the LTE physical layer and it has a level approximately given by the ratio between the average cyclic prefix time ($\bar{T}_{CP} = 4.77 \mu\text{s}$ for the normal cyclic prefix) and the useful symbol time (Ambiguity level = $20 \log_{10} (\bar{T}_{CP}/T_u) = -23 \text{ dB}$). In the proposed passive radar system, the considered instrumental range is shorter than 20 km in bistatic range and, therefore, this range ambiguity does not compromise its performance. Besides, there are weaker ambiguities at 6.67 km and 13.33 km due to the synchronization signals. If these ambiguities are expected to affect the performance of the system in the area of interest, mismatched filters could be used to reduce the level of sidelobes and ambiguities at a cost of a SNR loss, such as the reciprocal filter suitable for OFDM signals [Woj18; Rod23], which is based on a response equalization removing the data-dependence and achieving a 2D sinc-like ambiguity function in accordance to the signal bandwidth and CPI.

Regarding the Doppler resolution, using a CPI of 10 ms, the zero-range cut shows a -3 dB peak width of 172 Hz for the time domain Hamming windowed signal, which corresponds to a bistatic velocity resolution of 64.5 m/s (employing the 800 MHz LTE band). This poor velocity resolution can be improved by using longer CPIs. This also increases the signal-to-noise ratio (SNR) of the targets and, accordingly, the maximum detection range of the system as long

as the target coherence is maintained during the integration time. For this reason, in order to obtain a suitable velocity resolution and enhance detection range, a CPI of 250 ms is suggested for the considered passive radar system, which corresponds to a bistatic velocity resolution of approximately 2.8 m/s applying the Hamming window.

In the zero-range cut of the AF, Doppler ambiguities appear at multiples of 1000 Hz due to the pulsed structure of the LTE signals, which are divided in subframes of 1 ms. However, these ambiguities are not significant for the proposed system because they correspond to multiples of 1350 km/h in bistatic velocity (at 800 MHz center frequency), which are clearly much higher than the bistatic velocities of the expected targets.

An additional acquisition of a 50 ms-LTE signal transmitted with 20 MHz bandwidth was also analysed, showing similar results in terms of ambiguities, but with a higher bistatic range resolution in accordance to the increased bandwidth. Figure 3.9 represents the signal in the time domain, its spectrum, and the OFDM grid after synchronization and OFDM demodulation, showing the typical structure of the PSS, SSS, RS and control signals (i.e. "always on" signals) but a limited load in terms of user data signals (i.e. PDSCH). However, the computed ambiguity function represented in Figure 3.10 shows properties suitable for passive radar application despite the ambiguities already mentioned.

Therefore, taking into account the bistatic range and Doppler resolution, the floor level and the ambiguities estimated by means of the self AF of measured downlink LTE signals, it can be concluded that these signals are suitable for being used as illuminations of opportunity for passive radar systems, even when they predominantly contain the "always on" components.

3.3 LTE-R based passive radar system design

3.3.1 Hardware architecture

The geometrical deployment of the suggested passive multistatic radar system composed of two LTE-R transmitters of opportunity and two receiving nodes is depicted in Figure 3.11, where the distance between two consecutive LTE-R base stations (eNodeB 1 and eNodeB 2) is considered to be 10 km. A multistatic architecture is considered in order to improve target

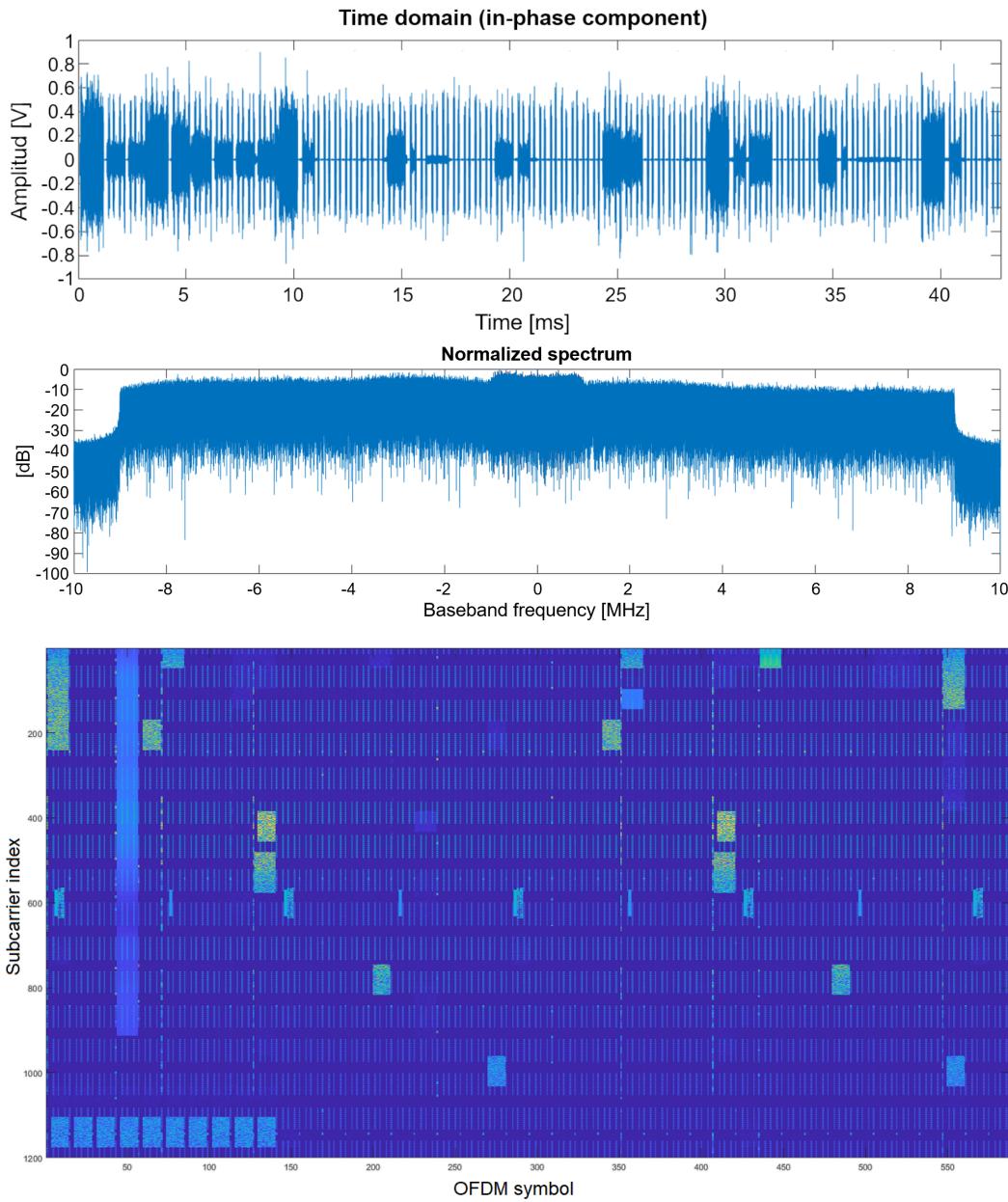


Figure 3.9: Acquisition of a 50 ms-LTE signal with 20 MHz channel bandwidth: Time domain in-phase component, normalized spectrum, and OFDM grid after demodulation.

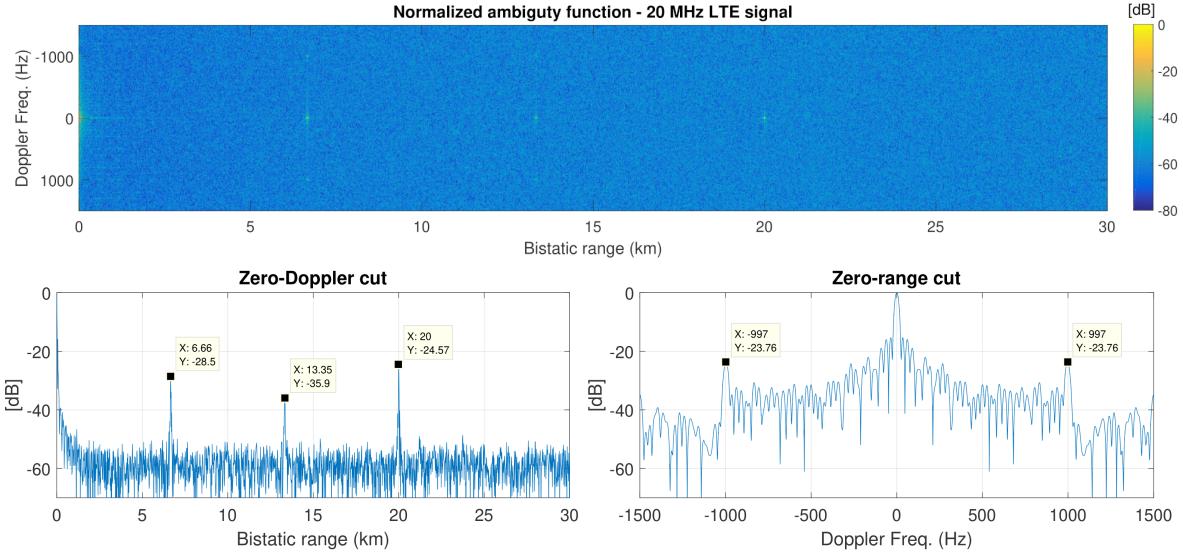


Figure 3.10: Normalized range-Doppler AF of a received 20 MHz-channel downlink LTE signal using a CPI of 50 ms (top) and associated zero-Doppler and zero-range cuts (bottom).

localization and target detection thanks to spatial diversity and multilateration [Sai05; Col12]. Besides, this deployment can be scaled up along the railway track or include more receiving nodes to improve the system performance and coverage.

Each receiving node is based on a SDR device (National Instruments’ USRP-2945) [Nat] with four coherent receiving channels capable of sampling an instantaneous bandwidth of 80 MHz, allowing the application of digital beamforming techniques to receive the reference and surveillance signals. In order to be able to spatially separate both endfire directions, the four antenna elements are arranged in a uniform linear array (ULA) with $\lambda/3$ spacing (12.5 cm for the 800 MHz LTE-R band) between them and broadside direction perpendicular to the railway track. Each antenna element has a 3 dBi gain and an omnidirectional radiation pattern.

As shown in Figure 3.12, the SDR modules comprise the radio frequency (RF) front ends, the intermediate frequency (IF) stages, 14 bit analog-to-digital converters (ADC) and a field programmable gate array (FPGA), where the signal processing can be performed to obtain the detections of the targets. The FPGA is connected through Peripheral Component Interconnect Express (PCIe) to a computer, which controls the SDR device and performs the distributed data processing of the target plots generated by the signal processing. Finally,

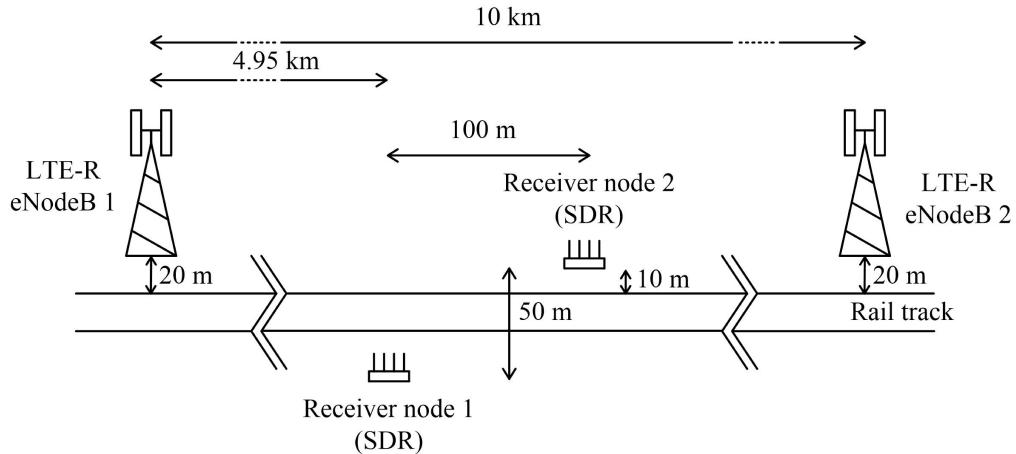


Figure 3.11: Geometrical deployment of the suggested passive multistatic radar system (figure not to scale).

