Tampere University

WENBO WANG

Novel Models and Algorithms Paving the Road towards RF Convergence

Tampere University Dissertations 684

Tampere University Dissertations 684

WENBO WANG

Novel Models and Algorithms Paving the Road towards RF Convergence

ACADEMIC DISSERTATION
To be presented, with the permission of
the Faculty of Information Technology and Communication Sciences
of Tampere University,
for public discussion in the Auditorium S2
of the Sähkötalo building, Korkeakoulunkatu 1, Tampere,
on the 9th December 2022, at 12 o'clock.

ACADEMIC DISSERTATION
Tampere University, Faculty of Information Technology and Communication Sciences
Finland

Responsible supervisor and Custos	Professor Elena Simona Lohan Tampere University Finland	
Supervisor	Professor Mikko Valkama Tampere University Finland	
Pre-examiners	Associate Professor Rui Dinis Universidade Nova de Lisboa Portugal	Professor Mohammed Elmusrati University of Vaasa Finland
Opponents	Associate Professor Rui Dinis Universidade Nova de Lisboa Portugal	Associate Professor Troels Bundgaard Sørensen Aalborg University Denmark

The originality of this thesis has been checked using the Turnitin OriginalityCheck service.

Cover design: Roihu Inc.

ISBN 978-952-03-2599-2 (print)
ISBN 978-952-03-2600-5 (pdf)
ISSN 2489-9860 (print)
ISSN 2490-0028 (pdf)
http://urn.fi/URN:ISBN:978-952-03-2600-5

HIILINEUTRAALI PAINOTUOTE
ClimateCalc CC-000025/FI
PunaMusta Printing

Carbon dioxide emissions from printing Tampere University dissertations have been compensated.

PunaMusta Oy – Yliopistopaino
Joensuu 2022

To my wife, Yining.

To my parents, Mingyan and Hongwei.

For your unconditional love!

PREFACE

It was the cold spring when the research work for the current thesis started, with the fat snowflake in the air I came to Tampere University of Technology, where I previously completed my master degree study. The research work lasted more than four years, from 2018 to 2022, at the Unit of Electrical Engineering, Tampere University (former Tampere University of Technology), Finland. During the study, several sources of funds financially supported the research, here I would like to take this opportunity to show my gratitude. These funds are from the Academy of Finland, the SESAR Joint Undertaking, ESA, Nokia Foundation, Pekka Ahonen Fund and the Finnish Foundation for Technology Promotion.

To begin with, I would like to express my deepest gratitude to my supervisor, Prof. Simona Lohan, for her excellent supervision and infinite patience. If the reader is currently looking for a PhD position, I recommend her as your supervisor. Besides, I wish to thank Prof. Mikko Valkama, for his support and guidance during the study.

I could not finish this journey without my dear companions. My colleagues, Rubén, Bo Sun, Philipp, Jukka, Islam and Niloofar, were fighting against the research questions with me. Their passion and humour inspired me largely for the publications that made this thesis. In addition, I appreciate the discussions and collaborations with Dr. Bo Tan, for many papers we wrote together. My gratitude extends to Emanuele and Wahyudin in GMV NSL, though we have not published anything yet, the discussions were always full of joy.

My sincere gratitude goes to my parents, Mingyan and Hongwei. I know the past few years were not easy for them with sudden illness situations, but they kept going. This reminds me the lines from the movie 'The Lord of the Rings', as I quote here,

"I wish it need not have happened in my time," said Frodo.
"So do I," said Gandalf, "and so do all who live to see such times.

> *But that is not for them to decide. All we have to decide is what to do with the time that is given us."*
>
> – J. R. R. Tolkien, The Fellowship of the Ring

Last, I would like to give a big hug to my wife, Yining. No words could ever express my gratitude to you, for your kindness, tolerance and patience. The COVID-19 time is tough, especially for a PhD student, but you are like a light in the end of a tunnel, which guides me and accompanies me through the whole journey. I love you!

Tampere, September 2022

Wenbo Wang

ABSTRACT

After decades of rapid evolution in electronics and signal processing, the technologies in communications, positioning, and sensing have achieved considerable progress. Our daily lives are fundamentally changed and substantially defined by the advancement in these technologies. However, the trend is challenged by a well-established fact that the spectrum resources, like other natural resources, are gradually becoming scarce. This thesis carries out research in the field of RF convergence, which is regarded as a mean to intelligently exploit spectrum resources, e.g., by finding novel methods of optimising and sharing tasks between communication, positioning, and sensing.

The work has been done to closely explore opportunities for supporting the RF convergence. As a supplement for the electromagnetic waves propagation near the ground, ground-to-air channel models are first proposed and analysed, by incorporating the atmospheric effects when the altitude of aerial users is higher than 300 m. The status quos of techniques in communications, positioning, and sensing are separately reviewed, and our newly developments in each field are briefly introduced. For instance, we study the MIMO techniques for interference mitigation on aerial users; we construct the reflected echoes, i.e., the radar receiving, for the joint sensing and communications system. The availability of GNSS signals is of vital importance to the GNSS-enabled services, particularly the life-critical applications. To enhance the resilience of GNSS receivers, the RF fingerprinting based anti-spoofing techniques are also proposed and discussed. Such a guarantee on GNSS and ubiquitous GNSS services drive the utilisation of location information, also needed for communications, hence the proposal of a location-based beamforming algorithm. The superposition coding scheme, as an attempt of the waveform design, is also brought up for the joint sensing and communications.

The RF convergence will come with many facets: the joint sensing and communications promotes an efficient use of frequency spectrum; the positioning-aided com-

munications encourage the cooperation between systems; the availability of robust global positioning systems benefits the applications relying on the GNSS service.

CONTENTS

Preface iii

Abstract v

List of Figures x

List of Tables xv

Abbreviations xvii

1 Introduction 1

1.1 History and status quo 1

1.2 Aim and scope 4

1.3 Research questions and methodology 4

1.4 Contributions and organisation 5

2 Wireless channel models 9

2.1 Channel models 9

2.1.1 Free-space loss 10

2.1.2 Log-distance path loss model 11

2.1.3 3GPP channel models 12

2.1.4 Comparisons 20

2.2 Atmospheric effects 23

2.2.1 Gas absorption 23

2.2.2 Clouds and fog 25

2.2.3 Rain 26

2.2.4 Comparisons 27

2.3 Overall path loss model 30
2.4 Discussion 34

3 Solutions in communications, positioning, and sensing 35
3.1 Wireless communications 35
3.1.1 Use cases in communications 36
3.1.2 Addressed challenges in communications 39
3.2 Wireless positioning 46
3.2.1 GNSS-based positioning 46
3.2.2 Other modern positioning methods 47
3.2.3 Challenges in positioning 47
3.2.4 Proposed solutions 48
3.3 Wireless sensing 49
3.3.1 Signal model 49
3.3.2 Matched filter 50
3.3.3 Detection rate and false alarm rate 52
3.3.4 Parameter estimation 53
3.4 Discussion 54

4 Physical layer security in GNSS 57
4.1 RF fingerprinting techniques 57
4.2 RF fingerprinting in GNSS 58
4.2.1 Navigation payload 59
4.2.2 Receiver chain 60
4.2.3 Pre-correlation method 61
4.2.4 Post-correlation method 64
4.2.5 Anti-spoofing based PVT solution 65
4.3 Measurements-based testing 66
4.3.1 Measurement campaigns 66
4.3.2 Spoofer identification 69
4.4 Discussion 70

5 Positioning-aided communications 73

5.1 Location-based beamforming 73

5.1.1 Optimisation of URA 75

5.1.2 Comparisons of beamforming techniques 77

5.2 Discussion 78

6 Joint sensing and communications 81

6.1 Superposition coding scheme 82

6.1.1 Signal processing in communications part 83

6.1.2 Signal processing in radar part 84

6.1.3 Optimisation problem 85

6.2 Detection rate comparisons 86

6.3 Discussion 91

7 Conclusion and future directions 93

7.1 The take-away points 93

7.2 The way ahead 98

References 99

Publication 1 115

Publication 2 125

Publication 3 141

Publication 4 149

Publication 5 157

Publication 6 195

Publication 7 207

Publication 8 215

List of Figures

1.1 The illustration of how the thesis is composed and the inter-relationship among publications. 6

1.2 An illustration of contributions from each publication. [P1]-[P8] denotes the publication 1 to publication 8. The abbreviations in the figure are listed here: Industrial Internet of Things (IIoT), Multiple-Input Single-Output (MISO), Multiple-Input Multiple-Output (MIMO), Radio Frequency (RF), Cramér-Rao lower bound (CRLB). 7

2.1 An illustration of path loss, shadowing and fading effects. The path loss is based on free space loss (introduced in Section 2.1.1), the shadowing follows log-normal distribution, the fading follows Rayleigh distribution. 10

2.2 Path loss versus T-R separation distance in LOS and NLOS scenarios. The carrier frequency is 2.1 GHz. 21

2.3 Path loss versus carrier frequency in LOS and NLOS scenarios. 21

2.4 Path loss versus altitude in LOS and NLOS scenarios. 21

2.5 Path loss versus T-R separation distance in LOS and NLOS scenarios. The carrier frequency is 2.1 GHz. 22

2.6 Path loss versus carrier frequency in LOS and NLOS scenarios. 23

2.7 Gas absorption. Specific attenuation versus carrier frequency in winter (dry air) and summer scenarios. 28

2.8 Clouds and fog. Attenuation versus carrier frequency in winter (dry air) and summer scenarios. 28

2.9 Rain effect. Attenuation versus rain rate. The elevation and tilt angles are 0 degree, the carrier frequency is 100 GHz. 29

2.10 Rain effect. Attenuation versus carrier frequency. The rain rate is 20 mm/h, The elevation and tilt angles are 0 degree. 29

2.11 Rain effect. Attenuation versus elevation angle. The rain rate is 20 mm/h, the carrier frequency is 100 GHz. 30

2.12 Rain effect. Attenuation versus tilt angle. The rain rate is 20 mm/h, the carrier frequency is 100 GHz. 30

2.13 Overall path loss. The path loss versus the T-R separation distance. For the sake of simplicity, the additional loss caused by the shadowing and fading effects and the extra loss caused by the atmospheric effects are not considered here. 31

2.14 Overall path loss. The path loss versus the carrier frequency. For the sake of simplicity, the additional loss caused by the shadowing and fading effects and the extra loss caused by the atmospheric effects are not considered here. 31

2.15 Overall path loss. The path loss versus the altitude of the user equipment. For the sake of simplicity, the additional loss caused by the shadowing and fading effects and the extra loss caused by the atmospheric effects are not considered here. 32

2.16 An illustration of extending 3GPP RMa and UMa models over 300 m altitude. 33

3.1 The different branches/classes in aviation category, the figure is derived from [P1]. 37

3.2 The predicted outage probability, based on the FSL and 3GPP models, the figure is derived from [P1]. Presuming the interference-free condition in mmWave bands, and 25 dB interference in cmWave bands. 40

3.3 The definition of elevation and azimuth angles. 41

3.4 The demonstration of radiation pattern of single-antenna system. . . 41

3.5 The demonstration of radiation pattern of multi-antenna system, i.e., the ULA. 42
3.6 The demonstration of radiation pattern of multi-antenna system, i.e., the URA. 43
3.7 Under SISO settings, comparisons between Terrestrial Users (TU) and Aerial Users (AU) in RMa and UMa scenarios. 45
3.8 Comparisons between MISO and MIMO schemes in RMa and UMa scenarios. The AU is short for Aerial Users. The comparisons are for one user case. 45
3.9 The demonstration of mono-static radar. A radar station is responsible for both transmitting and receiving signals, hence locating the target. 50
3.10 The process of radar receiving. 50
3.11 The output of matched filter. 52
3.12 The hypothesis testing, detection rate and false alarm rate. Blue dashed lines represent the mean values, red dashed line represents the threshold. 53

4.1 A generic architecture description of a transmitter for GNSS signals, valid for both satellites and spoofers. The differences lie in the hardware traits of the illustrated blocks. The red arrows indicate the signals do not carry extra 'fingerprints' from the previous unit; the blue arrows imply that the signals carry extra 'fingerprints' from the previous unit. Derived from [P6]. 59
4.2 The GNSS receiver chain, where the pre-correlation and post-correlation domains are defined. Derived from [P5]. 60

4.3 The conceptual classifier in pre-correlation methods. Examples of feature extractor are DWT, kurtosis, TKEO and spectrogram; examples of machine learning methods are SVM, KNN and LDA. . . . 61

4.4 Comparisons between LDA separation and random separation, corresponding projection histogram is on the right side. 64

4.5 The RF fingerprinting based anti-spoofing PVT solution. 66

4.6 The lab equipment and setups for measurement campaigns in Tampere, Finland. 67

5.1 An example how the location-based beamforming works. The red lobe denotes the steering angle in last time instant, the blue lobe denotes the current steering angle, the green lobe with dashed line denotes the ground truth, where the antenna should radiate towards in the moment. 74

5.2 The scenarios of demonstration and URA 3D geometry. 75

5.3 The directivity of an 4×4 URA when no angle errors are present. . . 76

5.4 The directivity of an 4×4 URA when angle errors are present. The location errors follow $\mathcal{N}(0, 50^2)$ (unit: m) in the horizontal direction, and follow $\mathcal{N}(0, 100^2)$ (unit: m) in the vertical direction. 77

5.5 The directivity versus the number of antenna elements, under two different angle errors. 78

6.1 The allocation of resource blocks in the superposition coding scheme. This example considers two users with simultaneous sensing and communications. 82

6.2 The communications signal processing of superposition coding at the user devices. 83

6.3 The radar signal processing of superposition coding at the base station. 84

6.4 An example of a base station simultaneously implementing communications and detection tasks. 86

List of Tables

2.1 Parameters in 3GPP models. 13

2.2 Part of parameters in InF subcategories, derived from [38]. 14

2.3 3GPP path loss models with shadowing. 15

2.4 3GPP LOS probability. 18

2.5 Parameters in demonstration. 20

3.1 Coverage of different technologies. 38

3.2 Design recommendations. 43

4.1 SV ID of selected signals (with C/N_0). 68

4.2 Classification results of pre-correlation methods, results are given as accuracy [%]. 69

4.3 Mean classification accuracy [%] results, benchmark comparison. . . 70

5.1 Prediction results (mean value), benchmark comparison 76

ABBREVIATIONS

3GPP	3rd Generation Partnership Project
AAU	Active Antenna Unit
ADC	Analogue-to-Digital Converter
ADS-B	Automatic Dependent Surveillance–Broadcast
AOA	Angle of Arrival
AU	Aerial Users
CDMA	code-division multiple access
cmWave	centimetre Wave
CNR	Carrier-to-Noise Ratio
CoMP	Coordinated Multi-Point
CR	Cognitive Radio
CRLB	Cramér-Rao lower bound
CSI	Channel State Information
DAC	Digital-to-Analogue Converter
DoS	Denial of Service
DR	Dead Reckoning
DSA	Dynamic Spectrum Access
DWT	Discrete Wavelet Transform
FAA	Federal Aviation Administration
FCC	Federal Communications Commission
FDMA	frequency-division multiple access

FSL	Free Space Loss
GA	General Aviation
GDOP	Geometric Dilution of Precision
GLONASS	Global Navigation Satellite System
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HPA	High Power Amplifier
ICAO	International Civil Aviation Organisation
IEEE	Institute of Electrical and Electronics Engineers
IIoT	Industrial Internet of Things
InF	Indoor Factory
InF-DH	Indoor Factory-Dense clutter, High base station
InF-DL	Indoor Factory-Dense clutter, Low base station
InF-HH	Indoor Factory-High Tx, High Rx
InF-SH	Indoor Factory-Sparse clutter, High base station
InF-SL	Indoor Factory-Sparse clutter, Low base station
InH	Indoor Hotspot
InHm	Indoor Hotspot mixed office
InHo	Indoor Hotspot open office
IoT	Internet of Things
ISAC	Integrated Sensing And Communications
ISM	Industrial Scientific Medical
ITU	International Telecommunication Union
KNN	K-Nearest Neighbours
KPI	Key Performance Indicators
LDA	Linear Discriminant Analysis

LEO	Low Earth Orbit
LOS	Line-Of-Sight
LTE	Long-Term Evolution
MA	Manned Aviation
MEO	Medium Earth Orbit
MIMO	Multiple-Input Multiple-Output
MISO	Multiple-Input Single-Output
mmWave	millimetre Wave
MUSIC	MUltiple SIgnal Classification
NLOS	Non-Line-Of-Sight
NMA	Navigation Message Authentication
NR	New Radio
NTN	Non-Terrestrial Networks
OCXO	Oven Controlled Crystal Oscillator
OFDM	Orthogonal Frequency-Division Multiplexing
OSNMA	Open Service Navigation Message Authentication
PCA	Principal Components Analysis
PDR	Pedestrian Dead Reckoning
PNT	Position, Navigation and Timing
PVT	Position, Velocity and Time
QoS	Quality of Service
RF	Radio Frequency
RMa	Rural Macrocell
RSS	Received Signal Strength
SDR	Software-Defined Radio
SIC	Successive Interference Cancellation
SINR	Signal-to-Interference-plus-Noise Ratio

SIR	Signal-to-Interference Ratio
SISO	Single-Input Single-Output
SNR	Signal-to-Noise Ratio
STFT	Short-Time Fourier Transform
sUAS	small Unmanned Aircraft System(s)
SV ID	Space Vehicle IDentifier
SVM	Support Vector Machine
T-R	transmitter-receiver
TDD	Time Division Duplex
TDOA	Time Difference of Arrival
TKEO	Teager–Kaiser Energy Operator
TOA	Time of Arrival
TU	Terrestrial Users
UA	Unmanned Aviation
UAV	Unmanned Aerial Vehicle
ULA	Uniform Linear Array
UMa	Urban Macrocell
UMi	Urban Microcell
URA	Uniform Rectangular Array
USRP	Universal Software Radio Peripheral
UWB	Ultra Wide Band
V2V	Vehicle-to-Vehicle

ORIGINAL PUBLICATIONS

[P1] W. Wang, J. Talvitie, E. J. Adamova, T. Fath, L. Korenciak, M. Valkama and E. S. Lohan. Empowering Heterogeneous Communication Data Links in General Aviation through mmWave Signals. *IEEE Wireless Communications* 26.6 (2019), 164–171. DOI: 10.1109/MWC.0001.1800593.

[P2] W. Wang, S. L. Capitaneanu, D. Marinca and E. S. Lohan. Comparative Analysis of Channel Models for Industrial IoT Wireless Communication. *IEEE Access* 7 (2019), 91627–91640. DOI: 10.1109/ACCESS.2019.2927217.

[P3] W. Wang and E. S. Lohan. Applicability of 3GPP Indoor Hotspot Models to the Industrial Environments. *2018 8th International Conference on Localization and GNSS (ICL-GNSS).* 2018, 1–5. DOI: 10.1109/ICL-GNSS.2018.8440893.

[P4] W. Wang, T. Fath, M. Valkama and E. S. Lohan. Modeling and Mitigating 5G Wireless Downlink Interferences for Low-altitude Aerial vehicles. *2020 International Conference on Localization and GNSS (ICL-GNSS).* 2020, 1–6. DOI: 10.1109/ICL-GNSS49876.2020.9115534.

[P5] W. Wang, I. Aguilar Sanchez, G. Caparra, A. McKeown, T. Whitworth and E. S. Lohan. A Survey of Spoofer Detection Techniques via Radio Frequency Fingerprinting with Focus on the GNSS Pre-Correlation Sampled Data. *Sensors* 21.9 (2021). ISSN: 1424-8220. DOI: 10.3390/s21093012.

[P6] W. Wang, E. S. Lohan, I. Aguilar Sanchez and G. Caparra. Pre-correlation and post-correlation RF fingerprinting methods for GNSS spoofer identification with real-field measurement data. *in Proceedings of NAVITEC.* Apr. 2022.

[P7] W. Wang, N. Okati, I. Tanash, T. Riihonen and E. S. Lohan. Location-Based Beamforming Architecture for Efficient Farming Applications with Drones. *2019 International Conference on Localization and GNSS (ICL-GNSS)*. 2019, 1–6. DOI: `10.1109/ICL-GNSS.2019.8752698`.

[P8] W. Wang, B. Tan, E. S. Lohan and M. Valkama. Converging Radar and Communications in the Superposition Transmission. *2021 17th International Symposium on Wireless Communication Systems (ISWCS)*. 2021, 1–6. DOI: `10.1109/ISWCS49558.2021.9562169`.

Author's contribution

The author's contributions in each publication are summarised in the following. The author of this thesis, Wenbo Wang, was the first author in all the following publications; the supervisor of Wenbo Wang, Elena Simona Lohan, involved in each publication and contributed largely in the topic ideas.

[P1] Wenbo contributed to the conceptualisation, writing, visualisation, methodology and data analysis; the rest of authors were responsible for the conceptualisation, writing, methodology and review.

[P2] Wenbo was responsible for the conceptualisation, writing, visualisation, methodology and data analysis; the rest of authors contributed to the conceptualisation, writing, visualisation and review.

[P3] Wenbo contributed to the conceptualisation, writing, visualisation, methodology and data analysis; Simona was responsible for the conceptualisation, writing, methodology and review.

[P4] Wenbo was responsible for the conceptualisation, writing, visualisation, methodology and data analysis; Simona contributed to the conceptualisation, writing, visualisation and methodology; the rest of authors helped in review and editing.

[P5] Wenbo contributed to the conceptualisation, writing, visualisation, methodology and data analysis; Andy and Tim were responsible for the measurement campaign; Simona was responsible for the conceptualisation, writing and methodology; the rest of authors helped in review and editing.

[P6] Wenbo contributed to the conceptualisation, writing, visualisation, methodology and data analysis; Simona contributed to the conceptualisation, writing, methodology and review; the rest of authors were responsible for review and editing.

[P7] Wenbo was responsible for the writing, visualisation, methodology and data analysis; Niloofar and Islam contributed to the conceptualisation, writing; the rest of authors helped in the review and editing.

[P8] Wenbo contributed to the conceptualisation, writing, visualisation, methodology and data analysis; Bo and Simona contributed to the conceptualisation, writing and methodology; Mikko helped in the review and editing.

1 INTRODUCTION

"The RF convergence is inevitable."

– the author's view

1.1 History and status quo

The communications, positioning, and sensing were born to serve their own purpose. In 1901, the first ever trans-Atlantic radio signal carrying Morse code for the letter 's' travelled nearly 3500 kilometres from Cornwall, England to Newfoundland, Canada. During World War II, the urge of using radio to detect and track aircraft sparked a surge in the radar technologies development. In February 1978, the first experimental prototype Global Positioning System (GPS) Block I satellite was launched in Vandenberg, United States. These three systems, wireless communications, radar and Global Navigation Satellite System (GNSS), have thrived over decades mostly on their own path. Though efforts of cooperation among systems could be found in both academia and industrial in the past, the concepts of RF convergence in recent years actually put the resolve to merge these systems.

To begin with, why do we need the RF convergence?

The frequency spectrum is congested. The problem of the scarcity of spectrum was raised after the exponential growth of wireless applications had begun, for example, one Federal Communications Commission (FCC) document [1] in 2003 could easily give the impression of spectrum being congested. To tackle the problem, the early endeavours have been made in the Cognitive Radio (CR) and Dynamic Spectrum Access (DSA) to uplift the spectrum efficiency. In the cognitive radio aspect, the works in [2, 3] address and promote various CR techniques for the efficient usage of spectrum; the authors in [4] design new waveforms in the context of CR to increase the spectrum efficiency; the research in [5] looks at the throughput metric for the secondary user of CR; the authors in [6, 7] carry out an implementation of CR, based on OFDM techniques. Regarding the dynamic spectrum access aspect, the works in [8, 9] review the state-of-the-art techniques in DSA for the purpose of boosting the spectrum efficiency; the authors in [10, 11] propose and discuss optimal sensing techniques in DSA; the research in [12, 13] investigates the access opportunities for secondary users in DSA. Recently, the concept of joint sensing and communications, as a very promising candidate to handle the spectrum congestion issues, has drawn large attention. The work in [14] conducts a short survey on the spectrum sharing between radar and communications; the authors in [15] review the cutting-edge techniques in a joint sensing-and-communications system; the work in [16] classifies the sensing and communications systems as *coexistence*, *cooperation*, and *co-design*; the authors in [17] build up the framework for the dual-function radar and communications; the research works in [18–20] propose the OFDM-based waveform design for joint systems; similarly, plenty of works in [20–30] discuss the self-interference cancellation, which is the key technique in a duplex system, the duplex system plays an important role in the *coexistence* of sensing and communications.

Location information is typically available and can be used for other tasks than localisation. Nowadays the location information could be acquired in the low-cost manner due to developments in GNSS. Therefore, the exploitation of the available location information may benefit the wireless communications in many ways. For example, the available location information can help to reduce the communications overhead in ad-hoc networks; for example, the authors in [31–33] explore the position-based routing strategies due to the accessible location information through cheap GNSS receiving. Utilising the location information may also help in saving time-frequency resource blocks; for example, the work in [34] studies the position-based beamforming and suggests the usage of location information provided by the GNSS in order to help saving time-frequency resource blocks. Several other studies [35, 36] also show that the usage of location information in wireless system enhances service quality for aerial users. The research works in [35, 36] propose a hybrid scheme by combining the traditional CSI-based and newly developed position-based beamforming for UAVs and it concludes that the hybrid scheme enhances the service quality for the aerial users.

With the above two motivations in mind, we take a step back to look at the bigger picture: the fundamentals for the study of joint sensing and communications, and the prerequisites for the utilisation of location information in wireless communications. The wireless channel models, as an essential part in RF convergence research, need intensive investigations; one main prerequisite for the widely usage of GNSS service is its resilience to any intended or unintended interference, in other words, attentions must be paid to ensure continuity of GNSS services.

Before the era of 5G wireless communications, the terrestrial users have been the dominant parts of the cellular services. Consequently, most of the channel models in the literature have focused on scenarios near the ground or on the ground. However, the prosperous markets of UAVs and other low-altitude civil aircraft has urged us to study extended channel models also for ground-to-air/air-to-ground scenarios. Moreover, the merging of sensing and communications systems also hints to us that the potential users, i.e., the aerial users, could benefit from the well-developed ground-to-air/air-to-ground wireless channel models. In the literature, the 3GPP released a few documents addressing the ground-to-air/air-to-ground channel models. For example, the documents in [37, 38] provide channel models under LTE considerations for aerial users up to 300 m altitude; the authors in [39] conduct thorough reviews on the recent findings of ground-to-air/air-to-ground wireless channel models. Nevertheless, a comprehensive study of channel models for aerial users, particularly above 300 m altitude, was still lacking at the time of doing this research work and it is a part addressed in this thesis.

Threats to the popular GNSS services have increased dramatically in the recent past, and are still posing serious problems nowadays. Various attacks to the GNSS receiver create vulnerabilities to users relying on the GNSS services. Labelled intentional threats to the GNSS are jamming, meaconing, and spoofing [40]. The authors in [41] reviews the intentional interference to the GNSS, and lists the state-of-the-art technologies in jamming and spoofing and existing countermeasures. The spoofing and its countermeasures have also been studied in both academia and industrial domains; for example, the work in [40] summarises several methods as the anti-spoofing countermeasures. In recent years, the machine-learning methods have become hot topics in many fields. As a consequence, the machine-learning methods have achieved astonishing developments. Researchers are intrigued by the ideas of incorporating machine-learning methods into the interference mitigation in GNSS and this is also a part addressed in this thesis.

1.2 Aim and scope

This work studies several developments towards the RF convergence, aiming at a deep understanding of channel models for both terrestrial and aerial users flying above 300 m, summarising innovations in communications, positioning and sensing, proposing resilient GNSS solutions, discussing location-aided communications and researching novel waveform design for joint sensing and communications systems. The overall goal is to pave the road towards RF convergence, by tackling various aspects in the three domains involved in the RF convergence: communications, sensing, and positioning.

At the beginning of the study, the classic and 3GPP channel models are reviewed and extended to fit both the ground and aerial users. The atmospheric effects are also investigated, especially considering the current tendency of spectrum shifting to the mmWave bands in 5G and beyond-5G communications. The channel models are treated as the bedrock for the later developments on the RF-convergence building blocks.

Then, the state-of-the-art in communications, positioning, and sensing is addressed with focus on scenarios such as civil aircraft and Industrial Internet of Things (IIoT) and techniques such as the multi-antenna system. Additional focus is put on interference mitigation in GNSS and on signal models of monostatic radar in the context of sensing aspects.

Last-but-not-least, several new algorithmic aspects are presented: a novel machine-learning-based anti-spoofing GNSS solution is proposed and discussed with real-field measurements; a location-based beamforming is described and validated by comparing with the existing techniques; and a new waveform design for joint sensing and communications is proposed and discussed under various scenarios, and especially for scenarios involving aerial users.

1.3 Research questions and methodology

According to the aim of this thesis, the main research questions are listed in the following:

Q1: “How to model the ground-to-air/air-to-ground channel models when the altitude of users is more than 300 m and the operating frequency of users is at mmWave bands?"

Q2: "How could the innovations in communications, in terms of mmWave and multi-antenna system, benefit the aerial users?"

Q3: "How are the predictive abilities of 3GPP models for various IIoT technologies in indoor industrial sites?"

Q4: "What anti-spoofing mechanisms based on machine learning can be used with raw GNSS data to support robust localisation and location-based applications?"

Q5: "To what extent, a location-based beamforming is beneficial towards joint positioning and communications?"

Q6: "Which scenario is feasible for the newly developed waveform in the joint sensing and communications system, and what is the performance of the new waveform design?"

The channel models are investigated mainly through the literature review and theoretical extensions, the 3GPP and ITU documents are preferable given their popularity in industrial. The proposed channel models need to be compared with other models under various scenarios. The studies in communications, positioning and sensing focus on the developments in interference mitigation for aerial users, security in GNSS and models of reflected echos in joint sensing and communications system. The proposed models and/or algorithms in communications, positioning and sensing are validated by numerical analysis and/or theoretical proofs. The anti-spoofing methods are tested by conducting a measurement campaign. The location-based beamforming is analysed through simulations, the results are compared with that from conventional methods. The novel waveform for the joint sensing and communications system is discussed under parameters estimations and detection rate comparisons.

1.4 Contributions and organisation

This thesis is composed of 8 publications, with the author of this thesis being the first author in all publications. The publications are either peer-reviewed conference papers, i.e., [P3, P4, P6-P8], or journal articles, i.e., [P1, P2, P5]. The publications cover different aspects in the topic of RF convergence. As shown in Fig. 1.1, the main focus of [P1-P3] is on the channel models, which later serve as the essential parts in communications, positioning, and sensing tasks in any receiver; with respect to the communications part, [P4] discusses the interference mitigation for aerial users in 5G; with respect to the positioning part, papers [P5, P6] propose and validate anti-spoofing methods for ensuring robustness of GNSS PNT; publication [P7] introduces and tests via simulations a location-aided communications algorithm; [P8] proposes a novel waveform design for joint sensing and communications system.

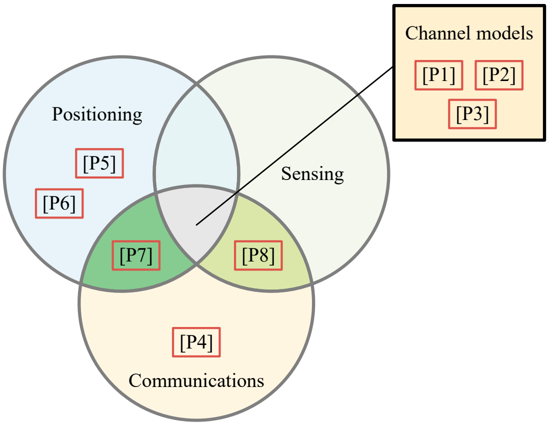


Figure 1.1 The illustration of how the thesis is composed and the inter-relationship among publications.

Specifically, with the assistance of Fig. 1.2, we summarise the main contributions of this thesis below:

- A comprehensive study on channel models is carried out. Based on 3GPP models and reported channel models, e.g., [42], for the aerial users we extend the Urban Macrocell (UMa) and Rural Macrocell (RMa) channel models to the above 300 m altitude scenarios, in [P1, P4]. Regarding to the usage of mmWave bands in 5G, we incorporate the atmospheric effects, based on the ITU documents, into the newly developed channel models, in [P4]. With the proposed channel models, we predict the system performance for cellular datalinks supporting low-altitude general aviation, in [P1]. As benefited from the survey of channel models, we also conduct the research in indoor channel models, the

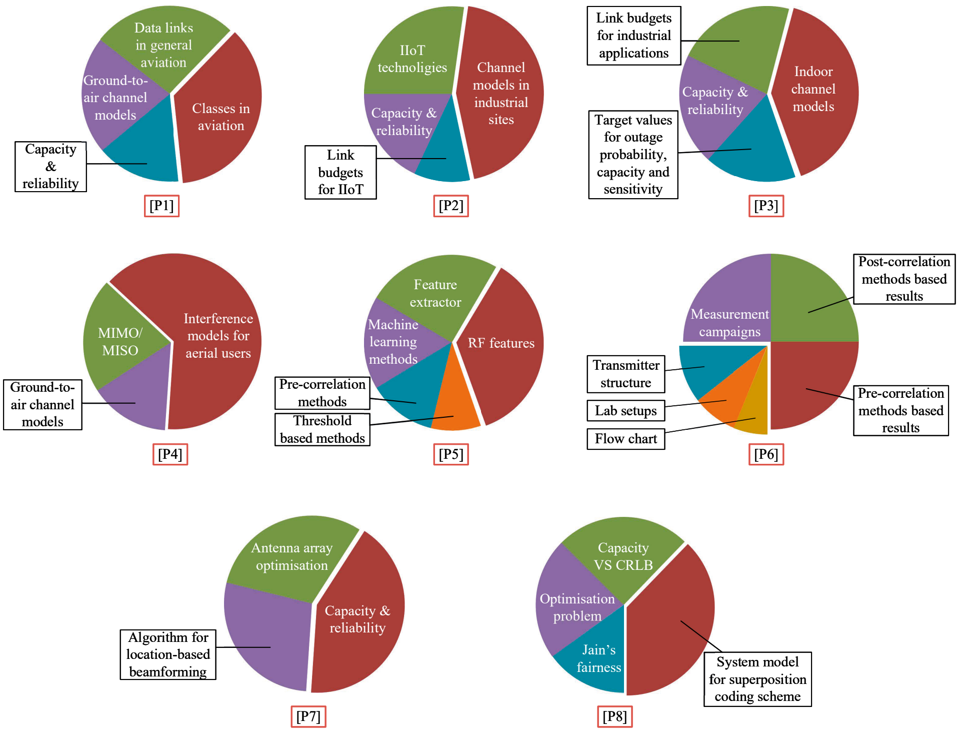


Figure 1.2 An illustration of contributions from each publication. [P1]-[P8] denotes the publication 1 to publication 8. The abbreviations in the figure are listed here: Industrial Internet of Things (IIoT), Multiple-Input Single-Output (MISO), Multiple-Input Multiple-Output (MIMO), Radio Frequency (RF), Cramér-Rao lower bound (CRLB).

predictions from models for the industrial environments are compared with the reported values from literature, in [P2, P3].

- For the first time, we introduce the high-level classification of aviation to the communications society, in [P1].
- We consider the multi-antenna system for the interference mitigation in the ground-to-air/air-to-ground communications, targeting both UAVs and other low-altitude airborne vehicles, in [P4].
- Thanks to the advancement of machine-learning methods, for the first time we apply RF fingerprinting with pre-correlation and post-correlation GNSS data in order to achieve the resilient GNSS Position, Velocity and Time (PVT) solutions, in [P5, P6]. The RF fingerprinting methods are thoroughly described and the hardware impairments (i.e., potential RF fingerprints) of GNSS sig-

nals transmitters are identified with explanations, in [P5]. Two measurement campaigns are carried out for the purpose of proof of concept, based on the real-field data testing we validate the RF fingerprinting methods for the anti-spoofing, in [P6].

- We investigate the possibilities of location-aided communications, i.e., the location-based beamforming. Several numerical analyses are implemented and compared with the conventional methods, i.e., the CSI-based methods. We could conclude the location-based beamforming has high tolerance of channel noise and lower the communications overhead, in [P7].
- We propose a novel superposition coding scheme for the joint sensing and communications system, particularly aiming at the control & command signals in aerial users communications task. The proposal is discussed in terms of optimisation of parameters estimation in sensing and capacity in communications, fairness in communications, detection rate in sensing, partial results in [P8].

The rest of this thesis is constructed as follows. Chapter 2 reviews the free space loss model, log-distance path loss model and 3GPP models, together with the introduction of the atmospheric effects from the ITU documents. The channel models are further developed to above 300 m altitude scenarios. Chapter 3 goes through the innovations in communications, positioning, and sensing: in the aspect of communications, the multi-antenna system is discussed; in the aspect of positioning, the anti-spoofing techniques are reviewed; in the aspect of sensing, the signal model and signal processing are introduced. Chapter 4 identifies in detail the sources of RF fingerprints from the GNSS signals transmitter. The RF fingerprinting techniques are introduced, and validated through real-field measurements. Chapter 5 introduces the location-based beamforming and corresponding simulations results, comparisons with other beamforming methods are conducted. Chapter 6 introduces the superposition coding scheme as the waveform design for the joint sensing and communications system, metrics such as parameters estimation and detection rate are evaluated under the new coding scheme. Last but not least, Chapter 7 concludes the main findings in the thesis, answers the research questions, and directs to the future research path.

2 WIRELESS CHANNEL MODELS

The study of wireless channel models provides the perception of fundamental limitations in the radio propagation. However, there is no easy way to comprehend the wireless channel analysis by considering every aspect that has influences in radio propagation. Signals travelling from one point to another may experience various obstacles, changing mobility, penetrating materials etc. As a consequence, the wireless channel models are typically given in simplified and statistical fashion.

This chapter will partially cover publications [P1-P4, P6] and serves as the prerequisite knowledge for these publications. In addition, the chapter intends to act as a manual for the 3rd Generation Partnership Project (3GPP) channel models and the International Telecommunication Union (ITU) atmospheric effects, and it also unifies the models previously given in [P1-P4].