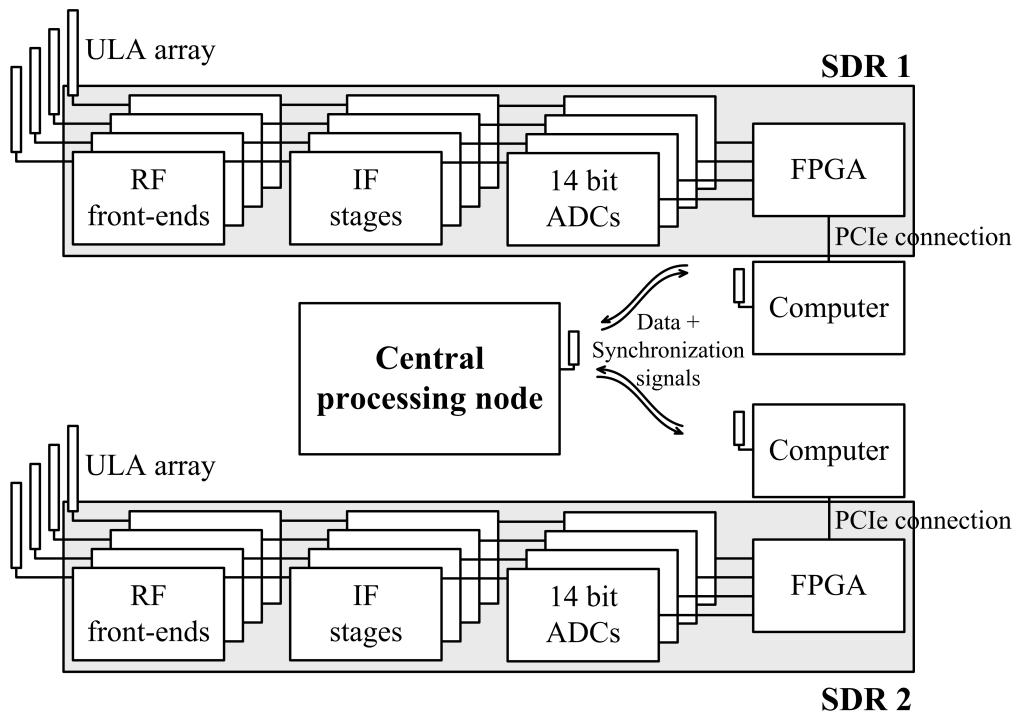


Figure 3.12: Hardware architecture of the passive multistatic radar system including the receiving nodes based on SDR devices and a central processing node.

the computer transmits through a radio link the data to a central processing node, which performs the centralized data fusion and processing. Besides, this central processing node broadcasts synchronization signals through the radio link to the distributed receiving nodes.

3.3.2 Signal processing and multistatic data fusion

The block diagram of the signal processing performed in each receiving node of the proposed passive multistatic radar system is shown in Figure 3.13. Firstly, a digital beamforming is applied in order to acquire the two reference signals from the two LTE-R illuminators of opportunity and several surveillance channels from different directions. To this end, different simultaneous antenna beams with distinct nulls and main lobe directions are synthesized. As shown in Figure 3.14, one reference beam is pointed to each LTE-R base station with a null in the direction of the other transmitter, whereas the overlapped surveillance beams have nulls in the direction of its associated transmitter of opportunity in order to reduce direct signal interference. Although, azimuth ambiguities arise from the ULA radiation patterns, these ambiguities are removed in the data fusion stage. To avoid blind zones in each transmitter-receiver pair, the signal received by the reference beam could also be used as a surveillance signal after direct signal and multipath cancellation, but it may have stronger interferences and, consequently, a lower target detection capability. However, even without using this approach, the whole 360° are covered with at least two transmitter-receiver pairs.

Using the signals received with the two reference beams, the transmitted LTE-R signals are reconstructed based on the physical layer specifications of the communication standard. This approach, as suggested in [Col12], allows us to avoid the use of two dedicated receiving channel for the reference signals.

In each surveillance channel, considering both reconstructed reference signals, direct signal and multipath cancellation [Lom12] is firstly applied to reduce direct path interference and remove the echoes due to static clutter. Afterwards, the windowed range-Doppler cross correlation function between each surveillance channel and each reference signal is calculated. Taking into account the cellular deployment of LTE-R, in which two adjacent base stations use separate frequency channels, a low interference between the two reference signals is assumed.

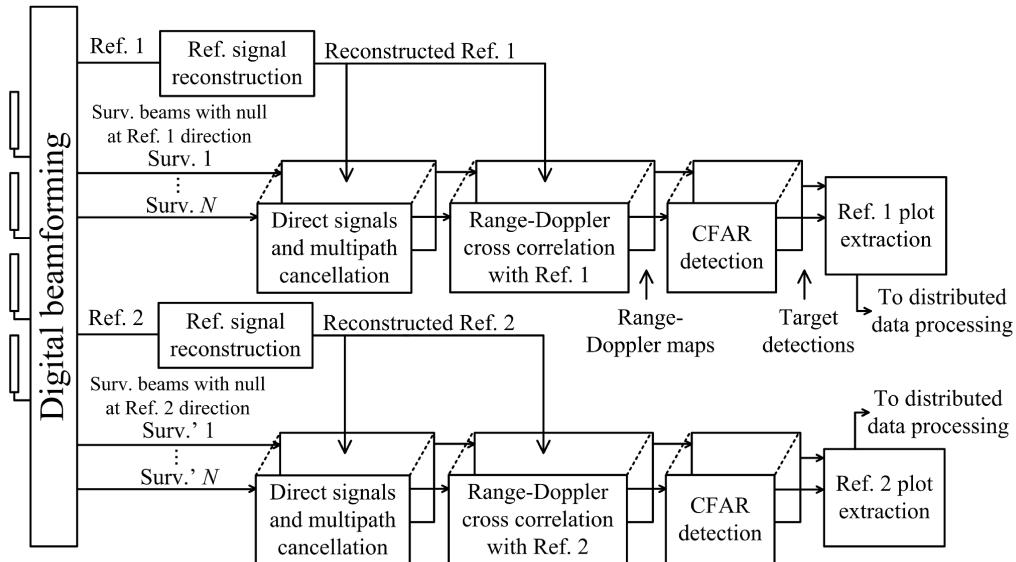


Figure 3.13: Block diagram of the signal processing applied in each receiving node of the passive multistatic radar system exploiting two LTE-R reference signal transmitted from two different eNodeB.

Therefore, being these reference signals almost orthogonal, the target echoes from the two base stations can be separated in each receiving node.

Finally, a Constant False Alarm Rate (CFAR) [Roh83] detector is applied to each range-Doppler map and the plot extractor obtains the bistatic range, azimuth and bistatic velocity estimations of the detected targets from the peaks of the cross correlation functions.

Regarding data processing and data fusion, a two-stage tracking [Le615; Mal09] is implemented. This approach is divided into a first distributed tracking for each transmitter-receiver pair using the plots extracted by the signal processing and a second centralized tracking in Cartesian coordinates after the association of the output data from the distributed tracking of multiple transmitter-receiver pairs. Data association is based on a bottom up processing [Fol05], in which a finite set of possible target position inside the area of interest are considered and target positions are located at local minima of an error function calculated for each grid point. This error function is given by the quadratic sum of the distances between the considered grid point and the closest measurement of each transmitter-receiver pair. This approach allows us to reduce the global false alarm rate of the system and avoid ambiguities and ghost targets with an attainable computational complexity even in multi-target situations.

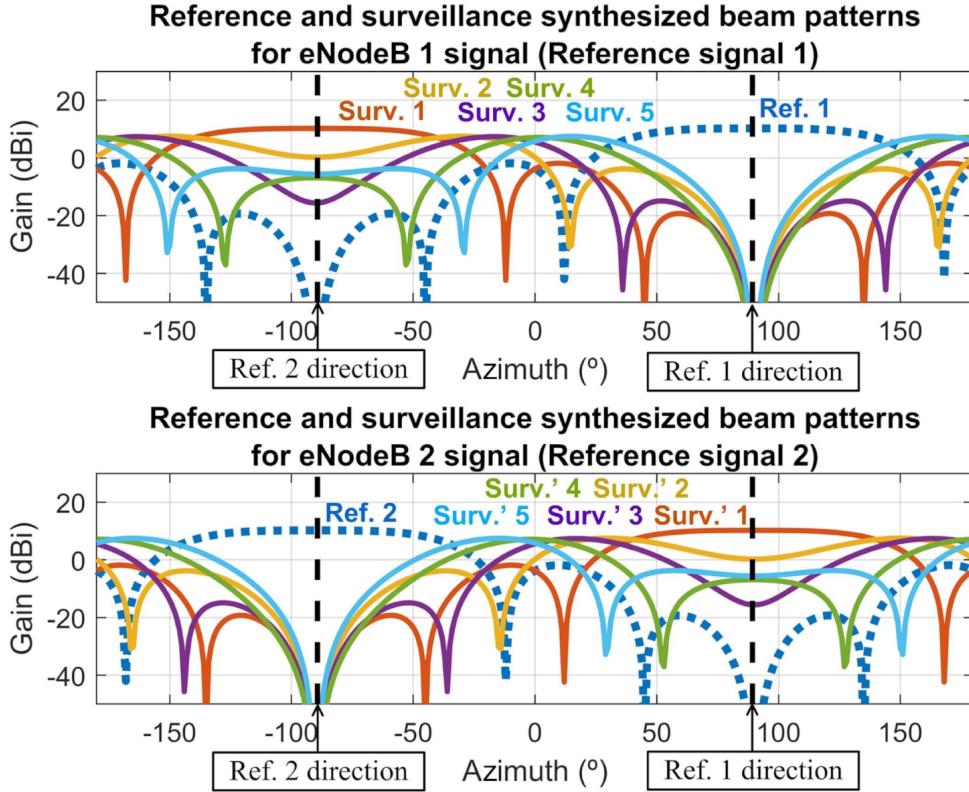


Figure 3.14: Reference (dotted lines) and surveillance (solid lines) synthesized beams of the receiver node 1 for the two considered LTE-R eNodeB illuminators of opportunity. Azimuth is considered with respect to the broadside direction of the array (i.e. perpendicular to the railway tracks). Note that, based on the considered geometrical deployment, the direction of arrival of the reference transmitters are approximately 90° and -90° in azimuth.

3.4 Estimation of covered area and simulation results

In order to demonstrate the technical feasibility of the proposed surveillance and monitoring system in terms of its maximum detection range, Figure 3.15 shows its estimated covered area based on the bistatic radar equation, presented in Equation 2.11, for the detection of cars, pedestrians and small drones, using the parameters presented in Table 3.2 and considering that at least one transmitter-receiver pair achieves 90% probability of detection (P_d) with 10^{-5} probability of false alarm (P_{fa}).

To estimate this covered area, an eNodeB antenna radiation pattern of 30° -3 dB-beamwidth pointed over the rail track towards the receivers and the synthesized surveillance beams for each reference signal have been taken into account. Besides, due to the expected suppression of the DSI and clutter by both the beamforming and the cancellation stage of the signal processing

Table 3.2: Parameters used for the estimation of the covered area

Parameter	Value
Transmitted power	40 W
Transmitter antenna gain	14 dB
Receiver antenna gain	Synthesized beams
Frequency band	800 MHz
CPI	250 ms
Receiver Noise Figure	5 dB
System losses and margin	5 dB
SNR _{min} for Swerling 1 target, $P_d = 90\%$ and $P_{fa} = 10^{-5}$	20.5 dB

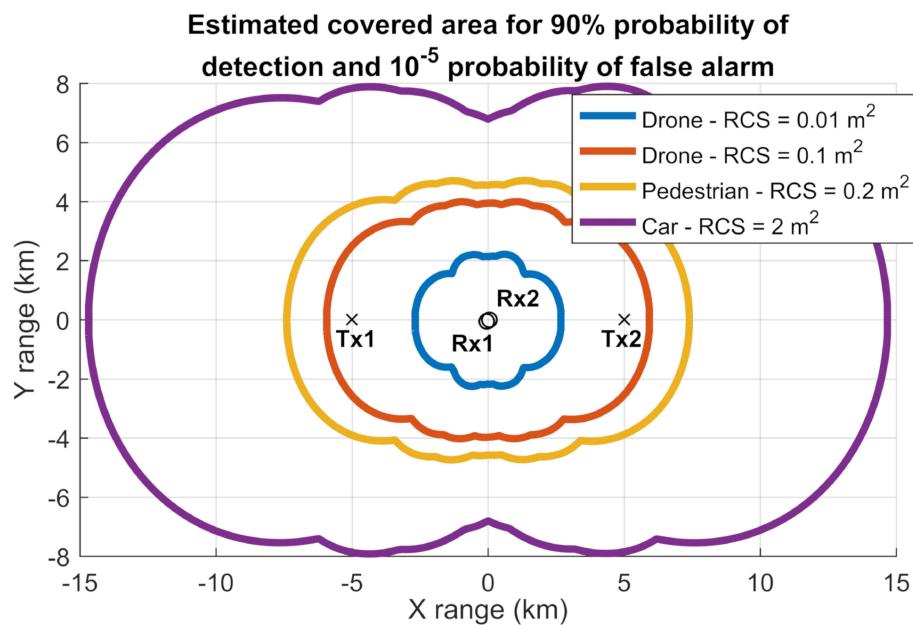


Figure 3.15: Estimation of the covered area by the passive multistatic radar system for the detection of cars, pedestrians and small drones considering that at least one transmitter-receiver pair achieves 90% probability of detection with 10^{-5} probability of false alarm.