2.1 Channel models

Modelling the wireless channel is the essence to further analysis of the radio system. With the knowledge of channel models, the Key Performance Indicators (KPI), such as coverage, outage probability, link budgets and throughput, etc., could be approximated for the system of interest. Furthermore, the KPI initiate the deployments of suitable radio system in a certain area.

Signals in the form of electromagnetic waves travel with power loss. The power loss caused by signals propagation can be mainly attributed to the Transmitter-Receiver (T-R) separation distance and the carrier frequency. Additionally, the signals attenuation is influenced by shadowing, reflection, refraction, scattering and diffraction of the radio wave. In statistical analysis, the path loss is typically characterised by the mean value of the signal strength variations, the large scale fading describes the signal strength variations after long travelling distance and the small scale fading describes the signal strength variations over short distance and by short period. The large scale fading typically includes the path loss and shadowing, while the small scale fading contains the fast fading, the slow fading and the multipath fading. Fig. 2.1 illustrates the effects of path loss, shadowing and fading; the path loss in the figure is based on the free space loss, the shadowing follows the log-normal distribution, and the fading follows the Rayleigh distribution. As a rule of thumb, the shadowing and fading usually bring a few extra dB loss in the received signal, on top of the path losses.

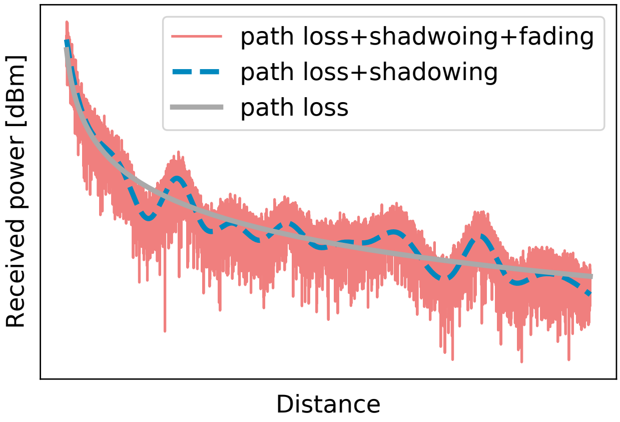


Figure 2.1 An illustration of path loss, shadowing and fading effects. The path loss is based on free space loss (introduced in Section 2.1.1), the shadowing follows log-normal distribution, the fading follows Rayleigh distribution.

The channel models could be described in many ways, the simplest one is the free space loss model; the most practical one is the log-distance path loss model; the most recognised one is the 3GPP models [43]. Free space loss considers purely Line-Of-Sight (LOS) propagation [44], log-distance path loss model is typically following a single slope model [45], 3GPP models are comprehensive but complex [43].

2.1.1 Free-space loss

The free space loss (FSL) model, which is derived from the Friis transmission formula, is usually treated as the benchmark for wireless channel analysis. Its merits lie on the simplicity of mathematical expression and a small number of parameters. In practice, the FSL is a good model to indicate the lower bound of path loss, though it is often too idealistic to accurately predict the wireless channel situation.

In mathematical form, the free space loss FSL is given by [44],

$$FSL = 20\log_{10}(d) + 20\log_{10}(f_c) + 32.45 \tag{2.1}$$

where d (unit: kilometre) denotes the distance between the transmitter and receiver, in many literature, this distance is also called T-R separation distance, f_c (unit: megahertz) denotes the operating frequency of signals.

2.1.2 Log-distance path loss model

In practice, one of the most used models in the literature is the log-distance path-loss model (also appears as one-slope model in some articles), when we decide to model the wireless channel of some indoor or outdoor scenarios. Its nature of being generic, simple and tractable makes it warmly welcomed by many researchers in the relevant fields. Based on log-distance path loss model, the authors in [46] study the channel loss on industrial sites at three Industrial Scientific Medical (ISM) bands, namely 900 MHz, 2400 MHz and 5200 MHz. The path loss model developed by [47], for investigating low-altitude Unmanned Aerial Vehicle (UAV) channel state, could be considered as a variant of log-distance path loss model that incorporating the 3GPP models in [37]. The work in [48] analyses the characterisation of air-ground wireless channel by adopting the log-distance path loss model. The air-ground channel models are also studied in [49], which compares log-distance path loss model with two-ray model in terms of complexity and accuracy.

The formula of log-distance path loss model is expressed as,

$$L_{\text{log-dist}} = L_0 + 10\alpha_{\text{PL}} \log_{10}\frac{d}{d_0} + \beta_{\text{PL}} \tag{2.2}$$

where $L_{\text{log-dist}}$ is the log-distance path loss (unit: dB), L_0 (unit: dB) is the path loss at the reference distance d_0 (unit: meter), α_{PL} is the path loss exponent (unitless), β_{PL} reflects the additional attenuation (unitless) caused by shadowing or multipath fading . β_{PL} follows Gaussian distribution (in dB) when only shadowing is present, and it follows Rayleigh distribution or Rician distribution (the envelop of signals in volts follows the mentioned distribution, β_{PL} is then equal to the 10 times of logarithm of the Rayleigh or Rician random variables.) when only multipath fading is present. The parameters α_{PL} and β_{PL} are usually derived by fitting the measurements.

This model, with its simplicity, is vastly adopted in many research works. However, its two parameters α_{PL} and β_{PL} are only loyal to a particular scenario. In other words, this model varies along with the surroundings changing. Nevertheless, it is still a good model as the basis to build on.

2.1.3 3GPP channel models

The 3GPP, as a well-acknowledged standards organisation, recently devotes considerable effort developing channel model for cellular networks, especially the 5G New Radio (NR) developments. The terrestrial channel models in [38] span from 0.5 GHz to 100 GHz operating frequency; [37] further extends the model up to 300 m altitude.

Unlike models in Section 2.1.1 and Section 2.1.2, 3GPP models, on one hand, they show slightly higher complexity than these two models; on the other hand, they thoroughly describe the trait of channel loss. As a consequence, 3GPP models are computed with many parameters as shown in Table 2.1.

Rural Macrocell (RMa) model characterises the path loss of signals propagation in rural areas, based on the following parameters: parameters the base station height h_{BS} (unit: meter), the user equipment height h_{UE} (unit: meter), the average street width W_s (unit: meter) and the average building height h_b (unit: meter). Details of parameters are as follows, the height of base station h_{BS} is assumed to range from 10 m to 150 m, the height of user equipment h_{UE} is from 1 m to 10 m, the street width W_s is from 5 m to 50 m, the building height h_b is from 5 m to 50 m. Additionally, the model applies a breakpoint distance d_{BP} (unit: meter) concept to divide the path loss calculation into two segments: 1) one segment with the horizontal distance d_{2D} (in meter) smaller than breakpoint distance and 2) the other segment with the horizontal distance greater than breakpoint distance. The breakpoint distance is calculated by considering the base station height and the user equipment height.

Urban Macrocell (UMa) model characterises the path loss of signals propagation in urban areas where the base station antenna is above rooftops. The height of base station h_{BS} is assumed to be 25 m, the height of user equipment h_{UE} is from 1.5 m to 22.5 m. The concept of breakpoint distance is also employed in this model.

Table 2.1 Parameters in 3GPP models.

Variables	Unit	Descriptions
d_{2D}	meter	horizontal distance
d_{3D}	meter	T-R separation distance
f_c	Hz/GHz*	carrier frequency
h_{BS}	meter	base station height
h_{UE}	meter	user equipment height
W_s	meter	average street width
h_b	meter	average building height
d_{BP}	meter	breakpoint distance
h_{E}	meter	effective environment height
h_c	meter	effective clutter height
d_{clutter}	meter	typical clutter size
r_{clutter}	percentage	clutter density

* in calculation of breakpoint distance, f_c is in Hz, otherwise f_c is in GHz.

Moreover, the breakpoint distance here is approximated by taking into account of the effective environment height h_{E} (unit: meter).

Urban Microcell (UMi) model characterises the path loss of signals propagation in urban areas where the base station antenna is below rooftops. The height of base station h_{BS} is set as 10 m, the height of user equipment h_{UE} is from 1.5 m to 22.5 m. This model utilises the breakpoint distance as well and applies it as in the UMa model, the effective environment height h_{E} is defined as 1 m.

Indoor Hotspot (InH) model characterises the path loss of signals propagation in indoor scenarios where existing strong reflection of signals and many obstacles in the path. The height of base station h_{BS} is assumed to be 3 m, the height of user equipment h_{UE} is 1 m. InH is further divided in to two subcategories: 1) **the mixed office (InHm)** and 2) **the open office (InHo)**. The difference between these two subcategories lies on the calculation of LOS probability, InHo has higher LOS probability than InHm.

Indoor Factory (InF) model characterises the path loss of signals propagation in factory halls. Based on the size of area and density of clutter, InF has five subcategories: 1) **InF Sparse clutter, Low base station (InF-SL)**, 2) **InF Dense clutter, Low base station (InF-DL)**, 3) **InF Sparse clutter, High base station (InF-SH)**, 4) **InF Dense clutter, High base station (InF-DH)** and 5) **InF High Tx, High Rx (InF-HH)**. The term 'clutter' refers to machinery, assembly lines, storage shelves etc. Part of parameters in five subcategories are defined in Table 2.2, these parameters are involved in the calculation of path loss and LOS probability.

Table 2.2 Part of parameters in InF subcategories, derived from [38].

Parameters	InF-SL	InF-DL	InF-SH	InF-DH	InF-HH
effective clutter height h_c (unit: meter)	$0-10$	$0-10$	$0-10$	$0-10$	$0-10$
typical clutter size d_{clutter} (unit: meter)	10	2	10	2	any
clutter density r_{clutter}	$<40\%$	$\geq 40\%$	$<40\%$	$\geq 40\%$	any

Remark. *The studies in [P2] were based on 3GPP TR 38.901 V14.3.0, while in current version (V16.1.0) of TR 38.901 the InF is newly added contents. To closely follow up the update of 3GPP channel models, InF will join the following discussions as well.*

2.1.3.1 Path loss

Details of path loss in 3GPP channel models will be addressed here. Descriptions of path loss models fall into two classes: LOS and NLOS. For the convenience of comparisons amongst 3GPP models, above-mentioned models are summarised in Table 2.3. The path loss for LOS and NLOS scenarios denote PL_{LOS} and PL_{NLOS} respectively. The shadowing effects are modelled as Gaussian distribution with standard deviation σ_{LOS} or σ_{NLOS} for LOS and NLOS cases respectively, the unit is dB. The formula calculating breaking point distance is added in the additional information column of the table.

Table 2.3 3GPP path loss models with shadowing.

Model	LOS/NLOS	**Path loss & shadowing** (Unit: dB)	**Additional information**
RMa	LOS	$1.5\,\mathrm{m} \le h_{\mathrm{UE}} \le 10\,\mathrm{m}$, $\begin{cases} 10\,\mathrm{m} \le d_{\mathrm{2D}} \le d_{\mathrm{BP}}, \quad \sigma_{\mathrm{LOS1}} = 4 \\ PL_{\mathrm{LOS1}} = 20\log_{10}(\frac{40\pi d_{\mathrm{3D}} f_c}{3}) + \min(0.03h_b^{1.72}, 10)\log_{10}(d_{\mathrm{3D}}) \\ \qquad - \min(0.044h_b^{1.72}, 14.77) + 0.002\log_{10}(h_b)d_{\mathrm{3D}} \\ d_{\mathrm{BP}} < d_{\mathrm{2D}} \le 10\,\mathrm{km}, \quad \sigma_{\mathrm{LOS2}} = 6 \\ PL_{\mathrm{LOS2}} = PL_{\mathrm{LOS1}}(d_{\mathrm{BP}}) + 40\log_{10}(\frac{d_{\mathrm{3D}}}{d_{\mathrm{BP}}}) \end{cases}$ (2.3) $10\,\mathrm{m} < h_{\mathrm{UE}} \le 300\,\mathrm{m}$, $PL_{\mathrm{LOS}} = \max(23.9 - 1.8\log_{10}(h_{\mathrm{UE}}), 20)\log_{10}(d_{\mathrm{3D}}) + 20\log_{10}\left(\frac{40\pi f_c}{3}\right)$ (2.4) $\sigma_{\mathrm{LOS}} = 4.2\exp(-0.0046h_{\mathrm{UE}})$	$d_{\mathrm{BP}} = 2\pi h_{\mathrm{BS}} h_{\mathrm{UE}} f_c / C$, $C = 3 \times 10^8\,\mathrm{m/s}$, f_c is in Hz for breakpoint distance calculation, C is speed of light, σ_{LOS1} and σ_{LOS2} (unit: dB) are shadowing fading standard deviation.
	NLOS	$1.5\,\mathrm{m} \le h_{\mathrm{UE}} \le 10\,\mathrm{m}$, $PL_{\mathrm{NLOS}} = \max(PL_{\mathrm{LOS}}, PL'_{\mathrm{NLOS}}), \quad \sigma_{\mathrm{NLOS}} = 8$ $PL'_{\mathrm{NLOS}} = 161.04 - 7.1\log_{10}(W_s) + 7.5\log_{10}(h_b) - \big(24.37 - 3.7(h_b/h_{\mathrm{BS}})^2\big)\log_{10}(h_{\mathrm{BS}}) + \big(43.42 - 3.1\log_{10}(h_{\mathrm{BS}})\big)\big(\log_{10}(d_{\mathrm{3D}}) - 3\big) + 20\log_{10}(f_c) - \Big(3.2\big(\log_{10}(11.75h_{\mathrm{UE}})\big)^2 - 4.97\Big)$ (2.5) $10\,\mathrm{m} < h_{\mathrm{UE}} \le 40\,\mathrm{m}$, $PL_{\mathrm{NLOS}} = \max(PL_{\mathrm{LOS}}, -12 + (35 - 5.3\log_{10}(h_{\mathrm{UE}}))\log_{10}(d_{\mathrm{3D}}) + 20\log_{10}\left(\frac{40\pi f_c}{3}\right))$ (2.6) $\sigma_{\mathrm{NLOS}} = 6$	

Continued

Model	**LOS/NLOS**	**Path loss & shadowing** (Unit: dB)		**Additional information**
UMa	LOS	$1.5\,\mathrm{m} \le h_{\mathrm{UE}} \le 22.5\,\mathrm{m}$, $\begin{cases} 10\,\mathrm{m} \le d_{\mathrm{2D}} \le d'_{\mathrm{BP}}, \quad \sigma_{\mathrm{LOS1}} = 4 \\ PL_{\mathrm{LOS1}} = 28.0 + 22\log_{10}(d_{\mathrm{3D}}) + 20\log_{10}(f_c) \\ d'_{\mathrm{BP}} < d_{\mathrm{2D}} \le 5\,\mathrm{km}, \quad \sigma_{\mathrm{LOS2}} = 4 \\ PL_{\mathrm{LOS2}} = 28.0 + 40\log_{10}(d_{\mathrm{3D}}) + 20\log_{10}(f_c) \\ \qquad -9\log_{10}\left((d'_{\mathrm{BP}})^2 + (h_{\mathrm{BS}} - h_{\mathrm{UE}})^2\right) \end{cases}$	(2.7)	$d'_{\mathrm{BP}} = 2\pi h'_{\mathrm{BS}} h'_{\mathrm{UE}} f_c / C$, h'_{BS} and h'_{UE} are the effective antenna height, $h'_{\mathrm{BS}} = h_{\mathrm{BS}} - h_{\mathrm{E}}$, $h'_{\mathrm{UE}} = h_{\mathrm{UE}} - h_{\mathrm{E}}$, h_{E} is the effective environment height.
		$22.5\,\mathrm{m} < h_{\mathrm{UE}} \le 300\,\mathrm{m}$, $PL_{\mathrm{LOS}} = 28.0 + 22\log_{10}(d_{\mathrm{3D}}) + 20\log_{10}(f_c)$ $\sigma_{\mathrm{LOS}} = 4.64\exp(-0.0066 h_{\mathrm{UE}})$	(2.8)	
	NLOS	$1.5\,\mathrm{m} \le h_{\mathrm{UE}} \le 22.5\,\mathrm{m}$, $PL_{\mathrm{NLOS}} = \max(PL_{\mathrm{LOS}}, PL'_{\mathrm{NLOS}}), \quad \sigma_{\mathrm{NLOS}} = 6$ $PL'_{\mathrm{NLOS}} = 13.54 + 39.08\log_{10}(d_{\mathrm{3D}}) + 20\log_{10}(f_c) - 0.6(h_{\mathrm{UE}} - 1.5)$	(2.9)	
		$22.5\,\mathrm{m} < h_{\mathrm{UE}} \le 100\,\mathrm{m}$, $PL_{\mathrm{NLOS}} = -17.5 + (46 - 7\log_{10}(h_{\mathrm{UE}}))\log_{10}(d_{\mathrm{3D}}) + 20\log_{10}\left(\frac{40\pi f_c}{3}\right)$ $\sigma_{\mathrm{NLOS}} = 6$	(2.10)	
UMi	LOS	$1.5\,\mathrm{m} \le h_{\mathrm{UE}} \le 22.5\,\mathrm{m}$, $\begin{cases} 10\,\mathrm{m} \le d_{\mathrm{2D}} \le d'_{\mathrm{BP}}, \quad \sigma_{\mathrm{LOS1}} = 4 \\ PL_{\mathrm{LOS1}} = 32.4 + 21\log_{10}(d_{\mathrm{3D}}) + 20\log_{10}(f_c) \\ d'_{\mathrm{BP}} < d_{\mathrm{2D}} \le 5\,\mathrm{km}, \quad \sigma_{\mathrm{LOS2}} = 4 \\ PL_{\mathrm{LOS2}} = 32.4 + 40\log_{10}(d_{\mathrm{3D}}) + 20\log_{10}(f_c) \\ \qquad -9.5\log_{10}\left((d'_{\mathrm{BP}})^2 + (h_{\mathrm{BS}} - h_{\mathrm{UE}})^2\right) \end{cases}$	(2.11)	$h_{\mathrm{E}} = 1\,\mathrm{m}$
		$22.5\,\mathrm{m} < h_{\mathrm{UE}} \le 300\,\mathrm{m}$, $PL_{\mathrm{LOS}} = \max(FSL, 30.9 + (22.25 - 0.5\log_{10}(h_{\mathrm{UE}}))\log_{10}(d_{\mathrm{3D}}) + 20\log_{10}(f_c))$ $\sigma_{\mathrm{LOS}} = \max(5\exp(-0.01 h_{\mathrm{UE}}), 2)$	(2.12)	