3.4. ESTIMATION OF COVERED AREA AND SIMULATION RESULTS

(e.g. ECA), it is assumed that the detection range is limited by thermal noise and not by the residual correlation sidelobes of the DSI and clutter after cancellation. Nevertheless, additional losses (i.e. system losses and margin) are considered to account for possible degradation effects.

The results show an estimated maximum detection range across the rail track of 7 km, 4.5 km and 4 km for cars of 2 m^2 RCS, pedestrians of 0.2 m^2 RCS and small drones of 0.1 m^2 RCS, respectively. Further deployment of receiving nodes along the track would be required if drones of smaller RCS have to be detected by the system. Besides, the considered geometry is scalable and repeatable along the track.

Figure 3.16 shows the obtained SNR of a small 0.1 m^2 RCS drone [Pis18] for the receiver 1 when using each reference signal. Since the reference beams are not used as surveillance beams, blind zones appear for each transmitter-receiver pair but not when all transmitter-receiver pairs are considered. Therefore, the proposed system achieves a suitable covered area for the considered application of railway network surveillance and monitoring, even for the detection of small consumer drones, whose malicious usage may entail safety threats which are becoming a bigger concern of HSR managers.

Furthermore, a dynamic range requirement of 96 dB is estimated taking into account the direct signal power and the minimum detectable target echo power. This stringent dynamic range requirement is common in passive radar systems [Mal14].

High-speed trains are usually over 200 m long and made of metallic structures. Therefore, they act as extended scatters causing strong reflections which can be also detected by the suggested passive radar in order to monitor the traffic of trains. The usage of OFDM with cyclic prefix is robust against these strong multipath components, and the transmitted signals are expected to be properly reconstructed to obtain the noise-free reference signals in spite of a train crossing the coverage area. However, these reflections cause ambiguities due to sidelobes and an increase in the noise floor level of the range-Doppler maps. Although a small area with reduced probability of detection for weak targets can appear near the crossing train in bistatic distance, these degrading effects are diminished thanks to the speed difference between high-speed trains and the typical targets of interest, the properties of the LTE-R

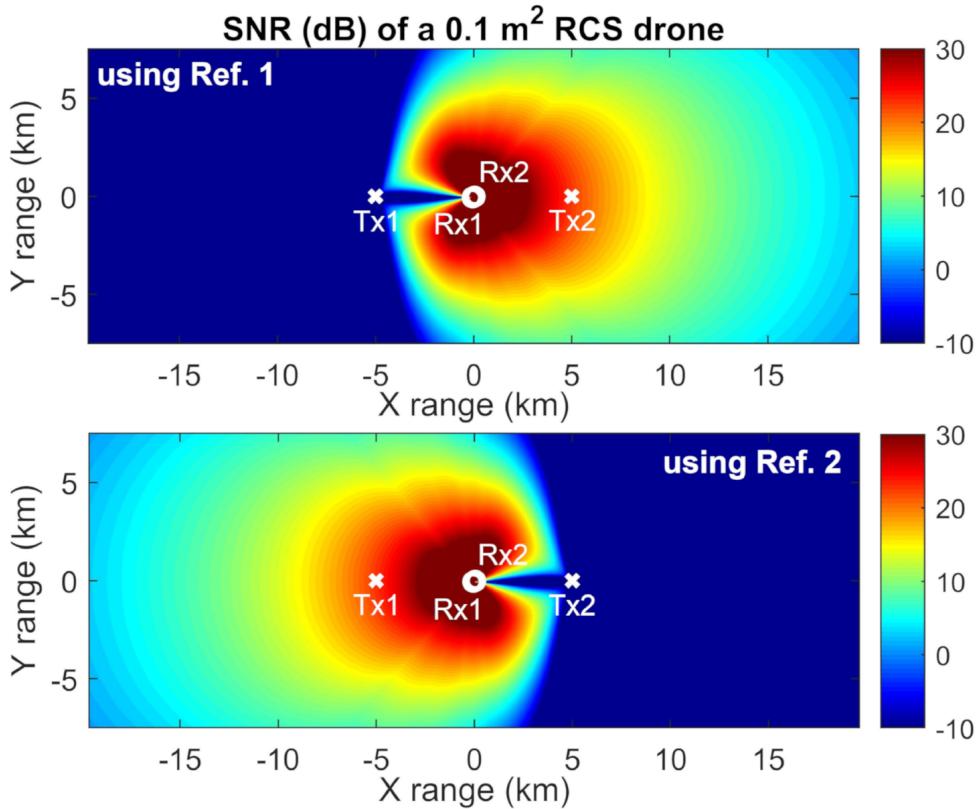


Figure 3.16: SNR in dB for the receiver 1 of a small drone with 0.1m^2 RCS when using the reference signal of the eNodeB 1 (top) and the reference signal of the eNodeB 2 (bottom).

ambiguity function in terms of sidelobe and noise floor levels, and the possibility to apply adaptive cancellation methods such as the Extensive Cancellation Algorithm (ECA) [Col16] or CLEAN algorithm [Kul08].

Finally, to illustrate the importance of applying accurate DSI and multipath cancellation techniques, Figure 3.17 shows the range-Doppler cross-correlation outputs, with and without DSI and multipath cancellation, between the LTE reference signal and a simulated surveillance channel. Apart from the interference produced by the direct signal, the simulated surveillance channel contains several multipath components due to static clutter and the returns of two weak targets (Target 1 and Target 2), which are, respectively, 40 dB and 50 dB below the direct signal interference. When DSI and multipath cancellation is not applied, the returns from the targets are masked by the noise floor and they cannot be detected. However, when DSI and multipath components are suppressed, the targets can be detected, but they give rise to range and Doppler ambiguities due to the signal structure, which can be reduced by

3.4. ESTIMATION OF COVERED AREA AND SIMULATION RESULTS

applying sidelobe reduction techniques, e.g. the reciprocal filter as a mismatched filter for the range compression [Rod23].

The analysis and results presented regarding the considered passive radar architecture and achievable performance show the potential of using downlink LTE signals as illumination of opportunity in passive radars. The suggested passive multistatic radar architecture and processing would be also applicable using other digital communication systems as illumination of opportunity, as long as they transmit in the operation band of the deployed SDRs and antennas, although the actual properties of the AF may change. Besides, the current widespread coverage of LTE system makes it possible to use the suggested multistatic and scalable architecture to provide cost-efficient surveillance services or support to other surveillance systems in different application scenarios including airports, highways or other critical infrastructures.

In order to experimentally validate the developed LTE-based passive radar system for surveillance applications and the application of digital beamforming techniques based on the use of multi-channel SDR devices, field tests with a cooperative target were performed, whose results are presented in the next chapter.

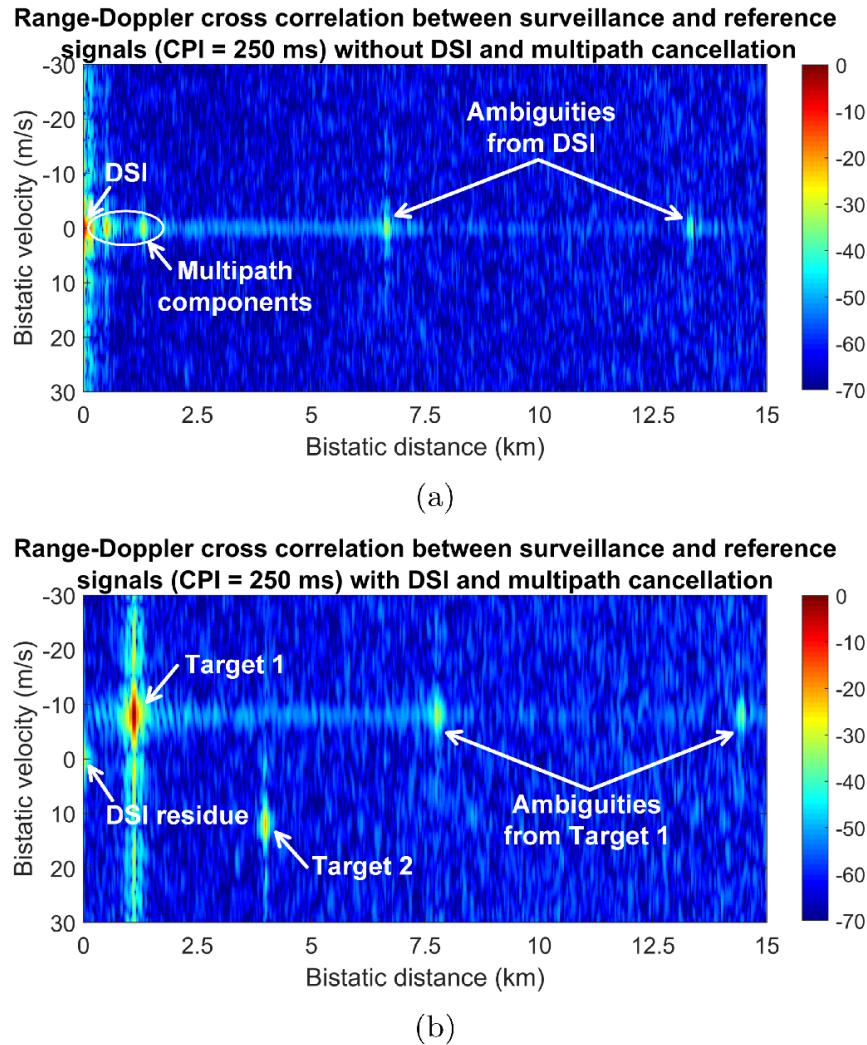


Figure 3.17: Output of the range-Doppler cross-correlation function between the LTE reference signal and a simulated surveillance channel, which contains DSIs, multipath components and the returns of two weak targets: a) Without DSIs and multipath cancellation, and b) With DSIs and multipath cancellation. Range-Doppler maps are normalized to the maximum value. The simulated targets masked by the correlation sidelobes of the DSIs and clutter can be detected when applying a DSIs and multipath cancellation stage. Applying the DSIs and clutter cancellation stage, ambiguities associated to Target 1 are also clearly observed, while those associated to Target 2 with lower RCS are mostly below the noise floor.

Chapter 4

LTE-Based Passive Radar System: Experimental Validation

In order to experimentally validate the proposed surveillance and monitoring system based on the use of downlink LTE signals, a measurement campaign was performed in a semi-urban environment using a single receiving node and a drone as a cooperative target. This chapter presents the results of these field measurements, including an analysis of the considered scenario, and the main conclusions obtained.

4.1 Description of the measurement scenario

The field measurements were carried out in the town of Riocabado (Ávila, Spain) using as illuminator of opportunity the base station located at $40^{\circ}49'43.5''\text{N}$, $4^{\circ}48'22.6''\text{W}$ operated by Vodafone and Orange. As receiving node, a National Instruments SDR USRP-2945 with four coherent receiving channels connected to isotropic antennas forming a non-calibrated non-uniform linear array was deployed at $40^{\circ}49'47.1''\text{N}$, $4^{\circ}48'0.5''\text{W}$. Besides, a DJI Phantom 4 drone was used as a cooperative target.