Continued

Model	LOS/NLOS	**Path loss & shadowing** (Unit: dB)	**Additional information**
	NLOS	$1.5\,\text{m} \le h_{\text{UE}} \le 22.5\,\text{m}$, $PL_{\text{NLOS}} = \max(PL_{\text{LOS}}, PL'_{\text{NLOS}}), \quad \sigma_{\text{NLOS}} = 7.82$ $PL'_{\text{NLOS}} = 22.4+35.3\log_{10}(d_{\text{3D}})+21.3\log_{10}(f_c)-0.3(h_{\text{UE}}-1.5)$ (2.13) $22.5\,\text{m} < h_{\text{UE}} \le 300\,\text{m}$, $PL_{\text{NLOS}} = \max(PL_{\text{LOS}}, 32.4+(43.2-7.6\log_{10}(h_{\text{UE}}))\log_{10}(d_{\text{3D}}) + 20\log_{10}(f_c))$ (2.14) $\sigma_{\text{NLOS}} = 8$	
InH	LOS	$PL_{\text{LOS}} = 32.4 + 17.3\log_{10}(d_{\text{3D}}) + 20\log_{10}(f_c), \quad \sigma_{\text{LOS}} = 3$ (2.15)	n/a
	NLOS	$PL_{\text{NLOS}} = \max(PL_{\text{LOS}}, PL'_{\text{NLOS}}), \quad \sigma_{\text{NLOS}} = 8.03$ $PL'_{\text{NLOS}} = 17.3 + 38.3\log_{10}(d_{\text{3D}}) + 24.9\log_{10}(f_c)$ (2.16)	
InF	LOS	$PL_{\text{LOS}} = 31.48 + 21.50\log_{10}(d_{\text{3D}}) + 19.00\log_{10}(f_c), \quad \sigma_{\text{LOS}} = 4.3$ (2.17)	n/a
	NLOS	InF-SL: $PL_{\text{NLOS,SL}} = \max(PL_{\text{LOS}}, PL'_{\text{NLOS}}), \quad \sigma_{\text{NLOS}} = 5.7$ $PL'_{\text{NLOS}} = 33 + 25.5\log_{10}(d_{\text{3D}}) + 20\log_{10}(f_c)$ (2.18)	
		InF-DL: $PL_{\text{NLOS,DL}} = \max(PL_{\text{LOS}}, PL'_{\text{NLOS}}, PL_{\text{NLOS,SL}}), \quad \sigma_{\text{NLOS}} = 7.2$ $PL'_{\text{NLOS}} = 18.6 + 35.7\log_{10}(d_{\text{3D}}) + 20\log_{10}(f_c)$ (2.19)	
		InF-SH: $PL_{\text{NLOS,SH}} = \max(PL_{\text{LOS}}, PL'_{\text{NLOS}}), \quad \sigma_{\text{NLOS}} = 5.9$ $PL'_{\text{NLOS}} = 32.4 + 23.0\log_{10}(d_{\text{3D}}) + 20\log_{10}(f_c)$ (2.20)	
		InF-DH: $PL_{\text{NLOS,DH}} = \max(PL_{\text{LOS}}, PL'_{\text{NLOS}}), \quad \sigma_{\text{NLOS}} = 4.0$ $PL'_{\text{NLOS}} = 33.63 + 21.9\log_{10}(d_{\text{3D}}) + 20\log_{10}(f_c)$ (2.21)	

2.1.3.2 LOS probability

3GPP models are categorised into LOS and NLOS cases, the details of LOS probability are listed in Table 2.4. The LOS probability denotes p_{LOS}.

Table 2.4 3GPP LOS probability.

Model	LOS probability
RMa	$1.5\,\mathrm{m} \leq h_{\mathrm{UE}} \leq 10\,\mathrm{m}$, $p_{\mathrm{LOS}} = \begin{cases} 1 & , \quad d_{2\mathrm{D}} \leq 10\,\mathrm{m} \\ \exp\Big(-\dfrac{d_{2\mathrm{D}}-10}{1000}\Big), & 10\,\mathrm{m} < d_{2\mathrm{D}} \end{cases}$ (2.22) $10\,\mathrm{m} < h_{\mathrm{UE}} \leq 40\,\mathrm{m}$, $p_{\mathrm{LOS}} = \begin{cases} 1 & , \quad d_{2\mathrm{D}} \leq d_1 \\ \dfrac{d_1}{d_{2\mathrm{D}}} + \Big(1-\dfrac{d_1}{d_{2\mathrm{D}}}\Big)\exp\Big(\dfrac{-d_{2\mathrm{D}}}{p_1}\Big), & d_{2\mathrm{D}} > d_1 \end{cases}$ (2.23) $p_1 = \max(15021\log_{10}(h_{\mathrm{UE}}) - 16053, 1000)$ $d_1 = \max(1350.8\log_{10}(h_{\mathrm{UE}}) - 1602, 18)$ $40\,\mathrm{m} < h_{\mathrm{UE}} \leq 300\,\mathrm{m}$, $p_{\mathrm{LOS}} = 1$
UMa	$1.5\,\mathrm{m} \leq h_{\mathrm{UE}} \leq 22.5\,\mathrm{m}$, $p_{\mathrm{LOS}} = \begin{cases} 1 & , \quad d_{2\mathrm{D}} \leq 18\,\mathrm{m} \\ \Big(\dfrac{18}{d_{2\mathrm{D}}} + \Big(1-\dfrac{18}{d_{2\mathrm{D}}}\Big)\exp\Big(-\dfrac{d_{2\mathrm{D}}}{63}\Big)\Big)\Big(1+\frac{5}{4}C'(h_{\mathrm{UE}})(\frac{d_{2\mathrm{D}}}{100})^3\exp\Big(-\frac{d_{2\mathrm{D}}}{150}\Big)\Big), & 18\,\mathrm{m} < d_{2\mathrm{D}} \end{cases}$ (2.24) where $C'(h_{\mathrm{UE}}) = \begin{cases} 0 & , \quad h_{\mathrm{UE}} \leq 13\,\mathrm{m} \\ (\dfrac{h_{\mathrm{UE}}-13}{10})^{1.5}, & 13\,\mathrm{m} < h_{\mathrm{UE}} \leq 23\,\mathrm{m} \end{cases}$ (2.25) $22.5\,\mathrm{m} < h_{\mathrm{UE}} \leq 100\,\mathrm{m}$, $p_{\mathrm{LOS}} = \begin{cases} 1 & , \quad d_{2\mathrm{D}} \leq d_1 \\ \dfrac{d_1}{d_{2\mathrm{D}}} + \exp\Big(\dfrac{-d_{2\mathrm{D}}}{p_1}\Big)\Big(1-\dfrac{d_1}{d_{2\mathrm{D}}}\Big), & d_{2\mathrm{D}} > d_1 \end{cases}$ (2.26) $p_1 = 4300\log_{10}(h_{\mathrm{UE}}) - 3800$ $d_1 = \max(460\log_{10}(h_{\mathrm{UE}}) - 700, 18)$ $100\,\mathrm{m} < h_{\mathrm{UE}} \leq 300\,\mathrm{m}$, $p_{\mathrm{LOS}} = 1$

Continued

Model	LOS probability
UMi	$1.5\,\mathrm{m} \leq h_{\mathrm{UE}} \leq 22.5\,\mathrm{m}$, $p_{\mathrm{LOS}} = \begin{cases} 1 & , \quad d_{2\mathrm{D}} \leq 18\,\mathrm{m} \\ \dfrac{18}{d_{2\mathrm{D}}} + \left(1 - \dfrac{18}{d_{2\mathrm{D}}}\right)\exp\left(-\dfrac{d_{2\mathrm{D}}}{36}\right), & 18\,\mathrm{m} < d_{2\mathrm{D}} \end{cases}$ (2.27) $22.5\,\mathrm{m} < h_{\mathrm{UE}} \leq 300\,\mathrm{m}$, $p_{\mathrm{LOS}} = \begin{cases} 1 & , \quad d_{2\mathrm{D}} \leq d_1 \\ \dfrac{d_1}{d_{2\mathrm{D}}} + \exp\left(\dfrac{-d_{2\mathrm{D}}}{p_1}\right)\left(1 - \dfrac{d_1}{d_{2\mathrm{D}}}\right), & d_{2\mathrm{D}} > d_1 \end{cases}$ (2.28) $p_1 = 233.98\log_{10}(h_{\mathrm{UE}}) - 0.95$ $d_1 = \max(294.05\log_{10}(h_{\mathrm{UE}}) - 432.94, 18)$

InH	Mixed office (InHm):
	$p_{\mathrm{LOS}} = \begin{cases} 1 & , \quad d_{2\mathrm{D}} \leq 1.2\,\mathrm{m} \\ \exp\left(-\dfrac{d_{2\mathrm{D}} - 1.2}{4.7}\right), & 1.2\,\mathrm{m} \leq d_{2\mathrm{D}} < 6.5\,\mathrm{m} \\ 0.32\exp\left(-\dfrac{d_{2\mathrm{D}} - 6.5}{32.6}\right), & 6.5\,\mathrm{m} \leq d_{2\mathrm{D}} \end{cases}$ (2.29)
	Open office (InHo):
	$p_{\mathrm{LOS}} = \begin{cases} 1 & , \quad d_{2\mathrm{D}} \leq 5\,\mathrm{m} \\ \exp\left(-\dfrac{d_{2\mathrm{D}} - 5}{70.8}\right), & 5\,\mathrm{m} \leq d_{2\mathrm{D}} < 49\,\mathrm{m} \\ 0.54\exp\left(-\dfrac{d_{2\mathrm{D}} - 49}{211.7}\right), & 49\,\mathrm{m} \leq d_{2\mathrm{D}} \end{cases}$ (2.30)

InF	$p_{\mathrm{LOS}} = \exp\left(-\dfrac{d_{2\mathrm{D}}}{k_{\mathrm{subsce}}}\right)$ (2.31) where $k_{\mathrm{subsce}} = \begin{cases} -\dfrac{d_{\mathrm{clutter}}}{\ln(1 - r_{\mathrm{clutter}})}, & \text{for InF-SL and InF-DL} \\ -\dfrac{d_{\mathrm{clutter}}}{\ln(1 - r_{\mathrm{clutter}})} \cdot \dfrac{h_{\mathrm{BS}} - h_{\mathrm{UE}}}{h_{\mathrm{c}} - h_{\mathrm{UE}}}, & \text{for InF-SH and InF-DH} \end{cases}$ (2.32) $p_{\mathrm{LOS}} = 1, \qquad \text{for InF-HH.}$ (2.33)

2.1.4 Comparisons

This section will explore 3GPP models in more details, especially taking the FSL as the baseline. The 3GPP RMa, UMa and UMi models are investigated in 3D space while the 3GPP InH and InF are in 2D space.

Following the suggestions in [38], for typical use cases, the base station height h_{BS} in RMa, UMa and UMi is respectively 35 m, 25 m and 10 m. Values of average street width W_s and average building height h_n in RMa are 20 m and 5 m. The rest of parameters are listed in Table 2.5.

Table 2.5 Parameters in demonstration.

Variable	Values	Variable	Values
h_{UE}	2 or 2...250 [m]	f_c	2.1 or 1...30 [GHz]
d_{3D}	3000 or 100...3000 [m]	$d_{\mathrm{3D,indoor}}$	100 or 1...150 [m]

* $d_{\mathrm{3D,indoor}}$ denotes the T-R separation distance in InH and InF models.

In a 3D space, as to RMa, UMa and UMi models, Fig. 2.2, Fig. 2.3 and Fig. 2.4 demonstrate separately the path loss versus T-R separation distance, the path loss versus carrier frequency, the path loss versus the height of user equipment (also known as altitude in figures).

In Fig. 2.2, under LOS conditions, path loss in all three models is close to FSL at small T-R separation distance till the breaking point reached. Once the breaking point is passed, the path loss values accelerate, particularly in UMi model. In NLOS case, being in rural or urban areas is a significant factor affecting the path loss.

In Fig. 2.3, path loss in all three models grows exponentially with the values of carrier frequency. In NLOS case, being in rural or urban areas is as well an important factor contributing to the path loss.

In Fig. 2.4, under both LOS and NLOS conditions, the path loss in all three models decreases with the altitude. In LOS case, path loss in RMa eventually converges to FSL; in NLOS case, over a certain altitude, RMa and UMa predict purely LOS propagation.

In a 2D space, with respect to InH and InF models, Fig. 2.5 and Fig. 2.6 demonstrate separately the path loss versus T-R separation distance, the path loss versus carrier frequency.

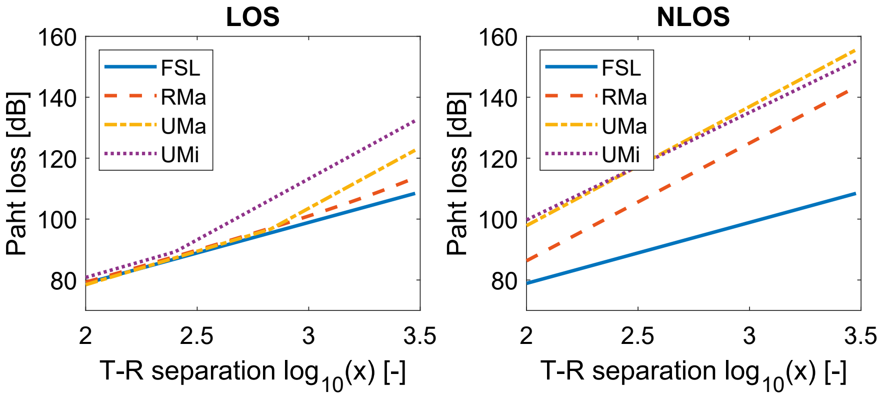


Figure 2.2 Path loss versus T-R separation distance in LOS and NLOS scenarios. The carrier frequency is 2.1 GHz.

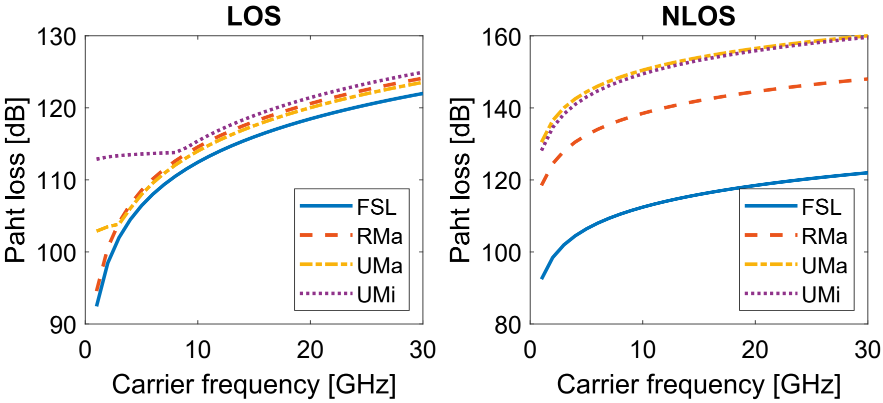


Figure 2.3 Path loss versus carrier frequency in LOS and NLOS scenarios.

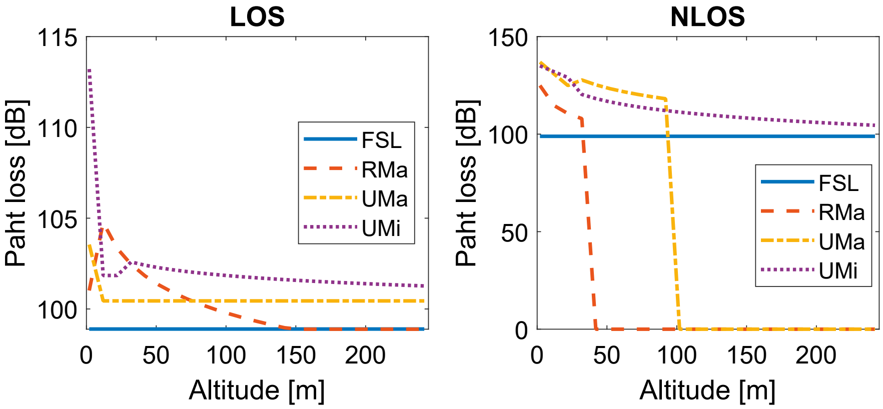


Figure 2.4 Path loss versus altitude in LOS and NLOS scenarios.

It is interesting to observe that, in Fig. 2.5 LOS case, the InF predicts a similar path loss as the FSL, the InH gives even smaller path loss values than the FSL for indoor office scenarios. Under NLOS conditions, all models give higher path loss values than the FSL except near field for the InH models. Surprisingly, the InHo predicts the highest path loss values among the InH and InF models after a certain T-R separation distance is passed.

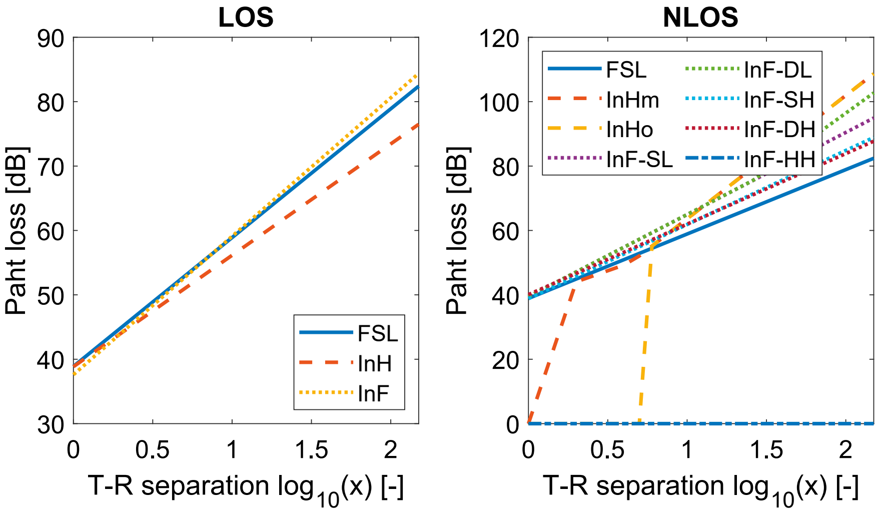


Figure 2.5 Path loss versus T-R separation distance in LOS and NLOS scenarios. The carrier frequency is 2.1 GHz.

In Fig. 2.6, a similar phenomenon is observed for the LOS case, that the InH shows lower path loss values than the FSL. While in the NLOS case, the InH models predict the highest path loss values.

In sum, the RMa and UMa models enter purely LOS signals attenuation when certain altitude thresholds are passed, especially the RMa model converges to the FSL at high altitudes. The InH models shows less signals attenuation than the FSL in the indoor office scenario under LOS conditions.

Remark. *From Fig. 2.2 to Fig. 2.6, the curve of FSL model in the NLOS plot was not meant to be compared with other NLOS loss models, it was simply treated as a bridge to connect the LOS and NLOS models in a comparative way.*

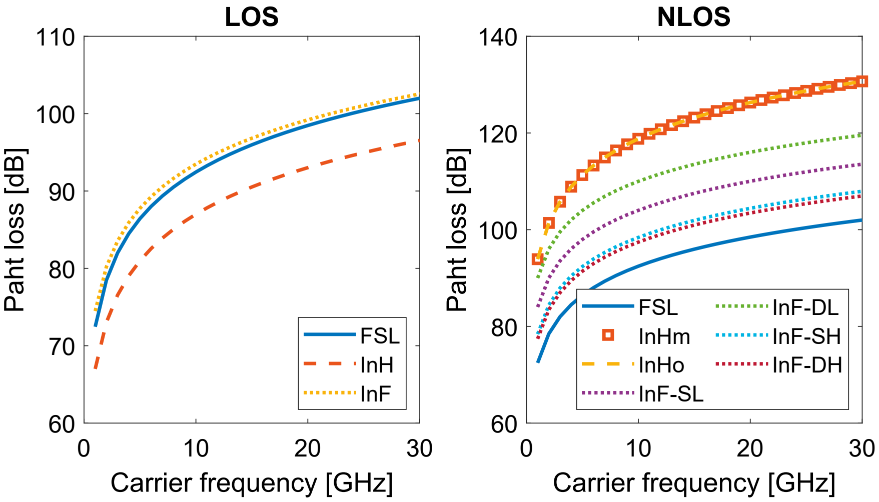


Figure 2.6 Path loss versus carrier frequency in LOS and NLOS scenarios.

2.2 Atmospheric effects

When we step into the territory of 5G New Radio (NR), it is inevitable to utilise the mmWave frequency bands. The electromagnetic waves carrying information are used to travel in the air through various media with negligible 'resistance' until they move to the high operating frequency. At high frequency bands, the 'resistance' caused by the media in the air cannot be ignored. It becomes of interest to study elements that compose the atmospheric effects, such as gas, clouds and fog, rain and snow.

To provide a reference for outdoor scenarios, we consider the reference standard atmospheres in ITU recommendation [50]. Since the research is conducted in Finland, the results shown in this work are under consideration of high altitude region until further notice.

2.2.1 Gas absorption

Signals attenuation caused by the gaseous absorption is due to water vapour, oxygen and dry air. Based on the model in the ITU recommendation [51], for a narrow-band signal, the total loss L_{gas} (unit: dB) caused by gaseous absorption is modelled by,

$$L_{\text{gas}} = (\gamma_d + \gamma_w) d_{3\text{D}} \tag{2.34}$$

where $d_{3\text{D}}$ (unit: km) is the T-R separation distance, γ_d and γ_w are the specific attenuation caused by dry air and water vapour respectively, their summation is given by,

$$\gamma_d + \gamma_w = 0.1820\big(N_o(f_c) + N_w(f_c)\big) \tag{2.35}$$

where f_c (unit: GHz) is the operating frequency, $N_o(f_c)$ and $N_w(f_c)$ are,

$$N_o(f_c) = \sum_i S_i F_i + N_D(f_c) \tag{2.36a}$$

$$N_w(f_c) = \sum_j S_j F_j \tag{2.36b}$$

where S_i is the strength of the i_{th} oxygen line, S_j is the strength of the j_{th} water vapour line, F_i is the oxygen line shape factor, F_j is the water vapour line shape factor, $N_D(f_c)$ is the dry continuum and given by,

$$N_D(f_c) = f_c p_d \left(\frac{300}{T}\right)^2 \left[\frac{6.14 \times 10^{-5}}{w\left[1 + \left(\frac{f_c}{w}\right)^2\right]} + \frac{1.4 \times 10^{-12} p_d \left(\frac{300}{T}\right)^{1.5}}{1 + 1.9 \times 10^{-5} f_c^{1.5}} \right] \tag{2.37}$$

where p_d (unit: hPa) is the dry air pressure, T (Unit: K) is temperature, w is expressed as,

$$w = 5.6 \times 10^{-4}(p_d + p_w)\left(\frac{300}{T}\right)^{0.8} \tag{2.38}$$

the variable p_w (unit: hPa) denotes the water vapour pressure and could be conveniently calculated by the formula,

$$p_w = \frac{\rho_w T}{216.7} \tag{2.39}$$

where ρ_w denotes the water vapour density at a certain altitude.

The variables S_i and S_j are formulated as,

$$S_i = a_1 p_d \times 10^{-7}\left(\frac{300}{T}\right)^3 \exp\left[\left(1 - \frac{300}{T}\right) a_2\right] \tag{2.40a}$$

$$S_j = b_1 p_w \times 10^{-1}\Big(\frac{300}{T}\Big)^{3.5} \exp\Big[\Big(1-\frac{300}{T}\Big)b_2\Big] \tag{2.40b}$$

the variables F_i and F_j are,

$$F_i = \frac{f_c}{f_i}\Big[\frac{\Delta f_o-(f_i-f_c)\delta_{\text{corr}}}{(f_i-f_c)^2+(\Delta f_o)^2}+\frac{\Delta f_o-(f_i+f_c)\delta_{\text{corr}}}{(f_i+f_c)^2+(\Delta f_o)^2}\Big] \tag{2.41a}$$

$$F_j = \frac{f_c}{f_j}\Big[\frac{\Delta f_w}{(f_i-f_c)^2+(\Delta f_w)^2}+\frac{\Delta f_w}{(f_i+f_c)^2+(\Delta f_w)^2}\Big] \tag{2.41b}$$

where f_i and f_j are oxygen and water vapour line frequency respectively, Δf_o, Δf_w and correction factor δ_{corr} are given by,

$$\Delta f_o = a_3 \times 10^{-4}\Big(p_d\Big(\frac{300}{T}\Big)^{0.8-a_4}+1.1p_w\Big(\frac{300}{T}\Big)\Big) \tag{2.42a}$$

$$\Delta f_w = b_3 \times 10^{-4}\Big(p_d\Big(\frac{300}{T}\Big)^{b_4}+b_5 p_w\Big(\frac{300}{T}\Big)^{b_6}\Big) \tag{2.42b}$$

$$\delta_{\text{corr}} = \Big(a_5+a_6\frac{300}{T}\Big) \times 10^{-4}(p_d+p_w)\Big(\frac{300}{T}\Big)^{0.8} \tag{2.42c}$$

Remark. *Values of $a_1, a_2, a_3, a_4, a_5, a_6$ and $b_1, b_2, b_3, b_4, b_5, b_6$ can be found from page 8 to page 10 in [51].*

2.2.2 Clouds and fog

The attenuation caused by clouds and fog becomes prominent while the signals moves over 10 GHz on the spectrum. From the point of the view of signals attenuation, the clouds and fog are essentially the same atmospheric phenomenon. Based on the model in the ITU recommendation [52], for a narrow-band signal, the clouds loss L_{cloud} (unit: dB) is,

$$L_{\text{cloud}} = K(f_c, T_{\text{cloud}})Md_{3\text{D}} \tag{2.43}$$

where M is the liquid water density in the cloud (or fog) (unit: g/m^3), $d_{3\text{D}}$ (unit: km) is the T-R separation distance, f_c (unit: GHz) is the operating frequency, T_{cloud} (unit: K) is the temperature in cloud (or fog), $K(\cdot)$ (unit: (dB/km)/(g/m^3)) is the the cloud liquid water attenuation coefficient and given by,

$$K(f_c, T_{\text{cloud}}) = \frac{0.819 f_c}{(1+\eta^2)\varepsilon''} \tag{2.44}$$

where η is,

$$\eta = \frac{2+\varepsilon'}{\varepsilon''} \tag{2.45}$$

where the derivatives ε' and ε'' are given by,

$$\varepsilon' = \frac{\varepsilon_0 - \varepsilon_1}{1+\left(\frac{f_c}{f_p}\right)^2} + \frac{\varepsilon_1 - 3.52}{1+\left(\frac{f_c}{f_s}\right)^2} + 3.52 \tag{2.46a}$$

$$\varepsilon'' = \frac{(\varepsilon_0 - \varepsilon_1) f_c}{\left[1+\left(\frac{f_c}{f_p}\right)^2\right] f_p} + \frac{(\varepsilon_1 - 3.52) f_c}{\left[1+\left(\frac{f_c}{f_s}\right)^2\right] f_s} \tag{2.46b}$$

where $\varepsilon_0, \varepsilon_1, f_p, f_s$ are,

$$\varepsilon_0 = 77.66 + 103.3\left(\frac{300}{T_{\text{cloud}}} - 1\right) \tag{2.47a}$$

$$\varepsilon_1 = 0.0671 \varepsilon_0 \tag{2.47b}$$

$$f_p = 20.2 - 146\left(\frac{300}{T_{\text{cloud}}} - 1\right) + 316\left(\frac{300}{T_{\text{cloud}}} - 1\right)^2 \tag{2.47c}$$

$$f_s = 39.8 f_p \tag{2.47d}$$

2.2.3 Rain

Signals usually suffers power loss propagating during rainy days. Based on the model in the ITU recommendation [53], for a narrow-band signal, the rain loss L_{rain} (unit: dB) is,

$$L_{\text{rain}} = \alpha R^{\beta} d_{\text{effective}} \tag{2.48}$$

where $d_{\text{effective}}$ (unit: km) is the effective distance [54] and formulated as,

$$d_{\text{effective}} = \frac{d_{\text{3D}}}{1 + \frac{d_{\text{3D}}}{35\exp(-0.015R)}} \tag{2.49}$$

the variable R (unit: mm/h) is rain rate, α and β are given by,

$$\alpha = \left[\alpha_H + \alpha_V + (\alpha_H - \alpha_V)\cos^2\theta\cos 2\psi\right]/2 \tag{2.50a}$$

$$\beta = \left[\alpha_H\beta_H + \alpha_V\beta_V + (\alpha_H\beta_H - \alpha_V\beta_V)\cos^2\theta\cos 2\psi\right]/2\alpha \tag{2.50b}$$

where $\alpha_H, \alpha_V, \beta_H, \beta_V$ are coefficients, θ is the elevation angle, ψ is the polarisation tilt angle relative to the horizontal. The coefficient can be derived from,

$$\log_{10}\alpha = \sum_{j=1}^{4}\left\{a_j \exp\left[-\left(\frac{\log_{10} f_c - b_j}{c_j}\right)^2\right]\right\} + m_\alpha \log_{10} f_c + c_\alpha \tag{2.51a}$$

$$\beta = \sum_{j=1}^{5}\left\{a_j \exp\left[-\left(\frac{\log_{10} f_c - b_j}{c_j}\right)^2\right]\right\} + m_\beta \log_{10} f_c + c_\beta \tag{2.51b}$$

where a, b, c, m can be found in page 2 [53], f_c (unit: GHz) is the operating frequency, α is either α_H or α_V, β is either β_H or β_V.

Remark. *Rain loss L_{rain} does not explicitly show the dependence on the altitude value. In the later discussion, we consider rain loss is 'altitude-free'.*

2.2.4 Comparisons

Based on the reference standard atmospheres in [50], we categorise parameters as temperature, air pressure and water vapour density into summer and winter classes. With 10 km T-R separation distance, ~~6 km altitude of the user equipment~~ the user at 6 km altitude, Fig. 2.7 illustrates signals attenuation versus carrier frequency in both winter and summer scenarios. We could observe three obvious peaks for the signals attenuation due to the gaseous absorption. Moreover, the moisture in the air lifts the attenuation to some extent. The signals attenuation peak around 60 GHz is caused by the oxygen absorption, which implies that carriers near 60 GHz are not suitable for long-distance wireless transmission.

The power loss caused by signals travelling through clouds or fog is demonstrated in Fig. 2.8, with respect to the carrier frequency. The attenuation grows along with the carrier frequency, and the moist air in summer escalates the attenuation.

From Fig. 2.9 to Fig. 2.12, we discuss the factors that influence the specific attenuation caused by rain. Fig. 2.9 shows the attenuation versus the rain rate. Normally,

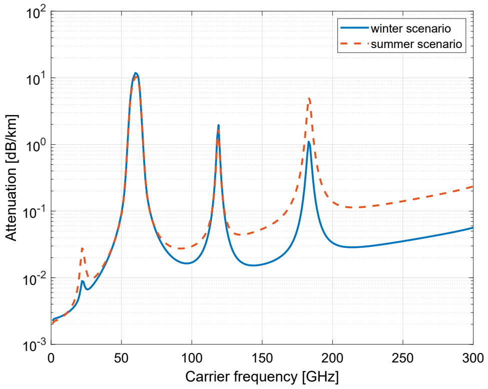


Figure 2.7 Gas absorption. Specific attenuation versus carrier frequency in winter (dry air) and summer scenarios.

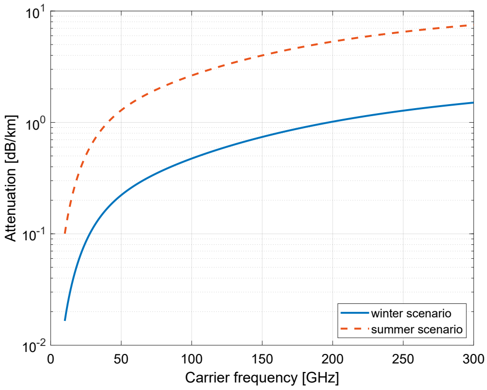


Figure 2.8 Clouds and fog. Attenuation versus carrier frequency in winter (dry air) and summer scenarios.

when the rain rate is over 50 mm/h, it is called violent rain. We investigate the signals attenuation within the span of 1 mm/h to 60 mm/h rain rate. The attenuation increase with the rainfall intensity. Fig. 2.10 shows the attenuation versus the carrier frequency. An unusual phenomenon is observed in the Fig. 2.10, that the attenuation declines after around 100 GHz carrier frequency. This may suggest that during a heavy rain (i.e., 20 mm/h), signals around 100 GHz operating frequency suffer the most among 10 GHz to 300 GHz signals.

Fig. 2.11 and Fig. 2.12 demonstrate the relationship between the signals attenuation caused by rainfall and angles. Specifically, the elevation angle refers to the angle that the path of signals propagating intersects with the direction of rain drops; the

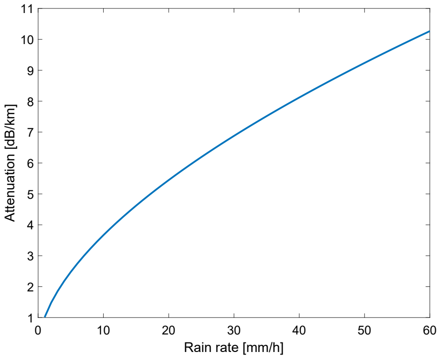


Figure 2.9 Rain effect. Attenuation versus rain rate. The elevation and tilt angles are 0 degree, the carrier frequency is 100 GHz.

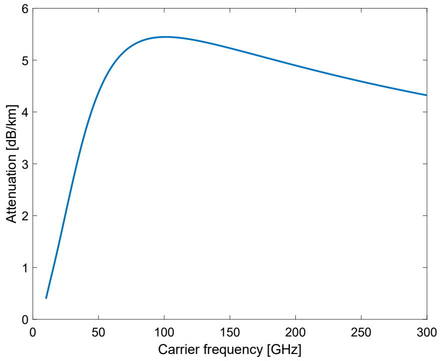


Figure 2.10 Rain effect. Attenuation versus carrier frequency. The rain rate is 20 mm/h, The elevation and tilt angles are 0 degree.

tilt angle shows the polarisation of signals transmission. Fig. 2.11 indicates that the 0 degree elevation angle leads to the maximum signals attenuation caused by rainfall. Fig. 2.12 indicates that the maximum attenuation occurs at 0 degree tilt angle.

To sum up, it is necessary to avoid 60 GHz band when designing a long-distance wireless data link; the signals suffer more path loss in a moist environment than in a dry environment; the signals attenuation caused by the rainfall weighs the most among all discussed atmospheric effects.

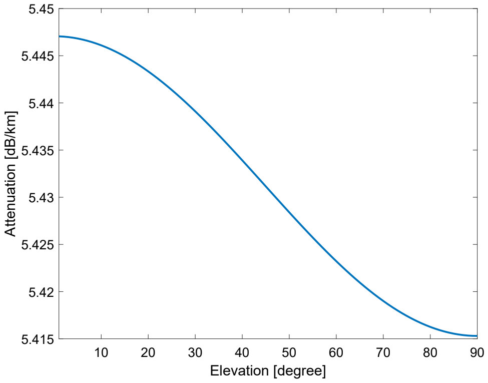


Figure 2.11 Rain effect. Attenuation versus elevation angle. The rain rate is 20 mm/h, the carrier frequency is 100 GHz.

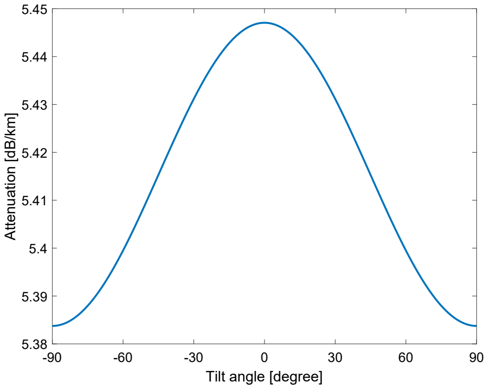


Figure 2.12 Rain effect. Attenuation versus tilt angle. The rain rate is 20 mm/h, the carrier frequency is 100 GHz.

2.3 Overall path loss model

The path where signals travel is highly likely to be a mixture of both LOS and NLOS conditions. An estimate of overall path loss could be formed by using the LOS probability,

$$PL_{\text{overall}} = PL_{\text{LOS}} p_{\text{LOS}} + PL_{\text{NLOS}}(1 - p_{\text{LOS}}) + \xi_{\text{add}} + \xi_{\text{atm}} \tag{2.52}$$

where PL_{overall} (unit: dB) denotes the mean path loss when both LOS and NLOS conditions exist, p_{LOS} is the LOS probability, ξ_{add} denotes the additional loss caused by the shadowing and fading effects, ξ_{atm} denotes the extra loss caused by the atmospheric effects.

With the definition of overall path loss, we look back the expectation of path loss predicted by the RMa and UMa models. By using the parameters in Table 2.5, Fig. 2.13 to Fig. 2.15 respectively demonstrate the overall RMa and UMa path loss versus the T-R separation distance, the carrier frequency and the altitude of the user equipment.

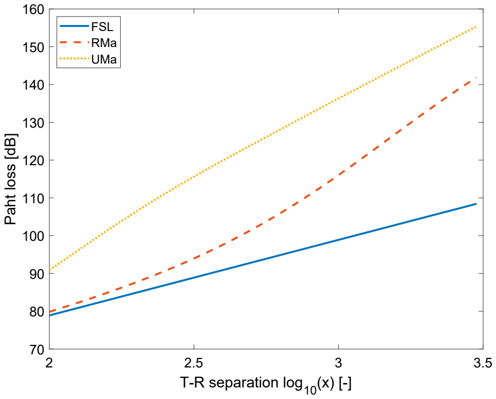


Figure 2.13 Overall path loss. The path loss versus the T-R separation distance. For the sake of simplicity, the additional loss caused by the shadowing and fading effects and the extra loss caused by the atmospheric effects are not considered here.

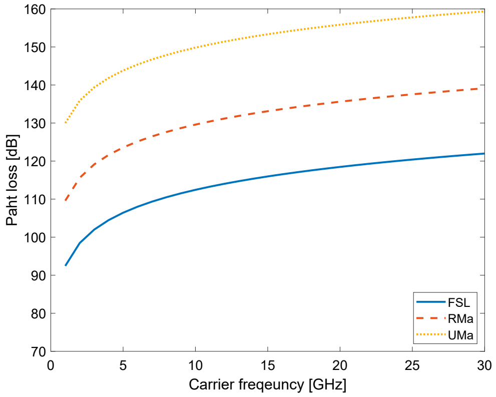


Figure 2.14 Overall path loss. The path loss versus the carrier frequency. For the sake of simplicity, the additional loss caused by the shadowing and fading effects and the extra loss caused by the atmospheric effects are not considered here.