This scenario is schematically represented in Figure 4.1. The baseline length between the transmitter and the receiver was 500 m and the broadside direction of the deployed four-element array was 100° with respect to North, pointing towards the area where the flights

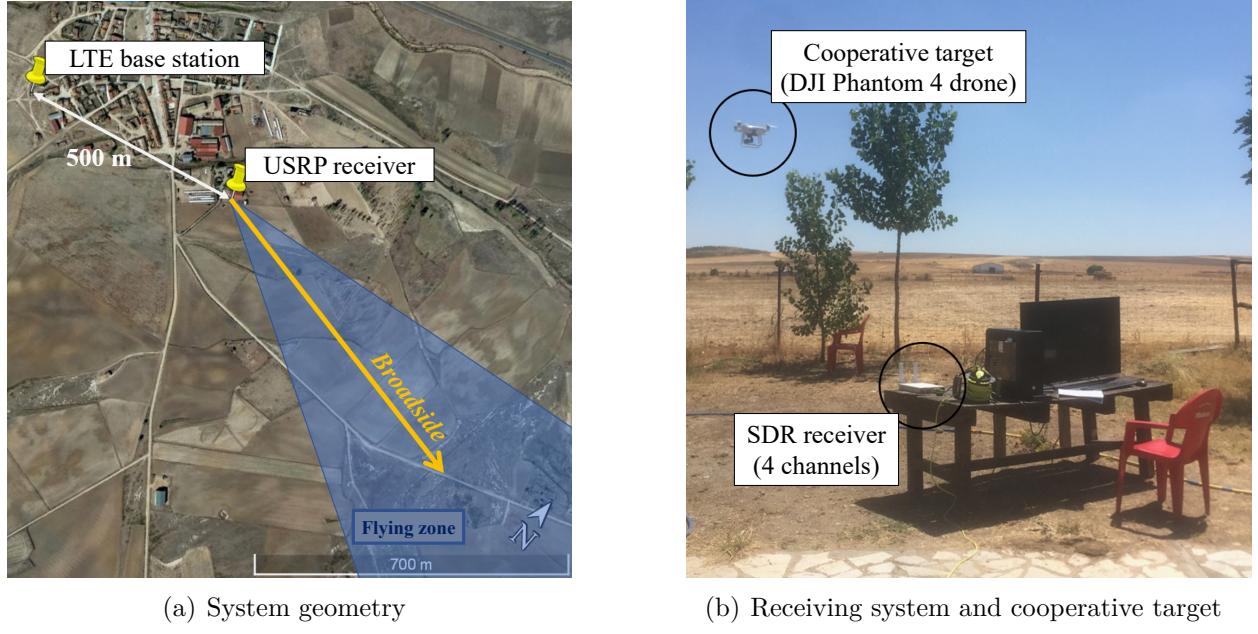


Figure 4.1: Measurement campaign scenario.

of the cooperative target were performed. These elements of the test scenario are described in more detail below.

4.1.1 LTE base station

The frequency channels assigned to the considered base station are specified in Table 4.1 based on the information provided in [Min]. Figure 4.2 represents an estimation of the equivalent isotropic radiated power (EIRP) of the base station as a function of the azimuth angle assuming a free space propagation model from the data reported in [Min].

Table 4.1: Frequency bands assigned to the considered LTE base station.

<i>Operator</i>	<i>Assigned band</i>
Orange	832.0 – 842.0 MHz
Vodafone	842.0 – 852.0 MHz
Orange	925.1 – 935.1 MHz
Vodafone	949.9 – 959.9 MHz
Orange	1859.9 – 1879.9 MHz

Among the channels assigned to the base station, the channels centered at 930.1 MHz with 10 MHz bandwidth and 1869.9 MHz with 20 MHz bandwidth were selected to carry out the measurements. In this way, the results obtained for both frequency channels and

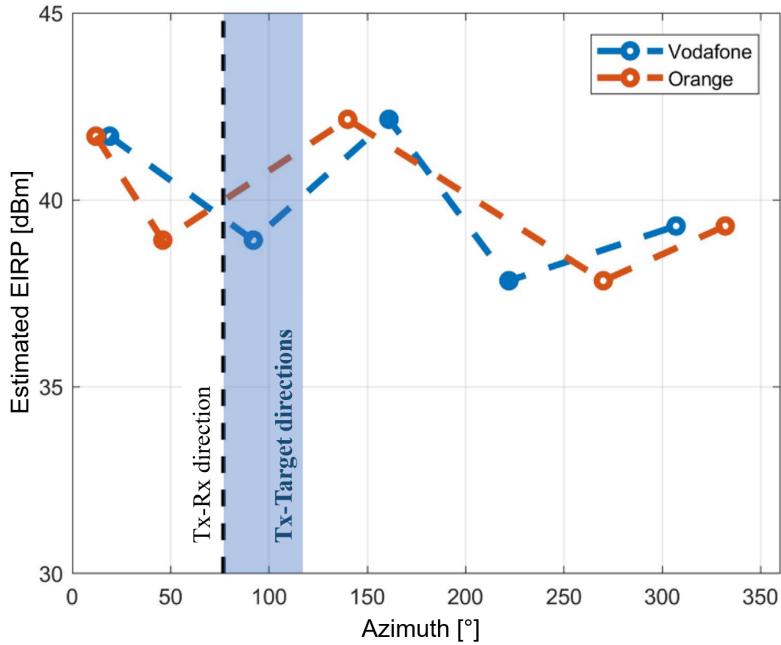


Figure 4.2: Estimated EIRP of the considered LTE base station as a function of the azimuth angle (with respect to North). The direction between the transmitter (Tx) and the receiver (Rx) and, based on the flying zone, the range of directions between the transmitter (Tx) and the cooperative target are indicated. The EIRP is estimated based on power flux density measurements at certain azimuths and distances from the base station reported in [Min] by considering a free-space propagation model. A linear interpolation (dashed lines) is applied between measurements (circles).

bandwidths can be compared, since transmissions at different frequencies involve different propagation [Sar03] and target and clutter scattering mechanisms [Pat18], resulting in different propagation losses, multipath components and target radar cross sections, while different signal bandwidths lead to different bistatic range resolutions.

The EIRP of the selected base station in the considered directions during the experiments is estimated to be higher than 40 dBm, which corresponds to a typical value for LTE base stations.

4.1.2 Passive radar receiver

A National Instruments USRP-2945 SDR device was used as the passive radar receiver with four low-cost omnidirectional LTE antennas. To maintain coherence between the channels and to evaluate the possibility of applying digital beamforming techniques, the USRP was

configured to share the same local oscillator between the four channels. The specified gain of the antennas for the 900 and 1800 MHz bands is 5 dBi and they were placed forming a non-calibrated non-uniform linear array with the configuration shown in Figure 4.3. The control of the SDR parameters and the acquisition of the signals were carried out using a program developed in LabView. The digitised received signals were recorded in a high-speed Solid-State Drive (SSD) for further offline processing. Given the LTE channels selected for the measurements, a receive center frequency of 930.1 MHz or 1869.9 MHz and an IQ sampling rate of 10 MHz or 20 MHz per receiving channel, respectively, were configured. The resolution of the Analogue-to-Digital Converters (ADC) of the used USRP SDR equipment is 14 bits, which limits the dynamic range to 84 dB.

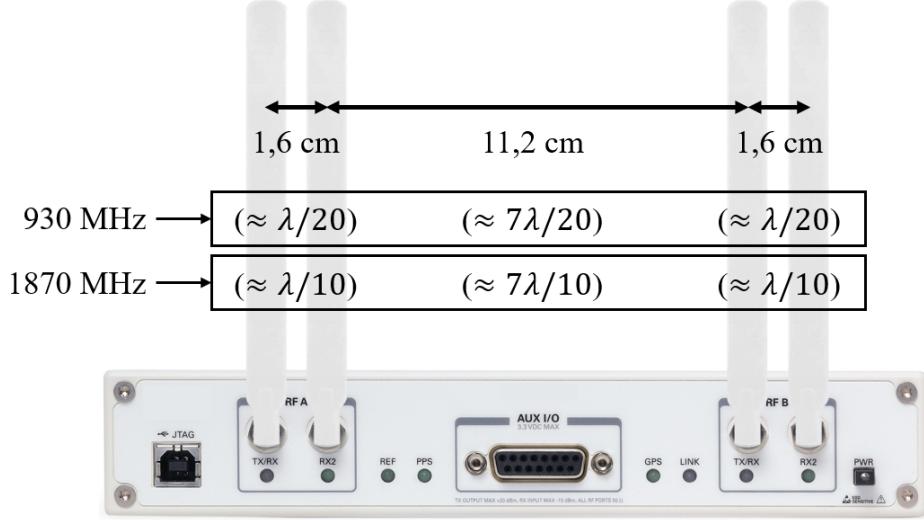


Figure 4.3: Configuration of the antennas connected to the USRP-2945 forming a non-calibrated non-uniform linear array. The approximate relative separations in terms of the associated wavelength (λ) of the considered channel center frequencies are shown.

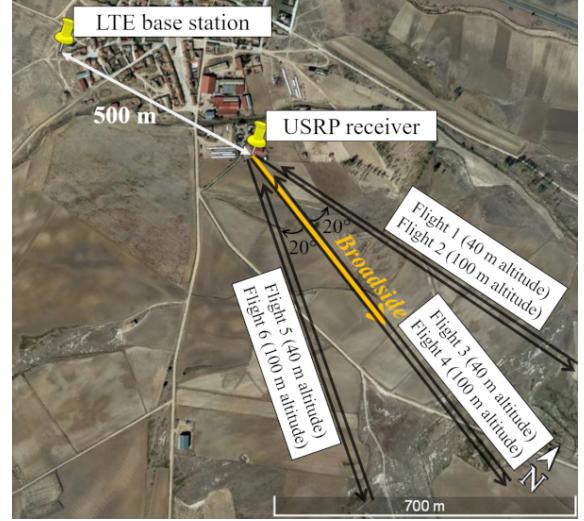
4.1.3 Cooperative target

A DJI Phantom 4 drone as shown in Figure 4.4(a) was used as a cooperative target, which conducted the flights shown in Figure 4.4(b) following radial directions to and from the receiver with distances up to 2000 m away from the receiver at two flight altitudes (40 m and 100 m) and at a speed between 10 and 20 m/s. However, log flight data were not available after the measurements.

Based on several studies [dQue19; Pis18; Sch15; Li16], most of them focused on monostatic configuration, the radar cross section (RCS) of this type of small drones varies between 0.01 m^2 and 0.1 m^2 , making them challenging targets, but of great interest due to the threats they may pose to high-speed railway networks.



(a) DJI Phantom 4 drone used as a co-operative target



(b) Flight trajectories

Figure 4.4: Cooperative target and conducted flights during the measurements.

4.2 Scenario analysis

Taking into account the measurement scenario and the parameters of the transmitter, the SDR receiver and the cooperative target, shown in Table 4.2, an estimation of the target signal-to-noise ratio (SNR) and of the ratio between the target power and the direct signal power was performed. Figure 4.5 shows the results for the LTE channel at 930 MHz, while Figure 4.6 shows the results for the channel at 1870 MHz considering a single receiving channel (i.e. without the application of digital beamforming techniques) and assuming a free space propagation model. To consider the effect of the antenna sidelobes in elevation, the transmitter and receiver antenna patterns have been modelled considering a sinc-like pattern based on the specified -3 dB-beamwidth of the antennas, resulting in the ripple observed in the results at short target ranges. Besides, the SNR of the direct signal is estimated to be 53.5 dB for the 930 MHz channel with 10 MHz bandwidth and 44.5 dB for the 1870 MHz

Table 4.2: Transmitter, receiver and target parameters used in the estimation of target SNR, target-to-direct signal power ratio and direct signal SNR.

<i>Parameter</i>		<i>Value</i>	
Center frequency		930.1 MHz	1869.9 MHz
Bandwidth		10 MHz	20 MHz
Integration time		0.1 s	0.2 s
Tx	EIRP	40 dBm	
	Elevation -3 dB-beamwidth	10°	
	Antenna tilt	0°	
Rx	Receiving antenna gain	5 dBi	
	Elevation -3 dB-beamwidth	25°	
	Antenna tilt	0°	
	Figure noise	5 dB	
	Target RCS	0.05 m ²	
	Additional losses	3 dB	

channel with 20 MHz bandwidth, which is well above the typical SNR requirements to be used as the reference signal [Cui15] without the need for reconstruction, as long as it does not present significant multipath components.

The difference in the target SNR between the 40 m-altitude flights and the 100 m-altitude flights is mainly due to the assumed elevation radiation pattern of the transmitting and receiving antennas. Besides, the variations that occur when the target is at a close range from the receiver (lower than 200 m) are due to the reception of the target scattered signals through the sidelobes of the receiving antenna.

These results show that for a target detection limited by noise, the estimated maximum detection range for the considered target (i.e. RCS of 0.05 m²) is close to 1000 m for both frequency channels when using an integration time of 0.1 s or 0.2 s, respectively. The required SNR of 18.3 dB has been set for a detection probability of 90%, a false alarm probability of 10⁻³, a Swerling 1 target model and a Cell Averaging Constant False Alarm Ratio (CA-CFAR) detection algorithm with 72 reference cells [Ric14].