Based on the observations on Fig. 2.15, we would like to emphasise that both RMa and UMa models predict the converging trend to the FSL model with the alti-

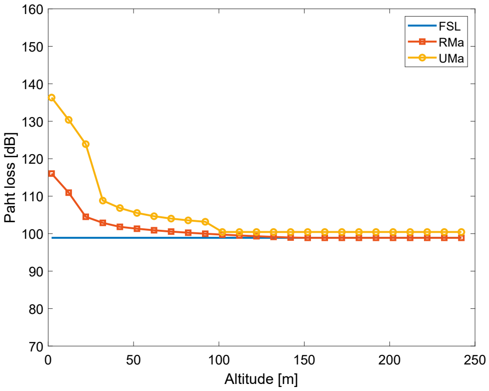


Figure 2.15 Overall path loss. The path loss versus the altitude of the user equipment. For the sake of simplicity, the additional loss caused by the shadowing and fading effects and the extra loss caused by the atmospheric effects are not considered here.

tude increasing. This fact brings up the following discussion—extending the current 3GPP RMa and UMa models to over 300 m altitude region.

A civil airborne vehicle could usually fly up to 3 km altitude, while the 3GPP RMa and UMa only cover up to 0.3 km altitude for path loss calculation. To fill the gap, with the illustration in Fig. 2.16 we propose the following strategy:

1. below 300 m altitude, the 3GPP RMa and UMa models are used;
2. above 300 m altitude, the FSL model is used. This consideration is based on two evidence:

    a. as shown in Fig. 2.15, both RMa and UMa models converge to the FSL at high altitude;

    b. as reported in [42], in both near-urban and sub-urban region, the collected measurements fit the FSL model at L-band and C-band above 504 m altitude.

Remark. *For several applications such as general aircraft or commercial aircraft or drones flying above* 300 *m, it is of interest to study channel loss models for airborne users up to* 3 *km altitude, the UMi model is not suitable in this scenario. Therefore, only RMa and UMa models are in the discussion for this section.*

For both RMa and UMa, it is complete LOS propagation when h_{UE} is over 100 m. Therefore, it is reasonable to infer LOS propagation when h_{UE} is greater than 300 m.

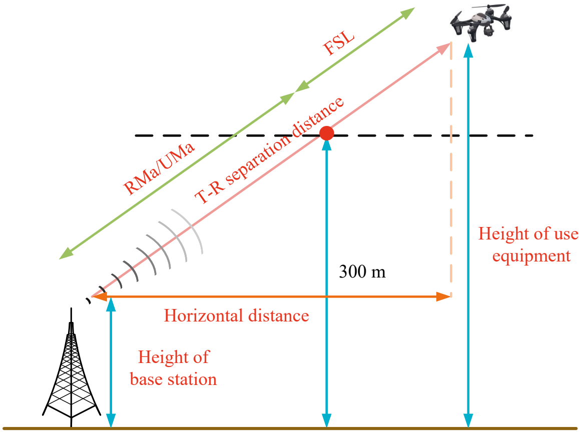


Figure 2.16 An illustration of extending 3GPP RMa and UMa models over 300 m altitude.

For the RMa scenario, if $h_{\text{UE}} > 300$ m we have,

$$PL_{\text{RMa,ext}} = 20\log_{10}\left(\frac{300 - h_{\text{BS}}}{h_{\text{UE}} - h_{\text{BS}}} \cdot d_{3\text{D}}\right) + 20\log_{10}\left(\frac{40\pi f_c}{3}\right) + 20\log_{10}\left(\frac{h_{\text{UE}} - h_{\text{BS}}}{300 - h_{\text{BS}}}\right) \tag{2.53}$$

where $PL_{\text{RMa,ext}}$ denotes the path loss in RMa when the altitude is over 300 m, with re-organisation of the above equation, we get,

$$PL_{\text{RMa,ext}} = 32.45 + 20\log_{10}(f_c) + 20\log_{10}(d_{3\text{D}}) \tag{2.54}$$

For the UMa scenario, if $h_{\text{UE}} > 300$ m, we could have,

$$PL_{\text{UMa,ext}} = 28 + 22\log_{10}\left(\frac{300 - h_{\text{BS}}}{h_{\text{UE}} - h_{\text{BS}}} \cdot d_{3\text{D}}\right) + 20\log_{10}\left(\frac{40\pi f_c}{3}\right) + 20\log_{10}\left(\frac{h_{\text{UE}} - h_{\text{BS}}}{300 - h_{\text{BS}}}\right) \tag{2.55}$$

where $PL_{\text{UMa,ext}}$ denotes the path loss in UMa, with further re-organisation of the equation, we get,

$$\begin{aligned} PL_{\text{UMa,ext}} =& 28 + 20\log_{10}(f_c) + 22\log_{10}(d_{3\text{D}}) \\ &+ 2\log_{10}(300 - h_{\text{BS}}) - 2\log_{10}(h_{\text{UE}} - h_{\text{BS}}) \end{aligned} \tag{2.56}$$

2.4 Discussion

This chapter introduces and discusses the FSL, log-distance path loss and 3GPP models as the channel models part, the gaseous absorption, clouds and fog and rain as the atmospheric effects part. Moreover, the concept of overall path loss is developed, the 3GPP RMa and UMa models are extended to cover a broader range of airborne vehicles. This chapter serves as the prerequisite knowledge for the following chapters.

In the channel models part, the highlight points are:

1. the 3GPP RMa and UMa models predict purely LOS propagation after certain altitudes passed;
2. both 3GPP RMa and UMa models converge to the FSL at high altitude;
3. the 3GPP InH model shows less signals strength loss than the FSL model in the indoor office scenario under the LOS condition.

In the atmospheric effects part, the highlight points are:

1. signals transmission suffers a large attenuation around 60 GHz band, which is due to the oxygen absorption;
2. a moist environment brings more signals attenuation than a dry environment;
3. rainfall creates the most signals power loss than other introduced atmospheric effects.

In the last, we would like to mention that the channel gain in this chapter was discussed under the assumption of the constant antenna gain. Naturally, signals at the low operating frequencies are usually transmitted by a larger antenna aperture, comparing with the antenna size used by signals at the high operating frequencies. The antenna size undoubtedly affects the channel gain, however, this consideration is not within the scope of this chapter.

3 SOLUTIONS IN COMMUNICATIONS, POSITIONING, AND SENSING

The communications are the means of exchanging information; the positioning is a cluster of techniques to geographically determine the location of a person, an subject, etc.; the sensing is a group of techniques to perceive the surroundings. The technologies of communications, positioning, and sensing have advanced for decades, they accomplish great achievements on their own path. With the rising of RF convergence thinking, the integration of above technologies become a popular topic, especially in the wireless communications society. This chapter specifically introduces both the basics and the state-of-the-art techniques in communications, positioning and sensing. Challenges in communications, positioning are addressed; novel use cases in communications are described and discussed; signal models for joint sensing and communications are proposed. Moreover, the contents of this chapter as well serves as the background knowledge for the following chapters. This chapter is related to publications [P1-P4].

3.1 Wireless communications

The wireless communications, which have long developed their capability of connectivity, accessibility and throughput, are irreversibly and profoundly shaping the paradigm of us exchanging thoughts, acquiring information, speaking opinions etc. The wireless communications, as the essential technology, are consistently motivated to move forward. For instance, the traditional terrestrial cellular networks are in extensive discussion of possible support for aerial users and merging with Industrial Internet of Things (IIoT); novel developments, such as multiple antenna system, beamforming etc., validate their applicability on these above use cases.

This section starts with use cases, followed by the addressed challenges in communications.

3.1.1 Use cases in communications

3.1.1.1 Aerial users

The Federal Aviation Administration (FAA) in [55] forecasts the domestic data: the hours flown in General Aviation (GA), commercial operations at FAA facilities and small Unmanned Aircraft System(s) (sUAS) market. The hours flown by GA are expected to increase from 25.6 million in 2019 to 29.4 million in 2041, with an average 0.6 percent per year. Particularly, the number in turbine aircraft category is forecast to grow 2.2 percent yearly. The commercial operations at FAA facilities possibly increase 3.4 percent per year. The registration number of both recreation and commercial sUAS grew rapidly in the past years, and FAA predicts that the registration number for recreation sUAS fleet continuously increases from 1.44 million units in 2020 to 1.55 million units by 2025; the registration number for commercial sUAS fleet increase 1.7 fold by 2025 than the number in 2020. The COVID-19 hits the world with setbacks in the aviation market, the statistics in the number of sUAS were addressed in [56, 57] from 1.1 million in 2017 to 2.4 million by 2022, however FAA in [55] modified the expectation in the number of sUAS to less than 2.2 million by 2022. Nevertheless, the steady growth in the market of GA and sUAS were still there during the pandemic.

Conventionally, the data links serving the aerial users are hybrid systems including satellite-based and ground-based communications. These systems are reliable but with high maintenance cost and unfriendly to emerging sUAS. With the steady growth of aerial users and their flown hours as stated by FAA forecast, the current network traffic may be soon congested. To improve the situations, the newly born 5G New Radio (NR) becomes an excellent candidate to meet the future traffic load of aerial users [58].

It is of interest to study the cellular based network infrastructure supporting civil aviation operations, especially the data links for low-altitude airborne vehicles. By the definition of the International Civil Aviation Organisation (ICAO), the GA includes all civil aviation operation. This definition is rather concise than precise, GA is commonly preferred as the subclass of Manned Aviation (MA) to the whole civil aviation.

For clarifying terms and introducing aviation to wireless communications community, our article [P1] defines the categories and sub-categories of aviation classes in Fig. 3.1.

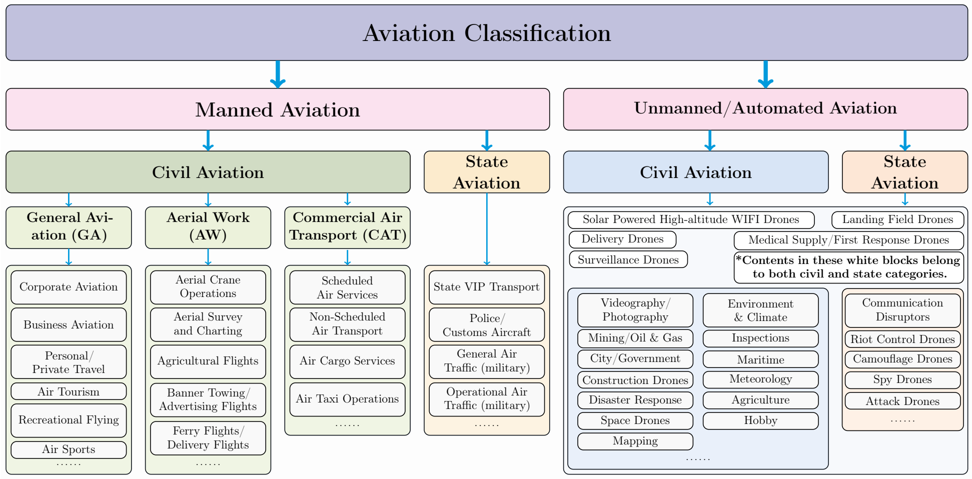


Figure 3.1 The different branches/classes in aviation category, the figure is derived from [P1].

Under the definition of aviation classes in Fig. 3.1, the contents in this work will concentrate on the low-altitude civil aviation in both MA and Unmanned Aviation (UA) categories. Currently two strategies are on the table for supporting the future air data traffic: 1) the cellular network to support aerial users and 2) the The Non-Terrestrial Networks (NTN) to enhance the transmission among aerial users. The term NTN is defined by 3GPP technical report [59], as quoted here, the NTN refers to '*Networks, or segments of networks, using an airborne or space-borne vehicle to embark a transmission equipment relay node or base station.*'

In current work, we focus on the cellular signals supporting the aerial users.

3.1.1.2 IIoT users

In the industrial site, sensors, flying drones, robots etc. via IIoT could be efficiently coordinated to improve the productivity. Especially, the flying drones possess the huge potential to boost the flexibility when applying the IIoT. Conventionally, the battery life, the connectivity and coverage of one IIoT scheme are the key indicators for the system performance. Combing with the channel models in Section 2.1, our interest lays on the approximation of coverage of a certain IIoT technology. Recently, the comparisons between cmWave and mmWave channel models for industrial robots were also addressed in [60].

As remarked in Section 2.1.3, 3GPP InF models are newly added in this thesis after the publication [P2]. In here, we create Table 3.1 with extra considerations of 3GPP InF models. The parameters used to provide the estimations in Table 3.1 were given in [P2]; all the coverage values are given at 1% outage probability. In addition, in here we replaced the industrial indoor channel loss model in [P2] with the 3GPP InF models.

Table 3.1 Coverage of different technologies.

Technology	Predicted coverage from studied models		Coverage measured or reported from literature
	worst value [m]	median value [m]	reported value [m]
NB-IoT	230	2061	1000–8000 in [61]
LoRa	731.9	1074.8	3400 in [62], 2000 in [63]
Sigfox	200	1865.2	3000–10000 in [64], 600 in [65]
Zigbee	1.1	83.6	30–50 in [66]
MIOTY	762.3	1137.5	claimed 5 km urban/ 15 km flat terrains [67]

Admittedly, the 3GPP InF models pessimistically predict the coverage of various IIoT technologies when comparing the results in Table 3.1 with results in [P2]. This inferred that different IIoT technologies suffers the limitation of indoor factory environment. In the indoor scenarios with most of the places being open area, the InH models are more preferable than InF models; the InF models are advised to use when the indoor scenarios are with many obstacles, especially metal objects.

3.1.2 Addressed challenges in communications

3.1.2.1 Outage models

The usage of millimetre Wave (mmWave) bands is a key feature in the 5G NR and beyond. To closely review the feasibility of mmWave bands for aerial users provides options for constructing the infrastructure supporting data links. Unlike most communications tasks, with respect to the airborne vehicles, we shift our main concern to command & control signals, which demand the high reliability for the data links. In addition, the study of channel models for UAV in urban environment could be seen in [68].

The outage probability could act as an indicator for the reliability. We derive the outage probability formula as the probability when the overall path loss calculated by (2.52) plus shadowing and fading is greater or equal to the maximum coupling loss MCL. Under this outage probability, the data link merely maintains connection, ergo the minimum requirement. The outage probability is expressed as,

$$P_{\text{out}} = \Pr(PL_{\text{overall}} + \xi_{\text{add}} \geq \text{MCL}) \tag{3.1}$$

where ξ_{add} denotes the additional loss caused by the shadowing and fading effects.

For the purpose of demonstration, we consider a target minimum Signal-to-Interference-plus-Noise Ratio (SINR) specified in the Long-Term Evolution (LTE) system with value being −5 dB and an achievable −30 dB SINR in the 5G NR by taking advantage of mmWave bands and Multiple-Input Multiple-Output (MIMO) gains. With detailed parameters in [P1] and channel models introduced in Section 2.1, Fig. 3.2 shows outage probability comparisons among 1 GHz, 8 GHz, 30 GHz, 60 GHz and 73 GHz frequency bands.

Clearly, in all scenarios the UMa case is with the worst reliability for data links. If we compare the centimetre Wave (cmWave) bands (i.e., 1 GHz and 8 GHz) with the mmWave bands (i.e., 30 GHz, 60 GHz and 73 GHz), under the assumptions of 25 dB interference in cmWave bands (in other words, the Signal-to-Interference Ratio (SIR) in cmWave bands is assumed to be 25 dB smaller than that in mmWave bands.), no significant difference in outage probability could be observed between the cmWave and mmWave bands. This further provides the implication of feasibility

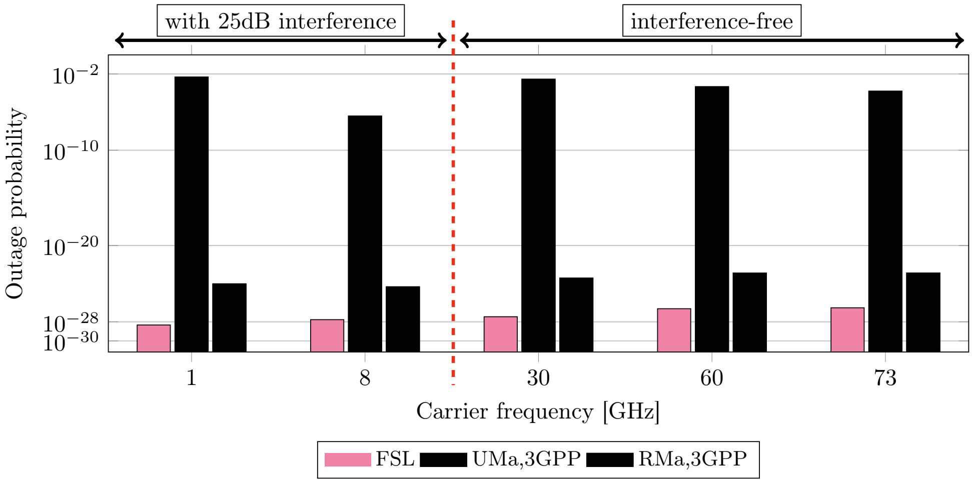


Figure 3.2 The predicted outage probability, based on the FSL and 3GPP models, the figure is derived from [P1]. Presuming the interference-free condition in mmWave bands, and 25 dB interference in cmWave bands.

using mmWave bands for the data links of aerial users, particularly the command & control signals.

3.1.2.2 3D antenna models

Along with the carrier frequency shifting from the cmWave regime to the mmWave regime, the size of the multi-antenna system constantly shrinks, therefore equipping the multi-antenna system becomes feasible for electronic devices transmitting signals in mmWave bands.

The single-antenna system is typically with fixed radiation pattern and non-steerable main lobe. In contrast, the multi-antenna system could easily change the radiation pattern and shift its main lobe. To understand this difference in depth, we introduce the concept of far-zone field, also known as beam pattern. By definition, we derive the far-zone field $B(\theta,\varphi)$ in [69] as,

$$B(\theta,\varphi)=A_{\text{ele}}(\theta,\varphi)AF(\theta,\varphi) \tag{3.2}$$

where $A_{\text{ele}}(\cdot)$ denotes the amplitude of an antenna element, $AF(\cdot)$ denotes the array factor, θ,φ are respectively the elevation and azimuth. To clear up the ambiguities on the definition of elevation and azimuth, Fig. 3.3 illustrates the spherical coordinate system in this work.