However, when analysing the ratio between the direct signal power and the target scattered signal power, this ratio is observed to be in absolute value above the receiver dynamic range for ranges from the receiver above 550 m when the drone is flying at 40 m altitude and at any distance when the drone is flying at 100 m. Therefore, if the considered estimation models fit

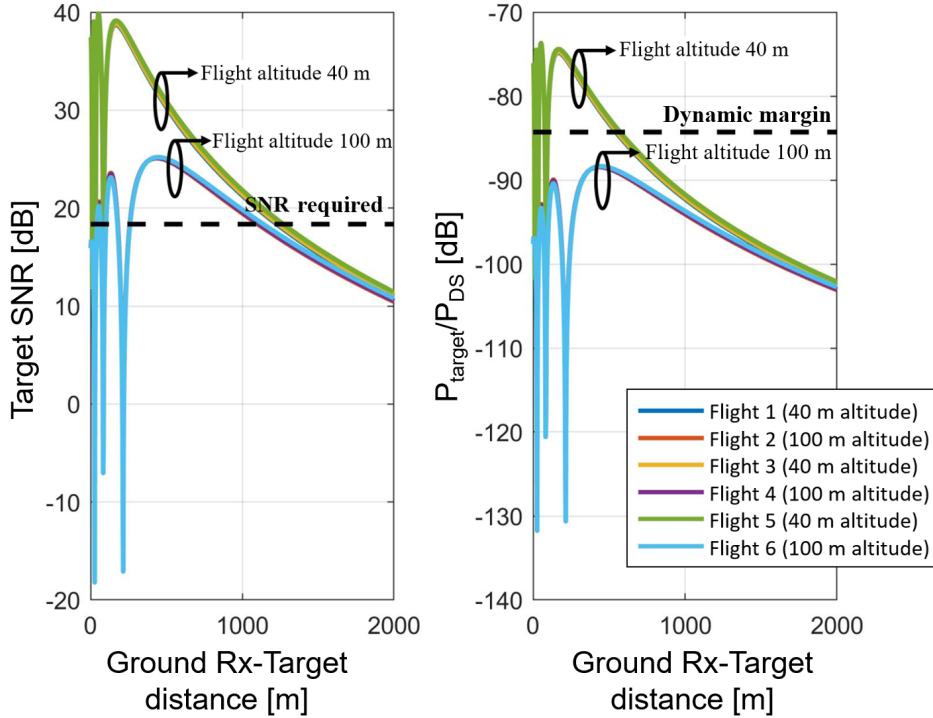


Figure 4.5: Estimated target SNR (left) and target-to-direct signal power ratio (right) for the LTE channel centered at 930 MHz with 10 MHz bandwidth.

In the real situation, the target detection might be mainly limited by the dynamic range of the receiver used. This result highlights the need to use receivers with a large dynamic range, being one of the main limitations of passive radars, especially in those architectures based on a single antenna to receive both the reference signal (direct signal) and the target reflected signals. To address this limitation, the use of directional antennas with radiation patterns that allow a certain cancellation in the direction of the transmitter of opportunity is usually considered, resulting in a blind zone for target detection. It should be noted that the use of digital beamforming techniques does not overcome this limitation, since the beamforming is performed by combining the digitised signals received by each antenna channel.

The coherent integration times to determine the target SNR, which have been also used for the processing of the performed measurements, have been set to 0.1 s for the 930 MHz channel and to 0.2 s for the 1870 MHz channel in order to ensure a phase and amplitude stability of the receiver during the integration time [Sla23] and to avoid significant target range migration effects. The resolution of the passive radar system in a quasi-monostatic

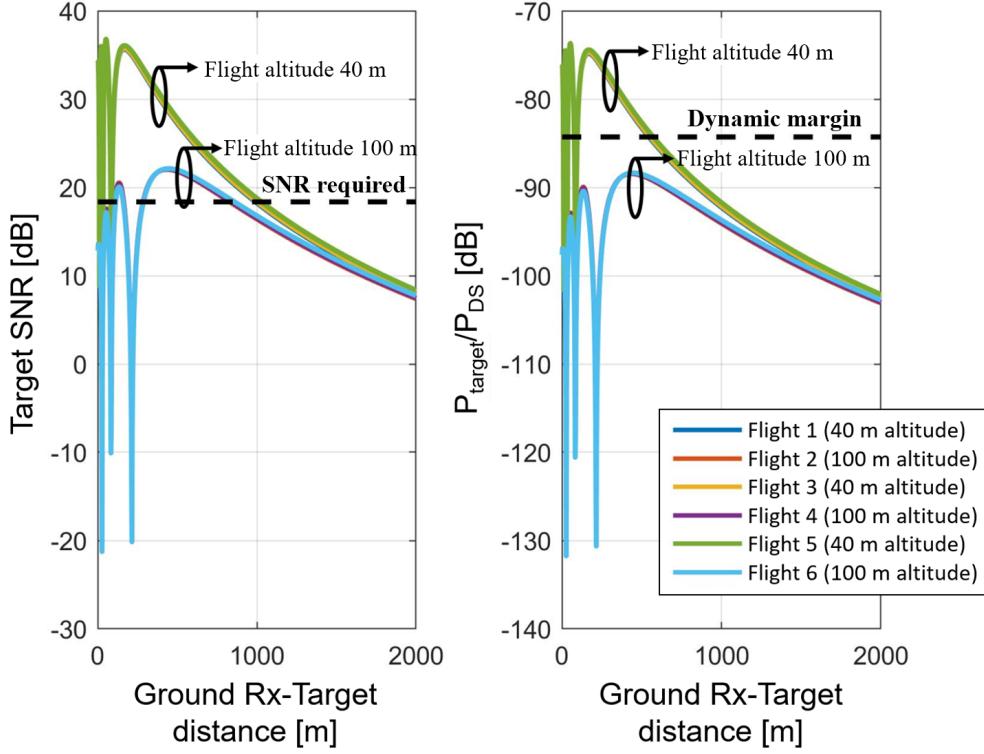


Figure 4.6: Estimated target SNR (left) and target-to-direct signal power ratio (right) for the LTE channel centered at 1870 MHz with 20 MHz bandwidth.

configuration, similar to the test scenario where the bistatic angle (Tx-Target-Rx) is close to zero, is approximately given by:

$$10 \text{ MHz bandwidth} \rightarrow \delta R = \frac{c}{2B} = 15 \text{ m} \quad (4.1)$$

$$20 \text{ MHz bandwidth} \rightarrow \delta R = \frac{c}{2B} = 7.5 \text{ m} \quad (4.2)$$

where c is the speed of light and B is the signal bandwidth. Therefore, the maximum integration time to prevent the target from crossing more than one range resolution cell at a linear velocity of 20 m/s in the radial direction is 0.75 s for a 10 MHz bandwidth and 0.375 s for a 20 MHz bandwidth. Increasing the integration time beyond this value would imply the need to apply motion compensation techniques in which some target dynamics must be assumed, increasing the complexity of the signal processing, especially when considering manoeuvrable targets such as drones.

Based on the geometry of the measurement scenario, Figure 4.7 shows the bistatic range, the Doppler frequency of the target (assuming a target speed of 20 m/s away from the receiver), and the bistatic angle as a function of the ground distance between the target and the receiver considering the different radial flights from the receiver at 40 m and 100 m altitudes, previously described.

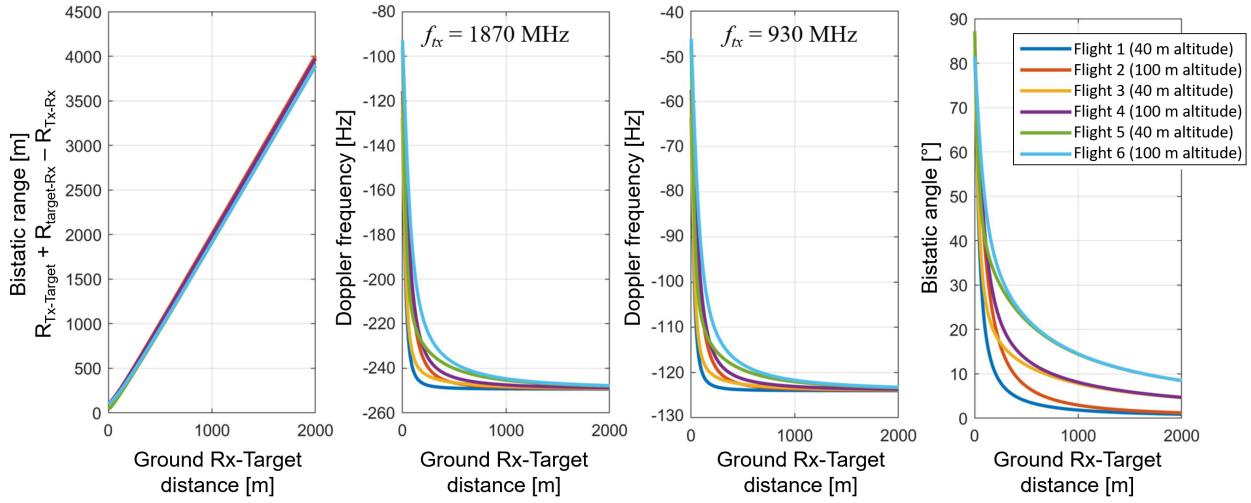


Figure 4.7: Analysis of the bistatic geometry: Bistatic range, Doppler frequency (assuming a target speed of 20 m/s away from the receiver) and bistatic angle as a function of the ground distance between the target and the receiver for the considered flight trajectories at two heights (40 and 100 m).

4.3 Received signal analysis

A time and frequency domain analysis of the captured signals with the four coherent channels was firstly performed. Figure 4.8 represents the digitised IQ signal in channel 1 and the spectrum for the four channels of a 100 ms capture for the channel centered at 930.1 MHz with a 10 MHz-bandwidth. As shown in this exemplary acquisition interval, the amplitude of the signals for this frequency channel was relatively uniform throughout the measurements. Therefore a mostly constant and high network load with user data transmission was observed in this channel, which reduces the level of ambiguities in range and Doppler due to pilot and synchronization signals when compared to the main lobe of the ambiguity function. Besides, the total transmitted power of the base station is expected to be higher when user data is

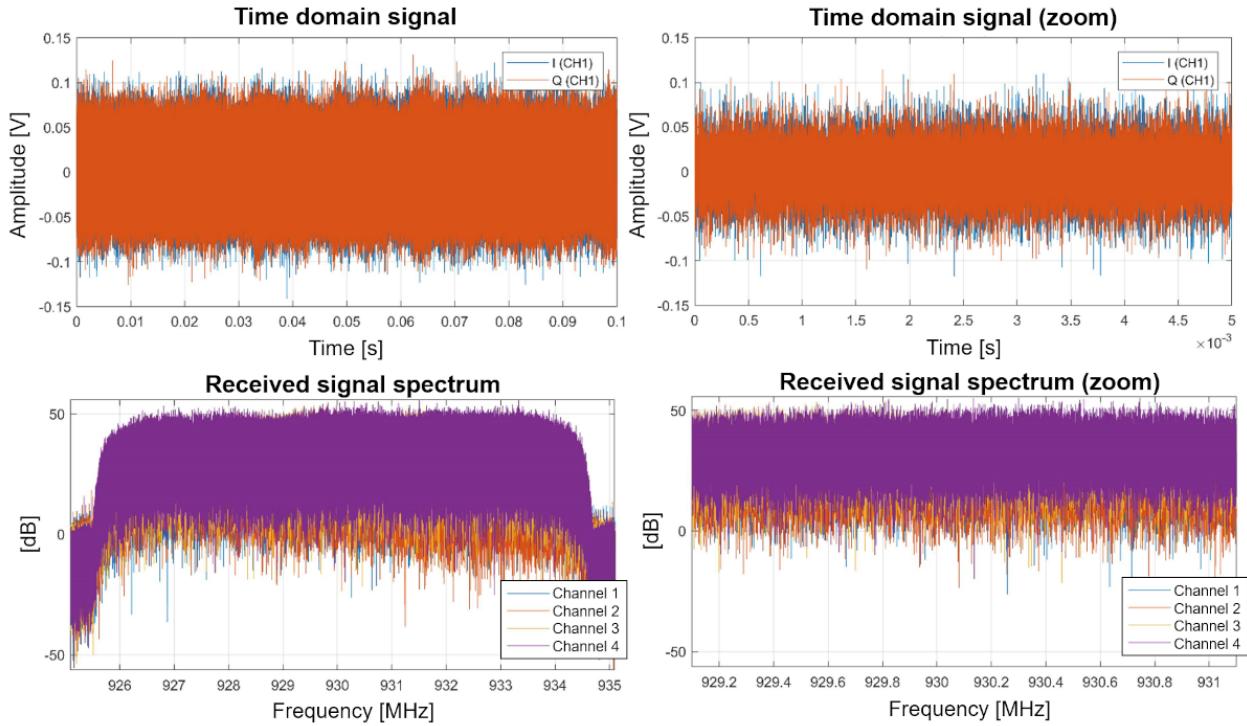


Figure 4.8: Received IQ signal on channel 1 (top) and spectra of the received signals on the four channels (bottom) for a 100 ms acquisition of an LTE channel centered at 930.1 MHz with 10 MHz bandwidth.

being transmitted than when most of the OFDM resource blocks are not used, improving the target SNR for the same coherent integration time.