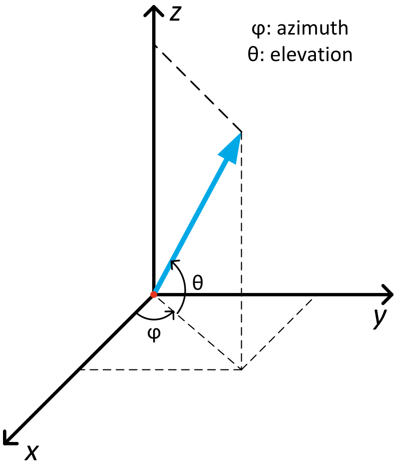
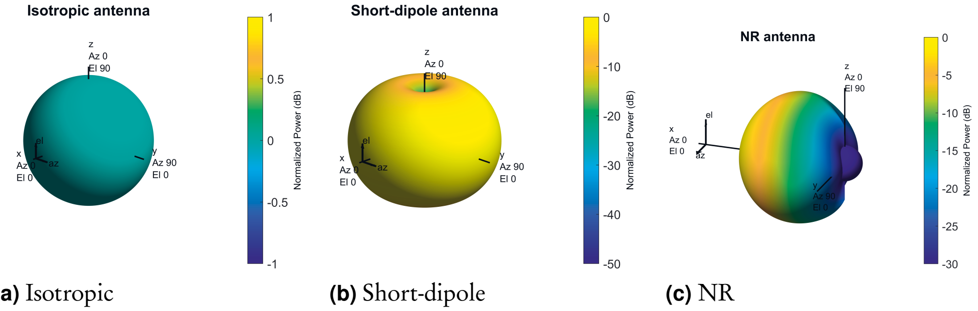


Figure 3.3 The definition of elevation and azimuth angles.

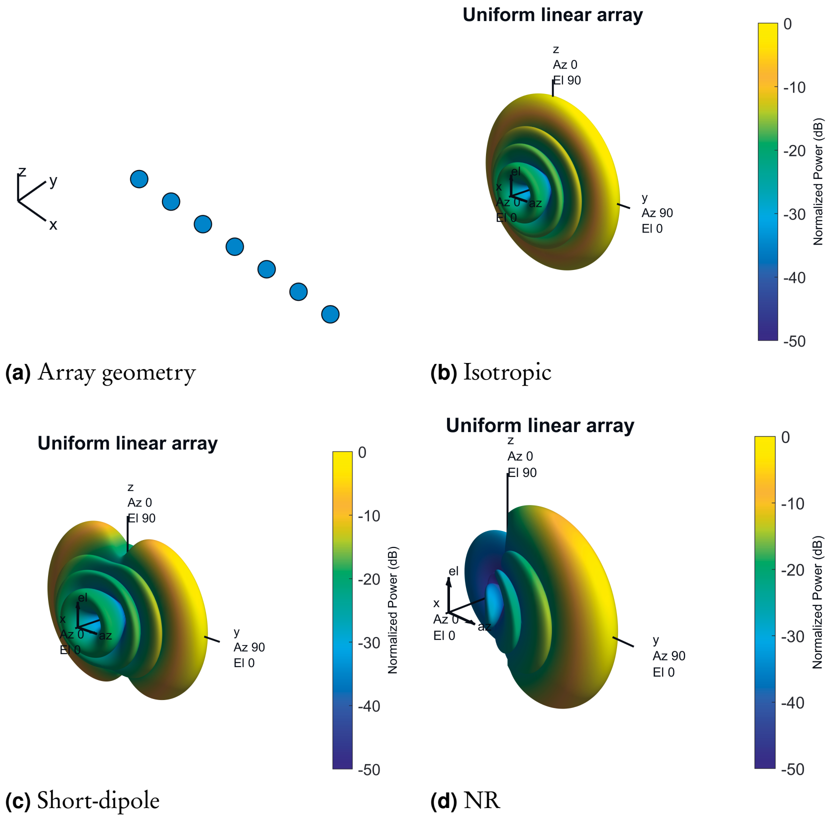
Fig. 3.4 demonstrates the radiation pattern of three different antenna types, namely the isotropic antenna, the short-dipole antenna and the NR antenna. The NR antenna, a 5G antenna, is derived from 3GPP document [38].



(a) Isotropic **(b)** Short-dipole **(c)** NR

Figure 3.4 The demonstration of radiation pattern of single-antenna system.

Fig. 3.5 and Fig. 3.6 present demonstrations for the Uniform Linear Array (ULA) and Uniform Rectangular Array (URA) respectively, using the isotropic, short-dipole and NR antenna elements. A total of eight antenna elements are deployed for both ULA and URA, particularly the URA uses 2 × 4 antenna elements layout. Comparing with the isotropic and short-dipole antenna elements, NR antenna elements shows difference in the antenna array property of be directional.



(a) Array geometry

(b) Isotropic

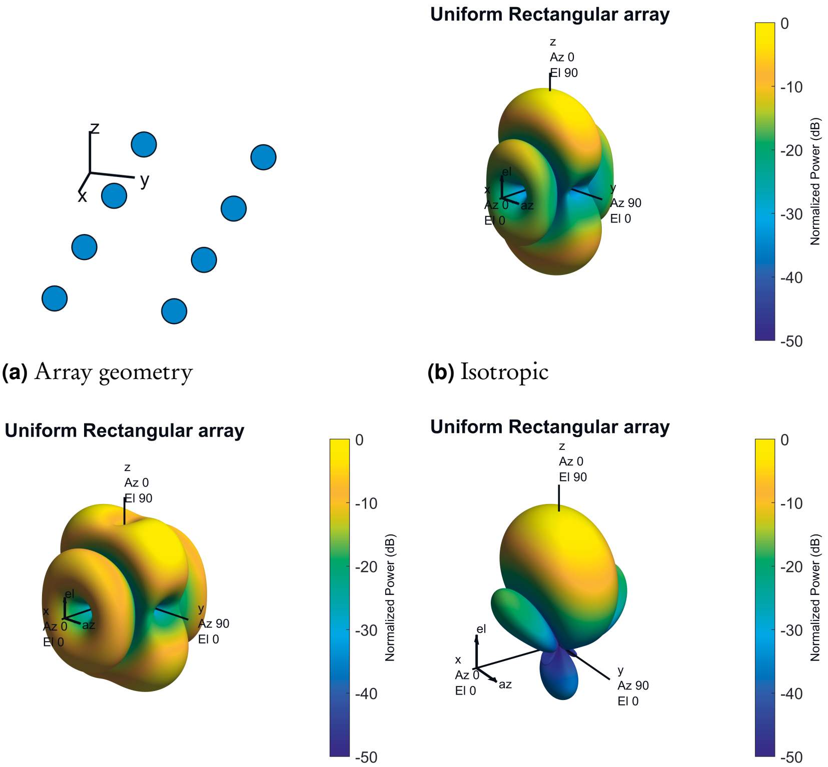
(c) Short-dipole

(d) NR

Figure 3.5 The demonstration of radiation pattern of multi-antenna system, i.e., the ULA.

The multi-antenna system brings many merits for modern communication systems. The usage of mmWave bands is often accused of high path loss, the multi-antenna system could compensate the loss by boosting the antenna gain; the air-to-ground transmission is naturally with a large amount of interference, the multi-antenna system could mitigate the interference by sophisticated design of beamforming schemes. Based on our studies, we provide the following recommendations in Table 3.2 for the design of antenna array. The recommendations are meant for one base station scenario.

The recommendations in Table 3.2 are the same for multiple base station scenarios when each base station operates independently. However, for multiple base stations operating with advanced techniques, e.g., Coordinated Multi-Point (CoMP) transmission and reception, the recommendations in Table 3.2 may not be valid.



(a) Array geometry

(b) Isotropic

(c) Short-dipole

(d) NR

Figure 3.6 The demonstration of radiation pattern of multi-antenna system, i.e., the URA.

Table 3.2 Design recommendations.

Type of beamforming	Analogue beamforming for single-user scenarios Hybrid beamforming for multi-user scenarios
Type of antenna array	URA[1]
Number of elements in URA	16×16 URA could tolerate maximum 3° angle errors in both elevation and azimuth; 8×8 URA could tolerate maximum 5° angle errors in both elevation and azimuth.
Inter-element spacing in URA	half wavelength
Size of one element in URA	The effect of size of one element is of little significance on the steering characteristics[2].

[1] For example, in 5G the base station deploys the Active Antenna Unit (AAU) with URA inside [70];

[2] see the reference [71].

3.1.2.3 Interference mitigation solutions

Unlike the traditional terrestrial networks, the support of aerial users with cellular communications faces several challenges. Amongst the main challenges, the interference becomes extra noticeable, for reasons described next. The aerial users have more chance to experience the LOS transmission than the terrestrial users do. This fact, on one hand, implies a better Received Signal Strength (RSS) for aerial users than terrestrial users; on the other hand, this indicates a stronger interference the aerial users may suffer compared to the terrestrial users.

To uncover the influence of interference in both aerial users and terrestrial users, we define the following metric of Signal-to-Interference Ratio (SIR),

$$\mathrm{SIR} = \frac{P_{rss}}{P_{int}} \tag{3.3}$$

where SIR is the SIR with linear scale, P_{rss} denotes the received signal strength (unit: Watt) and P_{int} denotes the whole incoming interference signal strength (unit: Watt).

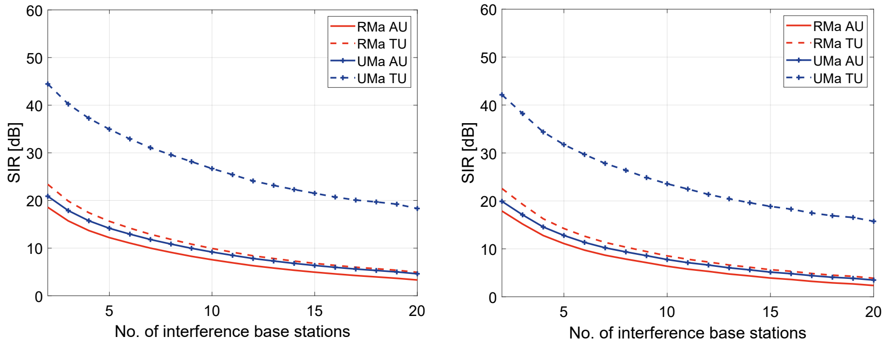
Among a group of users, their SIR values for communications is lower-bounded by a minimum value. We define a utility function $U(\cdot)$ to evaluate the level of interference when more than one users is involved,

$$U(\mathrm{SIR}^{(j)}) = \min_{j \in \mathbb{J}} \mathrm{SIR}^{(j)} \tag{3.4}$$

where $\mathbb{J}$ denotes the set containing all the users, $\mathrm{SIR}^{(j)}$ denotes the SIR of the j-th user.

Using the parameters and path-loss models proposed in [P4], the following paragraphs present the numerical analysis results for comparisons of SIR between terrestrial users and aerial users. Under Single-Input Single-Output (SISO) settings, Fig. 3.7 shows the comparisons between terrestrial users and aerial users in RMa and UMa scenarios. Both one-user and three-user cases are considered. Evidently, the aerial users suffer more from the interference than terrestrial users. If we focus on the urban area, the aerial users become even more vulnerable comparing with terrestrial users. Besides, the increase in the number of users worsens the SIR performance.

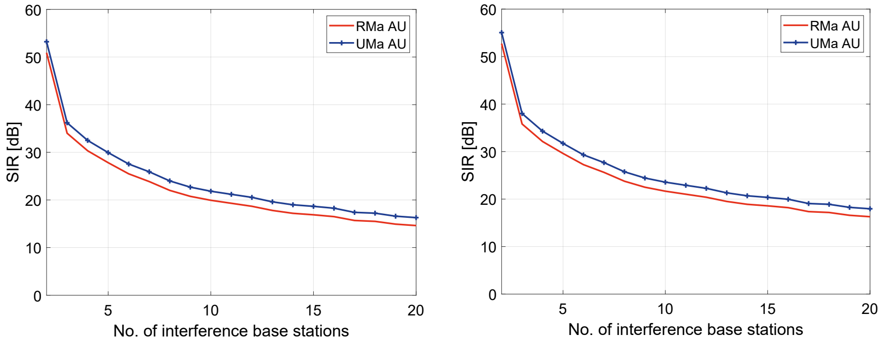
With the deployment of multi-antenna system, namely the Multiple-Input Single-



(a) one user **(b)** three users

Figure 3.7 Under SISO settings, comparisons between Terrestrial Users (TU) and Aerial Users (AU) in RMa and UMa scenarios.

Output (MISO) and MIMO, there is a silver lining for the aerial users. Fig. 3.8 presents the comparisons between MISO and MIMO schemes in RMa and UMa scenarios. It is obvious that the SIR of aerial users is uplifted; in other words, the interference aerial users suffered in SISO scheme has been mitigated to a large degree. The MIMO contributes extra few dB to the SIR in contrast with the MISO.



(a) MISO **(b)** MIMO

Figure 3.8 Comparisons between MISO and MIMO schemes in RMa and UMa scenarios. The AU is short for Aerial Users. The comparisons are for one user case.

In practice, the MISO scheme could suffice the need of aerial users for the mitigation of interference. A few extra dB improvement by the MIMO scheme will be at the cost of additional complexity for aircraft on-board communication devices.

3.2 Wireless positioning

The common positioning mechanisms [72] include the Time of Arrival (TOA) / Time Difference of Arrival (TDOA), the Angle of Arrival (AOA), the Received Signal Strength (RSS), and Dead Reckoning (DR). Using the above-mentioned techniques, currently there are two main systems performing positioning: satellite-based systems and terrestrial systems. The satellite-based systems consist of the famous Medium Earth Orbit (MEO) GNSS and Low Earth Orbit PNT solutions [73]. The terrestrial systems span a wide range of technologies: 1) the LTE network implements positioning with TDOA [74] and an indoor positioning works with mixed RSS data from WiFi and Global System for Mobile Communications (GSM) networks [75]; 2) an RSS-based indoor localisation methods using bluetooth [76]; 3) TOA-based algorithms using Ultra Wide Band (UWB) are studied in [77, 78].

3.2.1 GNSS-based positioning

The Global Navigation Satellite System (GNSS) has been developed for decades, it is successfully and vastly applied in modern electronic devices. Specifically, the GNSS nowadays is the essential part of positioning, navigation and timing services. With the rise of the GNSS markets, evil grows inside those trying to sabotage GNSS functioning. To maintain the safety of acquiring GNSS signals becomes vital to the GNSS based services.

To begin with, we briefly introduce the principles of GNSS positioning. In a Cartesian coordinate system, a location on earth could be represented by (x_u, y_u, z_u), then this location is possible to be determined by at least four satellites coordinates and their corresponding distance to this very location. In mathematical expression[79], we get the the location coordinate (x_u, y_u, z_u) by solving the following equation,

$$\rho_j = \sqrt{(x_j - x_u)^2 + (y_j - y_u)^2 + (z_j - z_u)^2} + C t_u, \quad j = 1, 2, 3, \ldots \tag{3.5}$$

where (x_j, y_j, z_j) is the location of the j_{th} satellite, ρ_j is the pseudorange measurement from the j-th satellite, C is the speed of light, t_u is the offset of the receiver clock from the system time.

In theory, with the knowledge from four satellites we could solve (3.5), hence the location of users.

3.2.2 Other modern positioning methods

The discussions on modern positioning (e.g., LEO PNT and 6G positioning) increased in the literature. The authors in [80] address that future positioning techniques in 6G should be compatible with existing 5G techniques, moreover positioning in 6G might be low-cost, low-complexity, high-accuracy and low-latency. The European Space Agency's Lionel Reis in [81] describes the LEO PNT as a very promising PNT reaching from indoors to the Moon. The research in [82] carries out Geometric Dilution of Precision (GDOP)-based analysis and concluded that current broadband LEO constellation with thousands more satellites could provide global coverage for PNT.

3.2.3 Challenges in positioning

3.2.3.1 Intentional interference

Most encountered intentional interference in GNSS are jamming and spoofing. The jamming is a straightforward attack where interference signals are generated in one or several operating frequency bands of GNSS. This kind of attack is also know as Denial of Service (DoS) attack, because the nature of jamming is to block the capability of the receiver to acquire authentic GNSS signals [41].

Regarding to the spoofing, let us imagine a scene. A sneaky but "sophisticated" spoofer is around waiting for prey, meanwhile, an "innocent" GNSS receiver comes nearby. In the blink of an eye, the location showing by a map application with the "innocent" GNSS receiver starts to deviate. But the stranger with the map application is unaware.

If we put mathematical terms for the above scene, it refers that we solve (3.5) with the spoofer-placed information. We may unconsciously solve (3.5) with one or several groups of (x_j, y_j, z_j) that actually come from the spoofer. In this sense, the user has potential to be misled by the GNSS-based services.

The spoofer, unlike the jammer, puts endeavours to mislead the users instead of blocking the GNSS-based services. With the advancement of modern electronics and signal processing, the spoofer tends to be low-cost and high-intelligence, which endangers the GNSS based services now more than ever.

3.2.3.2 Unintentional interference

As all GNSS signals travel from the space to the ground, the channel impairments, including the atmospheric effects, contribute the unintentional interference to the positioning. For example, the authors in [83] introduced a worldwide network monitoring the solar activity for the analysis of impact of ionospheric effects on GNSS performance.

In view of channel impairments, the 3GPP models and the atmospheric effects studied in Chapter 2 could serve as initial points to propose mitigation solutions for such impairments, however this work remains as an open issue for now.

3.2.4 Proposed solutions

We briefly review the current anti-spoofing techniques. The work in [40] categorises the spoofing countermeasures into four classes:

1. signal-processing-based methods
2. cryptographic-based methods
3. correlation with other GNSS sources, e.g., military code
4. antenna-based methods

The signal-processing-based methods do not need any extra modifications on current receiving mechanism. For example, the action can be done by the comparisons between local prediction of satellites locations and reported positions from the navigation message; the Doppler shift check is as well a simple but efficient countermeasure.

The cryptographic methods need to change the coding paradigm. For example, by providing the spreading code or navigation message with encryption could block the unwelcomed transmitter.

A second receiver as a reference could help to verify the authentic GNSS signals. For example, on L1 band the military code is in phase quadrature with the civilian one. Though the military code is not decoded by the civilian devices, it being out of phase with civilian code may imply that the spoofing is present. However the obvious drawback of this method is the fact that it highly relies on the fact that the reference receiver is trustworthy.

The antenna-based methods, among all the above methods, might be the most efficient and resilient one. For example, by utilising angle of arrival (AOA) discrimination, the signal from the spoofer might be identified; the multi-antenna system could null the signals coming from the low elevation angles to mitigate both terrestrial jamming and spoofing.

Our work falls into the first category: we exploit the satellite-hardware features and the channel features during satellite-to-ground transmission, thus, fingerprints can be formed to identify the spoofing signals. More details on RF fingerprinting based anti-spoofing methods are given in Chapter 4.

3.3 Wireless sensing

Integrating the sensing functions into the future cellular networks draws extensive discussions in the wireless communications community. This section briefly reviews the basics of radar technologies.

3.3.1 Signal model

In a mono-static radar system as depicted in Fig. 3.9, the reflected signal $\zeta(t)$ from the k-th target can be modelled as,

$$\zeta(t) = \sum_{k=1}^{K} x(t-\tau_k)\eta_k h_k^2 e^{j2\pi D_k t} + \xi S_{\text{int}} + S_{\text{clutter}} + \omega(t) \tag{3.6}$$

where $x(t)$ is the transmitted signal, τ_k and D_k are respectively the time delay and Doppler shift from the k-th target, h_k^2 is the channel loss of round-trip for the k-th target, η_k is the *voltage reflectivity* [1] of the k-th UE target, S_{int} is the instant radiating signal from the transmitter, ξS_{int} is the self-interference residual, S_{clutter} characterises clutter, $\omega(t)$ denotes the radar receiver additive Gaussian noise.