Figure 4.9 represents the digitised IQ signal on channel 1 and the spectrum for the four channels of a 200 ms capture for the channel centered at 1869.9 MHz with a 20 MHz-bandwidth. During the measurement, low user data transmission was observed in this channel and the acquired signals were composed mainly by the pilots and synchronization signals defined in the LTE standard (i.e. those considered "always on" signals). This suggests that the averaged transmitted power is lower because the OFDM grid is not fully loaded, also limiting the effective integration time when applying the passive radar cross-correlation processing.

In addition, a higher spectrum level variability is observed across the bandwidth, which may be due to a higher impact of multipath. In the zoomed spectrum for the central 2 MHz of the considered LTE channel, peaks due to the OFDM subcarriers associated with the pilot signals used in LTE can be observed. Although the channels were configured to share the same local oscillator, a frequency shift in channel 1 was observed possibly due to some hardware

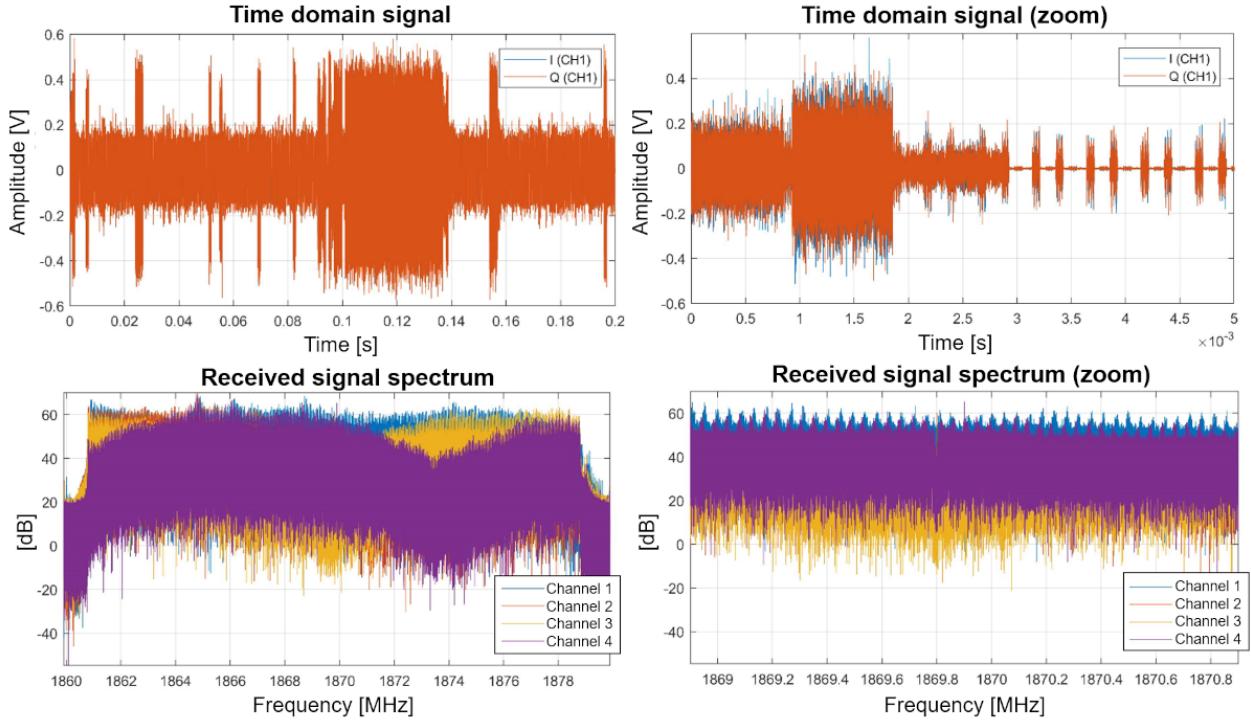


Figure 4.9: Received IQ signal on channel 1 (top) and spectra of the received signals on the four channels (bottom) for a 200 ms acquisition of an LTE channel centered at 1869.9 MHz with 20 MHz bandwidth.

problem of the SDR device. Therefore, in order to apply digital beamforming techniques that combine all four spatial channels, for this acquisition, a frequency shift compensation for the channel 1 would be necessary and the coherence between channels should be verified after this compensation. For this reason, in the measurements associated with the channel centered at 1869.9 MHz only channels 2, 3 and 4 were considered to analyse the application of beamfoming techniques, limiting the achievable array gain and the angular resolution when compared with the other acquisition.

Figure 4.10 shows the histograms of the digitised voltage values for the considered acquisitions for the frequency channels at 930 MHz and 1870 MHz. Since no automatic gain control was implemented, the received signals do not span the full dynamic range of the analog-to-digital converters (± 1 V), actually decreasing the effective dynamic range, which as shown before may limit target detection.

During time intervals when no user data is being transmitted, the amplitude and, therefore, the averaged power of the received signals is lower, since the base station only transmits

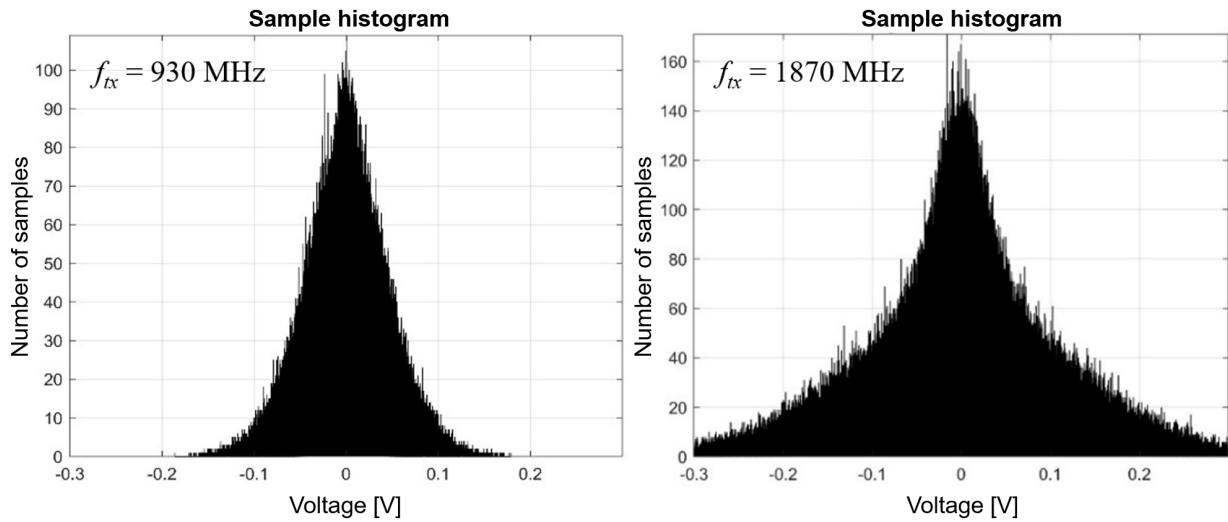


Figure 4.10: Histograms of the digitised voltage values for the considered acquisitions intervals of the frequency channels at 930 MHz and 1870 MHz.

pilots, synchronization and, possibly, broadcast signals. In these time intervals, the target SNR would also be reduced.

The SNR of the direct signals relative to the noise floor of the spectrum is estimated to be 40 dB for the 930 MHz channel and 35 dB for the 1870 MHz channel. These values are considerably lower than the previously estimated SNRs, possibly due to a lower transmitted power and higher propagation losses relative to the free space propagation model, but high enough to avoid the need for signal reconstruction.

4.4 Target detection results

The results of the signal processing for target detection based on the computation of the range-Doppler maps by means of the cross-correlation (in time and Doppler frequency) between the reference signal and the surveillance signal are analysed below. Reconstruction of the transmitted signal (by demodulation and subsequent remodulation) has not been considered because of the high estimated SNR of the received direct signals and the algorithmic complexity involved. It is important to note that in the case that the base stations use spatial multiplexing, i.e. conforming different antenna beams, which is most widely used in 5G [Cri23a], the target

and passive radar receiver need to be illuminated by the same beam in order to get the appropriate reference signal illuminating the target.

Figure 4.11 represents range-Doppler maps obtained from the autocorrelation of signals received by channel 1 while the drone was approaching at an altitude of 40 m on a radial direction of 80° with respect to North (i.e. flight 1). These results are examples of range-Doppler maps obtained for a single-antenna architecture without reconstructing the transmitted signal. As described before, a CPI of 0.1 s was used for the acquisition at 930 MHz and a CPI of 0.2 s for the acquisition at 1870 MHz. Note that the measurements at the different frequency channels were not simultaneous but presented a similar bistatic geometry with the drone approaching from an approximate distance of 300 m to the receiver at the start of the acquisitions.

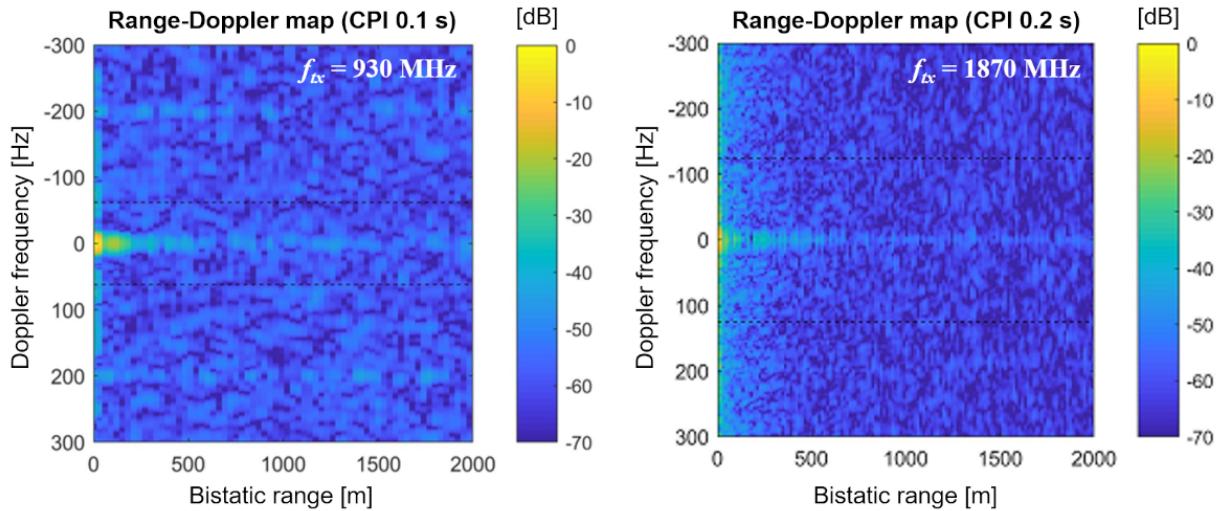


Figure 4.11: Range-Doppler maps (normalized to maximum value) computed as the autocorrelation of the signals recorded by channel 1 for a recording of the 930 MHz LTE channel (left) and a recording of the 1870 MHz LTE channel (right) during a flight of the drone at an altitude of 40 m on a radial direction of 80° (with respect to North), i.e. flight 1, towards the receiver.

The signal recorded for the 1870 MHz channel, although it leads to a higher range resolution due to its higher bandwidth, gives rise to higher levels of ambiguities in range and Doppler and a variable ambiguity function, as shown in Figure 4.12, due to the predominant transmission of pilot and synchronization signals, in contrast to the signal recorded for the 930 MHz channel, which showed a higher and continuous payload of user data. However, the high levels of direct

signal interference (DSI) and multipaths at close ranges prevent the detection of the target in both cases, which is covered by the sidelobes of the ambiguity function of the considered signals. Moreover, direct signal interference and multipath cancellation techniques cannot be applied considering a single-antenna architecture without reference signal reconstruction because the received reference signal contains the target scattered signals, which would also be cancelled. Therefore, a single-antenna architecture without reconstruction of the transmitted signal is not feasible for LTE-based passive radars given the typical levels of DSI and multipath components.

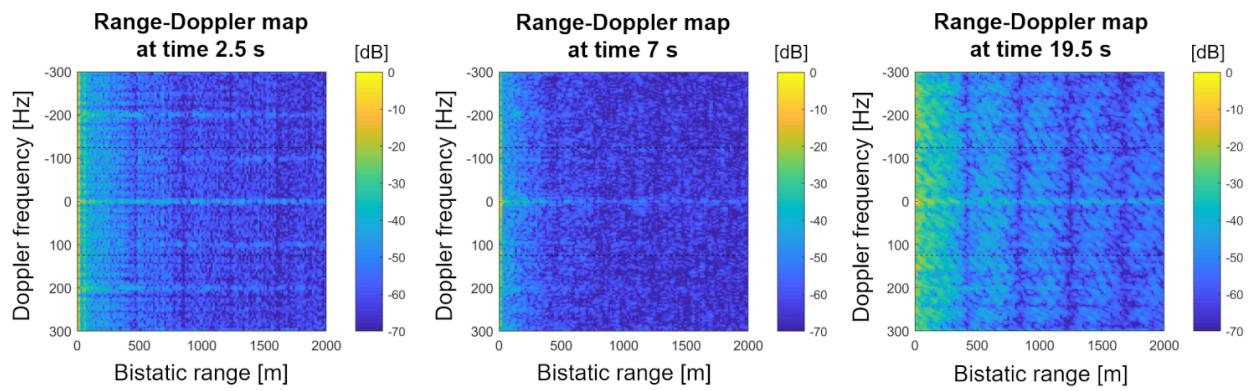


Figure 4.12: Range-Doppler maps (normalized to maximum value) for several time intervals computed as the autocorrelation of the signals recorded by channel 1 for the 1870 MHz LTE channel, showing the ambiguity function variability depending on the content and user payload of the transmitted LTE signal.

Therefore, taking into account the previous analysis and architecture design based on the use of SDR receivers with multiple coherent channels, the application of digital beamforming techniques was experimentally evaluated. However, in order to avoid the complexity of calibrating the deployed array, including the receiving elements and channels, the relative position between elements, and the orientation and position of the array in a global coordinate reference system (i.e. World Geodetic System 84, –WGS84–), an adaptive digital beamforming approach was proposed and validated.

Figure 4.13 shows the proposed signal processing based on extracting a reference signal by maximizing the output power of a beamformer defined by the weight vector \mathbf{w}_{\max} with four input channels, and a surveillance signal by minimizing the output power of a beamformer defined by the weight vector \mathbf{w}_{\min} with the same four input channels, subject to the sum of the

squares of the beamformer weight magnitudes being 1. Besides, based on the obtained reference and surveillance signals, an Extensive Cancellation Algorithm (ECA) [Col09] to further cancel the DSI and multipath components in the surveillance signal before the range-Doppler map computation is performed.

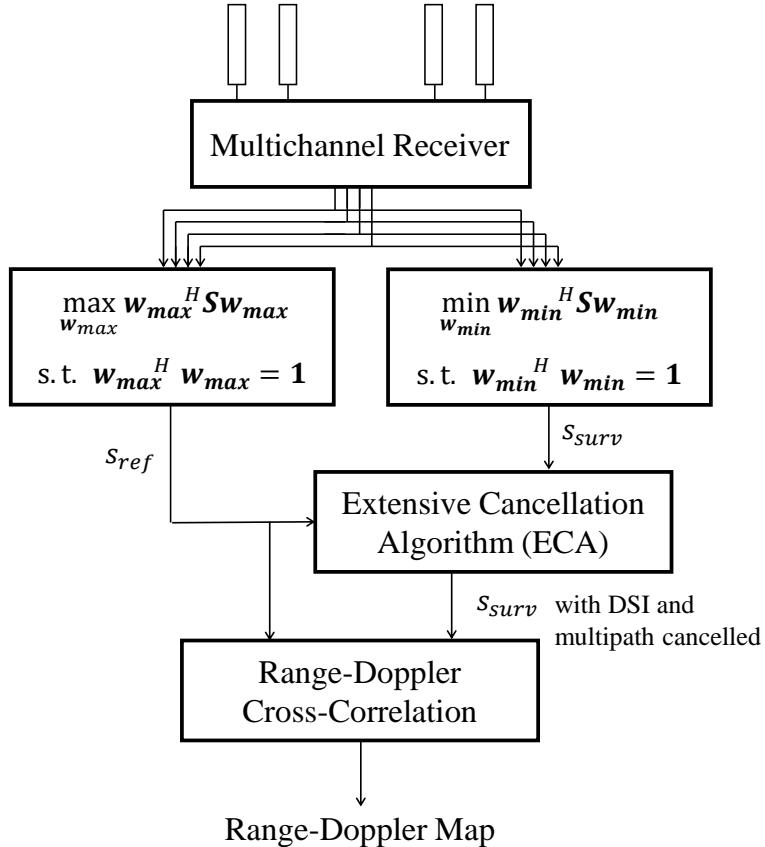


Figure 4.13: Proposed signal processing for the computation of the range-Doppler maps based on adaptive digital beamforming ($\mathbf{w}_{\max}, \mathbf{w}_{\min}$ = beamformer weight vectors, \mathbf{S} = sample covariance matrix between the received signals in the different channels, s_{ref} = reference signal, s_{surv} = surveillance signal).

As already said, this adaptive signal processing does not require the calibration of the phase differences between the receiver channels depending on the Direction of Arrival (DoA) of the signals, but makes the assumptions that the direct signal is the component received with the highest power level, which is the common situation when the LTE base station is in Line of Sight (LOS), and that some multipath components are received with higher power level than the target scattered signals, to avoid the cancellation of the target in the surveillance signal when applying the minimization algorithm. However, as discussed in the previous chapter, the beamfoming process results in blind sectors with decreased target detection

capability in the direction of the direct signal and possible strong multipaths and, in the case of undersampled arrays, associated ambiguous (i.e. grating lobes) directions depending on the array configuration.

Figure 4.14 represents the range-Doppler maps obtained by applying the proposed digital beamforming approach with and without the DSI cancellation step using the ECA algorithm for the same recording intervals of Figure 4.11 of the two considered LTE bands. For the 930 MHz channel, all four channels have been considered, while for the 1870 MHz channel, three channels (channels 2-4) have been considered due to the coherence problem discussed above. During these measurements, the drone followed a radial trajectory with an 80° direction with respect to North at a height of 40 m and an approximate speed of 20 m/s towards the receiver, i.e. an estimated Doppler frequency of 124 Hz for the channel at 930 MHz and of 249 Hz for the channel at 1870 MHz, given the pseudo-monostatic configuration for flight 1.

As can be observed, for the recording of the 930 MHz-LTE channel, the proposed adaptive digital beamforming allows to partially cancel the direct signal in the surveillance channel, which leads to a decrease in the noise floor level enabling the detection of the cooperative target (drone) at about 250 m from the receiver (i.e. 500 m bistatic range) and of a closer moving target present in the scenario (vehicle) during that measurement. However, the residual of the DSI and static clutter (multipath) limits the target SNR, which can be improved by applying the ECA algorithm, further reducing the noise floor level and enhancing target detectability.

Nevertheless, the applied processing does not allow the detection of the cooperative target for the measurements at the 1870 MHz-LTE channel, mainly due to: (i) the reduced transmitted power for this channel as almost no user payload data was being transmitted, (ii) higher propagation losses associated to a higher transmitting frequency, and (iii) higher level of sidelobes in Doppler due to the signal structure and caused by DSI and multipath components, which result in a high level of the noise floor despite the application of the beamforming and ECA steps. These ambiguities are mainly due to the fact that for the recordings of the 1870 MHz-LTE channels, the pilot and synchronization signal components were predominant in the received signal, with low user data payload transmission. In these cases, reconstructing the transmitted pilot and synchronization signals would be necessary in

order to apply mismatched filters to reduce the level of secondary lobes, e.g. the reciprocal filter, considerably increasing the complexity of the signal processing. This result highlights one of the main limitations of not having control over the transmitter and the importance of properly selecting the transmission channel and appropriate signal intervals with data payload [Mak22] to apply the passive radar signal processing.

Figure 4.15 represents the sequence of range-Doppler maps obtained for the 930 MHz-LTE channel measurements during the drone flight, where the detections of the drone and the opportunistic moving vehicle present in the scenario can be observed. The variability of the drone SNR, possibly due to RCS fluctuations or signal propagation mechanisms (e.g. two-ray ground-reflection propagation [dQue19]), results in some range-Doppler maps in which the drone is not detected, although the overall probability of detection is high and suitable to apply target tracking algorithms for ranges up to 250 m. Therefore, these results demonstrate the feasibility of detecting small drones at close range using a LTE-based passive radar implemented with a multi-channel receiver and digital beamfoming techniques.

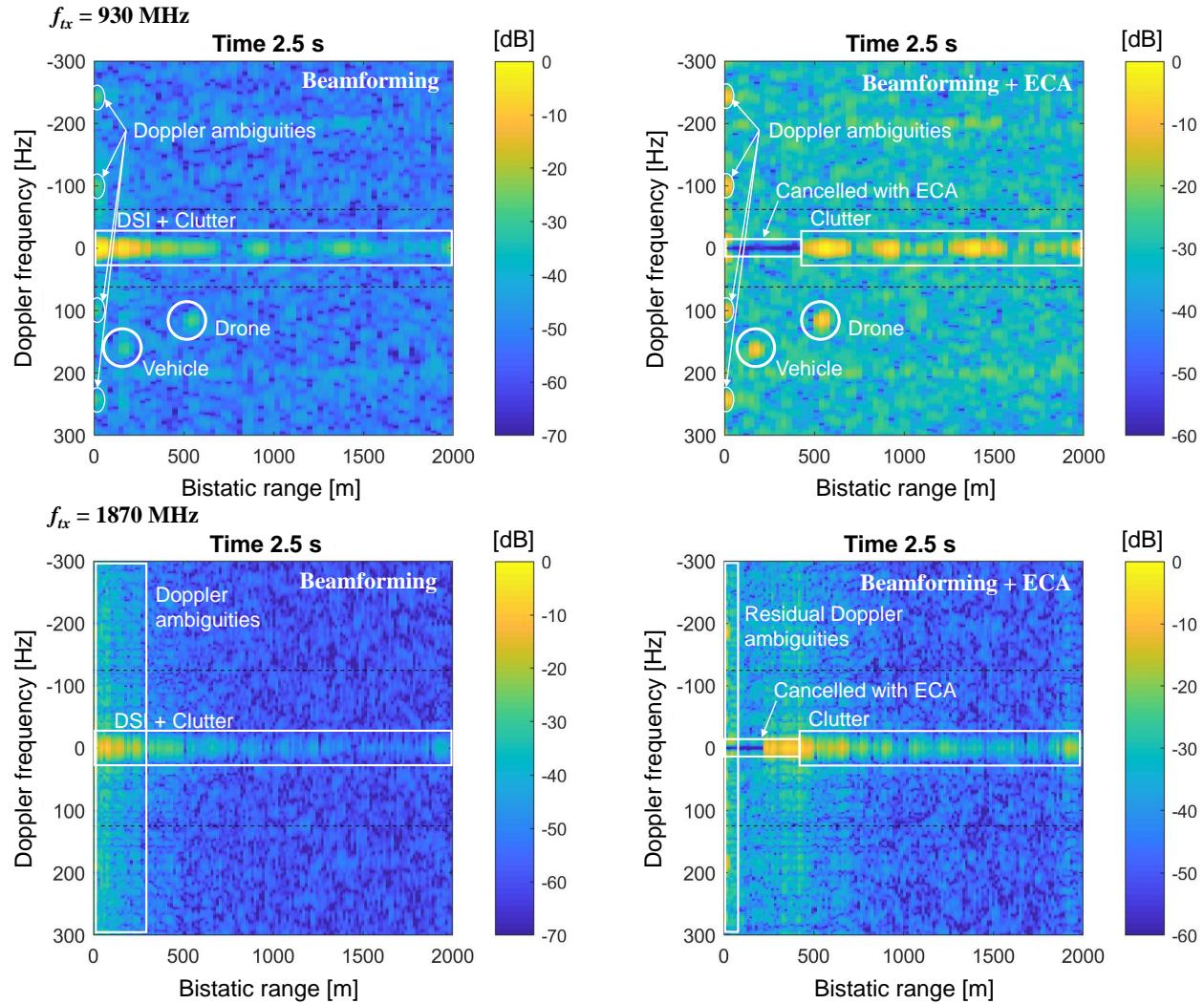


Figure 4.14: Range-Doppler maps applying the proposed adaptive digital beamforming (left) and both the digital beamforming and ECA (right) for a recording of the 930 MHz-LTE channel (top) and a recording of the 1870 MHz-LTE channel (bottom) during a flight of the drone at an altitude of 40 m on a radial direction of 80° (with respect to North) with 20 m/s velocity, i.e. flight 1, towards the receiver. Dashed black lines mark the Doppler frequency associated to a velocity of ± 10 m/s for the pseudo-monostatic configuration (i.e. bistatic angle equal to 0°). Note that the measurements at the different frequency channels were not simultaneous but presented a similar bistatic geometry with the drone approaching from an approximate distance of 300 m to the receiver at the start of the acquisitions (Time 0 s).

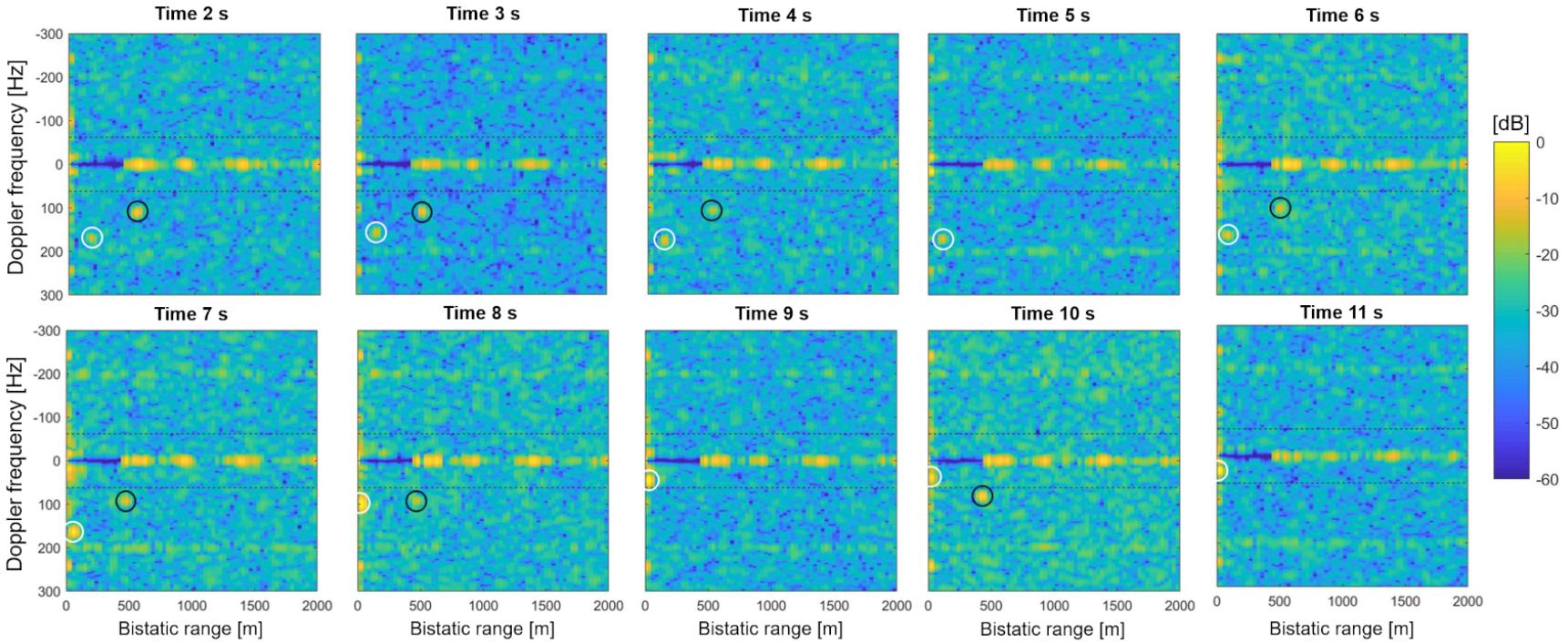


Figure 4.15: Sequence of range-Doppler maps obtained for the 930 MHz-LTE channel measurements during a flight of the drone at an altitude of 40 m on a radial direction of 80° (with respect to North) with 20 m/s velocity, i.e. flight 1, towards the receiver. Black circles mark the peaks associated to the cooperative drone, while white circle mark the peaks associated to the opportunistic moving vehicle in the measurement scenario. Dashed black lines mark the Doppler frequency associated to a velocity of ± 10 m/s for the a pseudo-monostatic configuration (i.e. bistatic angle equal to 0°).

However, in the measurements made when the drone was flying in radial directions of 100° and 120° with respect to North (flights 3-6), the target was not detected despite applying the proposed signal processing based on digital beamforming and DSI and clutter cancellation. The main reason of this is the non-suitable geometry of these measurements scenarios, shown in Figure 4.16, while using a linear array, since the direction of flights 5 and 6 is equivalent to the direction the LTE transmitter and the direction of the flights 3 and 4 only differs by 20° . Therefore, the considered adaptive beamforming technique that minimizes the total power in the surveillance signal may also significantly cancel the target signal, preventing its detection. It should be noted that the use of a limited number of receiving spatial channels reduces the angular resolution and the capability to spatially separate the receiving signals, since the digitally synthesized antenna patterns have wide main beams.

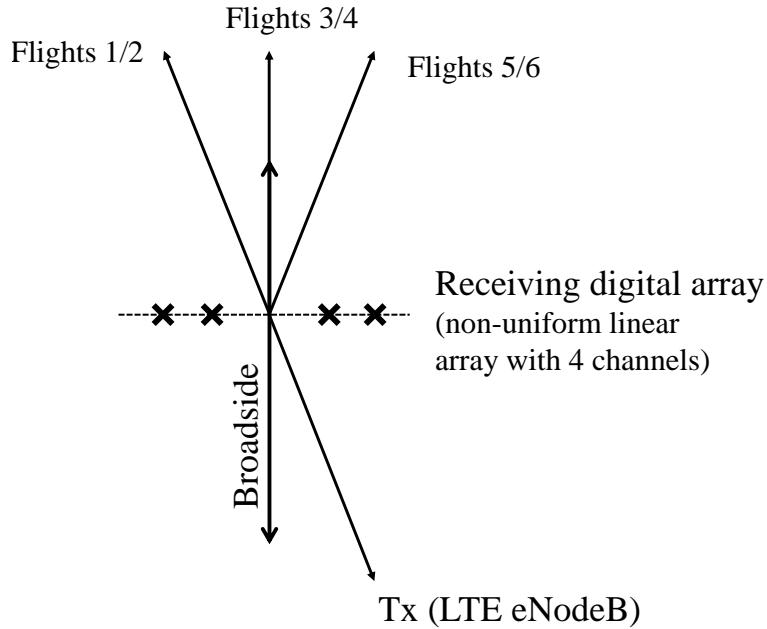


Figure 4.16: System geometry showing the directions of arrival of the drone signals for flights 1-6 during the measurement campaign and the direction of arrival of the direct signal from the LTE transmitter (Tx).

Although the use of the LTE downlink signal has been validated for the detection of close targets using multichannel COTS SDR devices and applying adaptive digital beamforming techniques, these results highlight the need to deploy the array with a suitable geometry with respect to the area of interest or distributed receiver networks to avoid blind sectors. Besides, the detection performance of the proposed system will benefit from the increase in the number

of coherent channels due to the progress of SDR technology [Mol22], the optimisation of the array geometry [del17] and the incorporation of Forward Scattering Radar (FSR) modes [Col21; Col20; Bla23a; Raj16] that allow the detection of targets that cross the baseline between the transmitter and the receiver, forming a kind of electronic fence.

4.5 Conclusions

The results of the measurement campaign have validated the feasibility of detecting small drones at close range using the proposed passive radar architecture based on the use of LTE downlink signals as illumination of opportunity, multi-channel COTS SDR receivers and adaptive digital beamforming techniques that do not required the calibration of the array. The main advantage of this system lies in its reduced cost compared to active radars, thanks to the use of already deployed communications infrastructure as illuminators of opportunity and the increasingly lower cost and better performing commercial multi-channel SDR devices as receiver nodes. In addition, this system does not require frequency allocation and operates in all light and weather conditions. Therefore, it is a system with the potential to be deployed along high-speed railway networks or other critical infrastructures using multiple receiver nodes to perform surveillance and to cope with the detection of small drone-based threats. Besides, the wide instantaneous field of view (FOV) of the system makes it particularly suitable for carrying out target detection tasks, integrated with narrow FOV optical sensors that perform detection confirmation and target classification. This integrated architecture also addresses the reduced range resolution of the LTE-based passive radar, which may hinder the discrimination of close targets with the same speed (e.g. in drone swarms), by separating the targets and classifying the threat in the optical domain.

However, certain limitations have been identified that need further analysis in order to improve the performance and robustness of the proposed system. These limitations are mainly related to the required dynamic range of the receivers, the effects of the network load on the performance of the radar system and the existence of blind sectors when applying digital beamforming techniques.

The reception of the direct signal and target scattered signals using omnidirectional antennas results in very demanding requirements on the dynamic range of the receivers which can impose a stronger limitation of the system detection range than the thermal noise of the receivers, especially when the considered base station is located close to the passive radar receiver. To address this limitation, deployment optimisation is possible using link budgets based on propagation models. In addition, a complementary approach is the use of directional antennas pointed towards the surveillance area that partly attenuate the direct signal component, or the use of separate reference (pointed towards the base station) and surveillance (pointed towards the surveillance area of interest) antennas. Besides, signal processing techniques have been presented [Axe03; Che19; Kum20; Sed21] that address the dynamic margin limitation and the detection of weak signals received simultaneously with strong signals, increasing the effective dynamic range of the receivers. Since the analysis of the scenario showed that the detection capabilities for some measurements might be limited by the dynamic margin of the receiver, the application of these techniques might improve the results here presented.

The results of the direct signal analysis and the ambiguities and sidelobes that occur in the range-Doppler maps when pilot and synchronization signals predominantly composed the transmitted signals, which give rise to target masking effects, show that, in operational scenarios, some cooperation from the base station to maintain a certain level of network load, transmitting idle data, or forcing the transmission of user data by connecting to the base station might be necessary. In order to achieve a more robust passive radar operation using only opportunistic transmissions (i.e. without cooperation from the base station or forcing data transmission), adaptive selection methods of the base station, frequency channel and suitable signal intervals for target detection can be applied if, given the dense deployment of mobile communication systems, several base stations and channels are available.

The occurrence of blind sectors due to the application of digital beamforming techniques can be addressed by increasing the number of digital channels (i.e. number of digital array elements), by deploying distributed passive radar sensor network to cover the whole area of interest, or by applying FSR approaches. A larger number of array elements and, therefore,

of degrees of freedom, in addition to increasing the array gain, improves the capability to spatially separate the received signals, the adaptability of the system to cancel interference signals and clutter, and the accuracy of the DOA estimation techniques. In addition, sensor networks provide spatial diversity, improving the detectability of targets with fluctuating RCS, and enable the application of multistatic techniques such as multilateration algorithms to perform three-dimensional target localisation and tracking. Besides, the application of FSR techniques based on LTE signals would allow the detection of targets crossing the baseline between the base station and the receiver, expanding the considered passive radar coverage. The FSR configuration also tends to results in higher target RCS, even for stealth and low-RCS targets, improving their detectability. Therefore, its experimental analysis is considered of special interest as future work in the context of surveillance applications for critical infrastructures such as high-speed railway networks.

Besides, further validation of the system in more complex and urban operational scenarios is required, where multipath and line-of-sight blocking effects are typically more significant than in semi-urban or rural areas as the one considered in the presented proof of concept. In fact, although the maximum detection range that has been experimentally achieved for drone detection is at least one order of magnitude lower than the typical range of commercial active radars, the exploitation of illuminators of opportunity (i.e. no need to transmit signals) and its lower cost make the LTE-based passive radar system potentially more suitable for deploying sensor networks that may overcome the line-of-sight limitations of urban environments.