[1] voltage reflectivity is a term used in [84] that is related to the radar cross-section (RCS) of the target.

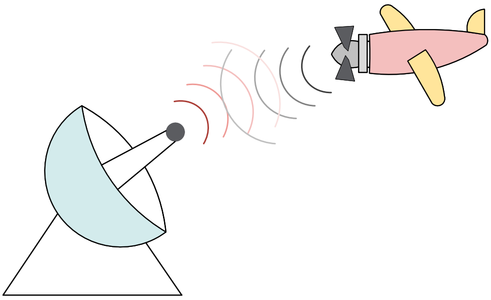


Figure 3.9 The demonstration of mono-static radar. A radar station is responsible for both transmitting and receiving signals, hence locating the target.

With the reflected echoes, the radar firstly processes it through whitening filter, then through the matched filter, as shown in Fig. 3.10. The whitening filter removes the clutter S_{clutter} and makes the Gaussian noise white. The outputs of whitening filter feed into the matched filter and this maximises the Signal-to-Noise Ratio (SNR) at a certain time delay relating to the range.

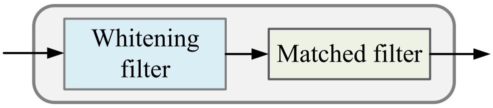


Figure 3.10 The process of radar receiving.

Ideally, the term self-interference residual ξS_{int} could be eliminated in the received signals and the Doppler shift is as well cancelled in advance. The reflected echoes $\zeta(t)$ for the k-th target after the whitening filter reduces to,

$$\zeta^{(k)}(t) = \eta_k h_k^2 x(t - \tau_k) + n(t) \tag{3.7}$$

where $n(t)$ is $w(t)$ after whitening filter, $n(t) \sim \mathcal{N}(0, \sigma_n^2)$, σ_n^2 is the power of noise.

3.3.2 Matched filter

Assuming the Doppler shift is cancelled in advance, the response of matched filter is in the following form [84],

$$h_{\text{MF}}(t) = x^*(-t), \quad 0 \le t \le \Delta T \tag{3.8}$$

where $(\cdot)^*$ denotes the complex conjugate, ΔT denotes the process duration. Applying convolution between inputs and response of matched filter, we could get the outputs of matched filter for the k-th target,

$$z(t) = \int_{0}^{\Delta T} \zeta(\tau) x^*(\tau - t) \mathrm{d}\tau \tag{3.9a}$$

$$z^{(k)}(t) = \int_{0}^{\Delta T} \Big\{ x(\tau - \tau_k) \eta_k h_k^2 + n(t) \Big\} x^*(\tau - t) \mathrm{d}\tau \tag{3.9b}$$

where τ is a dummy variable.

When $t = \tau_k$ meets, the (3.9b) becomes,

$$z^{(k)}(\tau_k) = \eta_k h_k^2 \int_{0}^{\Delta T} |x(t)|^2 \, \mathrm{d}t + n(t) \int_{0}^{\Delta T} x^*(\tau - t) \mathrm{d}\tau \tag{3.10}$$

by defining the energy of radar signals over duration ΔT as E_r,

$$E_r = \int_{0}^{\Delta T} |x(t)|^2 \, \mathrm{d}t \tag{3.11}$$

the (3.9b) becomes,

$$z^{(k)}(\tau_k) = \eta_k h_k^2 E_r + n(t) \int_{0}^{\Delta T} x^*(\tau - t) \mathrm{d}\tau \tag{3.12}$$

We could consider (3.12) as,

$$z^{(k)}(\tau_k) \sim \mathcal{N}(\mu_z, \sigma_z^2) \tag{3.13a}$$

$$\mu_z = \eta_k h_k^2 E_r \tag{3.13b}$$

$$\sigma_z^2 = \sigma_n^2 E_r \tag{3.13c}$$

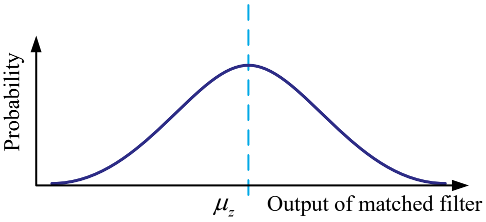


Figure 3.11 The output of matched filter.

As shown in Fig. 3.11, the output of matched filter follows Gaussian distribution with the mean value being μ_z.

Remark. *The Doppler shift in the echoes carries sensing information, for the purpose of simplicity, we assume that the Doppler shift is cancelled in advance in this section.*

3.3.3 Detection rate and false alarm rate

Often, there are two hypotheses in the output of matched filter: no target is present and a target is present. These two opposing hypotheses are conventionally marked as $\mathscr{H}_0$ and $\mathscr{H}_1$:

$$\mathscr{H}_0 : \text{no target is present}$$
$$\mathscr{H}_1 : \text{a target is present}$$

where $\mathscr{H}_0$ and $\mathscr{H}_1$ are called *null hypothesis* and *alternative hypothesis*.

In the mathematical form, considering (3.13), we could write $\mathscr{H}_0$ and $\mathscr{H}_1$ as:

$$\mathscr{H}_0 : \mathcal{N}(0, \sigma_z^2) \tag{3.14}$$
$$\mathscr{H}_1 : \mathcal{N}(\mu_z, \sigma_z^2) \tag{3.15}$$

the above two hypotheses could be visualised in Fig. 3.12, meanwhile, we could define the detection rate and false alarm rate by the assistance of Fig. 3.12. λ_{th} denotes the threshold.

Given a threshold λ_{th}, the detection rate could be expressed by using Q function,

$$P_{\text{D}} = \text{Q}\Big(\frac{\lambda_{\text{th}} - \mu_z}{\sigma_z}\Big) \tag{3.16}$$

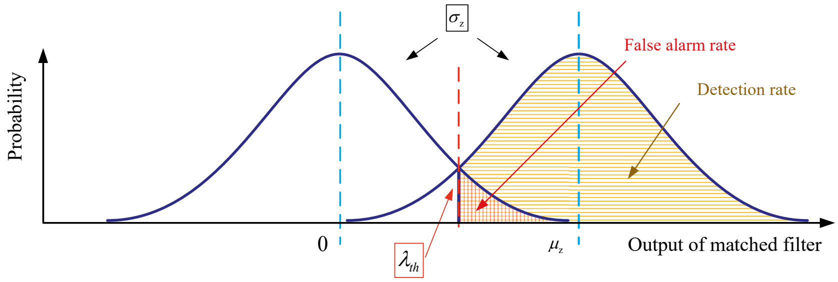


Figure 3.12 The hypothesis testing, detection rate and false alarm rate. Blue dashed lines represent the mean values, red dashed line represents the threshold.

where Q function is the tail probability of standard normal distribution and defined as,

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_{x}^{\infty} e^{\left(-\frac{u^2}{2}\right)} \mathrm{d}u \tag{3.17}$$

in the similar way, the false alarm rate yields to,

$$P_{\mathrm{F}} = \mathrm{Q}\left(\frac{\lambda_{\mathrm{th}}}{\sigma_z}\right) \tag{3.18}$$

In practice, the maximum false-alarm rate, as the tolerance of a system, is normally in the requirement for a designer. The threshold and the detection rate could be computed accordingly.

3.3.4 Parameter estimation

Provided the reflected echoes, let the unknowns being the parameters to be estimated, we are able to get the sensing information, such as the range, the velocity etc. For example, to estimate the time delay (i.e., equivalent to the range), we have,

$$\hat{\tau}_k = P(\tau_k | \zeta^{(k)}(t)) \tag{3.19}$$

The estimation of parameters in radar signal processing with an unbiased estimator has the minimum, which is often represented by the Cramér-Rao lower bound

(CRLB). We formulate the CRLB for the estimation of time delay as,

$$\mathbb{E}\left[(\hat{\tau}_k - \tau_k)^2\right] \geq \frac{1}{\mathbb{E}\left\{\left[\frac{\partial}{\partial \tau_k} \log L\left(\zeta^{(k)}(t); \tau_k\right)\right]^2\right\}} \tag{3.20}$$

where $\mathbb{E}(\cdot)$ is the expectation operator, $L\left(\zeta^{(k)}(t); \tau_k\right)$ is the likelihood function of τ_k, and whose logarithm form could be determined by,

$$\ln L\left(\zeta^{(k)}(t); \tau_k\right) = C_{\text{const}} - \frac{1}{2\sigma_n^2}\left(\zeta^{(k)}(t) - \eta_k h_k^2 x(t - \tau_k)\right)^2 \tag{3.21}$$

where C_{const} is a constant irrelevant to the variable t. We could further get the partial derivative,

$$\frac{\partial}{\partial \tau_k} \log L\left(\zeta^{(k)}(t); \tau_k\right) = -\frac{\eta_k h_k^2}{\sigma_n^2} n(t) x'(t - \tau_k) \tag{3.22}$$

substituting (3.22) into (3.20),

$$\mathbb{E}\left[(\hat{\tau}_k - \tau_k)^2\right] \geq \frac{\sigma_n^4}{\eta_k^2 h_k^4} \cdot \frac{1}{\mathbb{E}\left\{\left[x'(t - \tau_k)\right]^2\right\}} \tag{3.23}$$

where the term $\mathbb{E}\left\{\left[x'(t - \tau_k)\right]^2\right\}$ is system dependent.

3.4 Discussion

This chapter specifically reviews the status quo and advancements in communications, positioning, and sensing technologies. In a similar manner to Chapter 2, this chapter also serves as the background knowledge for the following chapters.

Regarding the communications aspects, the main points have been as follows:

1. Two use cases are presented, namely the aerial users and IIoT;
2. The mmWave bands are validated to be reliable for control & command signals of aerial users by numerical analysis, the coverage is predicted through 3GPP models and compared with reported measures from literature;
3. Novel techniques, such as the multi-antenna system and interference mitigation, are discussed;

4. A New NR antenna element from [38] was studied in the context of multi-antenna systems;
5. The MISO scheme is proved to be efficient on interference mitigation for aerial users scenarios by numerical analysis.

Regarding the positioning aspects, the main points have been as follows:

1. The principles of GNSS positioning and spoofer are briefly introduced;
2. A short summary of anti-spoofing techniques is presented.

Regarding the sensing aspects, the main points have been as follows:

1. A detailed signal model is given under the assumption of mono-static radar scenario;
2. The matched filter, detection and false alarm rates, and parameter estimation are respectively discussed and a simplistic model is used for the discussion.

The next 3 chapters describe in more details the novel algorithms and methods proposed in this thesis work.

4 PHYSICAL LAYER SECURITY IN GNSS

The GNSS module is fast becoming the basic building block in more and more modern wireless electronic devices. A large number of life-critical applications, such as autonomous cars and drone taxis, already depend or will depend on the GNSS functionalities. Consequently, securing GNSS Position, Navigation and Timing (PNT) meets the best interest of many existing and unborn applications.

Two major evil-doings against the GNSS implementation are out there: the jamming and spoofing. Spoofing and jamming concepts have already been defined in Section 3.2. This chapter puts focus on the study of the anti-spoofing methods.

There are many existing discussions corresponding to the anti-spoofing techniques in the literature. A cross-check on the location of satellites between the prediction from ephemeris data and external sources hints the presence of spoofing [85]; the Navigation Message Authentication (NMA), being a scheme that uses public key to assure the receiving authentic navigation message, enhances the resilience of GNSS receivers to the spoofing [86–89]. Moreover, Galileo has started to test the Open Service Navigation Message Authentication (OSNMA) [90]. Antenna-based countermeasures were explored to resist spoofing attack in [91–93].

As one variant of signal processing methods, in the following we exploit the RF fingerprinting techniques in GNSS to perform the spoofing countermeasure. The RF fingerprinting methods have the potential of high robustness as they are based on direct raw data, which is harder to pamper with than any other data such as navigation data (e.g., the method of comparing ephemeris data with external source in [85]). This chapter covers publications [P5, P6].

4.1 RF fingerprinting techniques

For most of the time, the RF fingerprinting refers to a cluster of techniques putting endeavours identifying the transmitters, channels, and/or receivers through their unique and inherent features, by the assistance of newly emerging machine-learning methods. In a stricter sense, also adopted in this thesis, the RF fingerprinting particularly means the identification of a transmitter or emitter (e.g., if it is genuine or not). However, many recent papers use the RF fingerprinting terminology in the context of location estimation based on channel characterisation. Without a further specification, the term RF fingerprinting in this thesis is in the strict sense by default.

The RF fingerprinting techniques have been applied in many scenarios: Wi-Fi signals in [94] and ZigBee signals in [95] are respectively studied in the Internet of Things (IoT) domain; the detection of fake base station is performed in the cellular system [96]; the Automatic Dependent Surveillance–Broadcast (ADS-B) signals in [97] and controller signals in [98] are respectively studied in aviation domain.

Though the RF fingerprinting techniques are not newly developed concepts, a comprehensive study of implementing the RF fingerprinting techniques in the GNSS, especially for the purpose of anti-spoofing, was still lacking at the moment when we started our work on this thesis.

4.2 RF fingerprinting in GNSS

The RF fingerprinting in GNSS, different from in other systems, rely on the following characteristics of GNSS systems: i) transmitters uninterruptedly broadcast signals; ii) the Global Positioning System (GPS), Galileo and Beidou use code-division multiple access (CDMA), Global Navigation Satellite System (GLONASS) uses frequency-division multiple access (FDMA); iii) the GNSS satellites are equipped with high-end electronics, unlike spoofers, which usually rely on less costly electronics; iv) there is a limited number of GNSS satellites in the space; v) genuine GNSS signals experience a space-to-ground propagation, unlike spoofers, which are usually installed on terrestrial platforms, and thus experience ground-to-ground propagation. Based on the above facts in GNSS, in the following sub-sections, we study the transmitters structures and the receiver chains for genuine GNSS and spoofer GNSS transmitters, propose various RF fingerprinting techniques and RF fingerprinting based position, velocity and time (PVT) solution.

4.2.1 Navigation payload

To closely examine the architecture of GNSS signals transmitters, we would be able to reveal the difference in the hardware impairments (also known as RF fingerprints) between a GNSS satellite and a GNSS spoofer. Based on [P5] [99, 100], we built the block diagram in Fig. 4.1 to describe a generic architecture of a transmitter for GNSS signals.

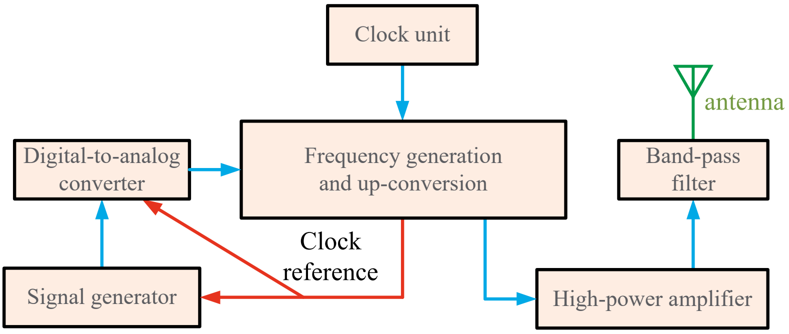


Figure 4.1 A generic architecture description of a transmitter for GNSS signals, valid for both satellites and spoofers. The differences lie in the hardware traits of the illustrated blocks. The red arrows indicate the signals do not carry extra 'fingerprints' from the previous unit; the blue arrows imply that the signals carry extra 'fingerprints' from the previous unit. Derived from [P6].

Inside a GNSS satellite, the clock unit shown in Fig. 4.1 typically consists of multiple atomic clocks—one active and the rest as the redundancy; for example, rubidium atomic frequency standards and passive hydrogen masers are used in the Galileo system [101]. By contrast, a typical GNSS spoofer has no budgets for expensive atomic clocks; for example, an over €10000 Universal Software Radio Peripheral (USRP) RIO series software-defined radio (SDR) uses an Oven Controlled Crystal Oscillator (OCXO).

A Digital-to-Analogue Converter (DAC) unit exists in both the genuine and spoofer GNSS signal transmitters, but the GNSS satellites are very likely with a better non-linearity and lower phase noises DAC than common spoofers. During the up-conversion processing, GNSS satellites could easily do the job with a lower level of phase noises and I/Q imbalance than spoofers do. The High Power Amplifier (HPA) in GNSS satellites is commonly capable of amplifying signals with a better linearity and less frequency-dependent variations than an adequate power amplifier typically used in spoofers. As for the last stage before the antenna radiating, GNSS satellites are equipped with band-pass filters characterised by flat response of desired band signals and steep cut-off, whereas spoofers are with less steep cut-off ranges. The hardware impairments differences existing in satellites and spoofer set the ground of RF fingerprinting in GNSS as they produce distinctive features for each transmitter.

4.2.2 Receiver chain

During the GNSS signals receiving, there are several stages to carry out the RF fingerprinting techniques as shown in Fig. 4.2. Taking the correlator as the reference, we deliberately selected two stages, namely the pre-correlation domain and the post-correlation domain, in the receiver chain to collect samples for the implementation of the RF fingerprinting. The choice to focus only on pre- and post-correlation stages was motivated by a lack of literature addressing these domains, as most GNSS anti-spoofing mechanisms in the literature focused on navigation techniques [102, 103]. The samples for the pre-correlation domain are right from the Analogue-to-Digital Converter (ADC) outputs, i.e., the I/Q raw data; while the samples for the post-correlation domain are from the acquisition outputs, i.e., the correlation outputs.

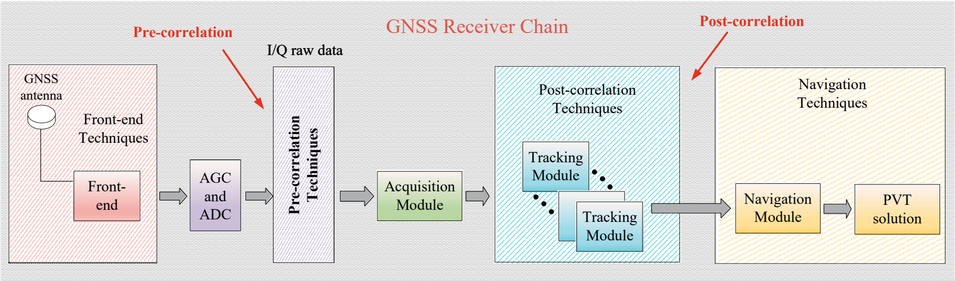


Figure 4.2 The GNSS receiver chain, where the pre-correlation and post-correlation domains are defined. Derived from [P5].

4.2.3 Pre-correlation method

With the I/Q raw data as the samples, the pre-correlation methods utilise a conceptual 'classifier' to identify whether the spoofer signals are mixed within or not. We design the conceptual 'classifier', depicted in Fig. 4.3, as a combination of feature extractor and machine learning methods, the abbreviations in Fig. 4.3 are listed here: Discrete Wavelet Transform (DWT), Teager–Kaiser Energy Operator (TKEO), Support Vector Machine (SVM), K-Nearest Neighbours (KNN), Linear Discriminant Analysis (LDA). Section 4.2.1 described various inherent hardware features in the GNSS signals transmitters, it is rational to infer that some features are more distinguishable than others. The feature extractor 'picks out' the distinguishable features, then feeds to the machine learning method processing.

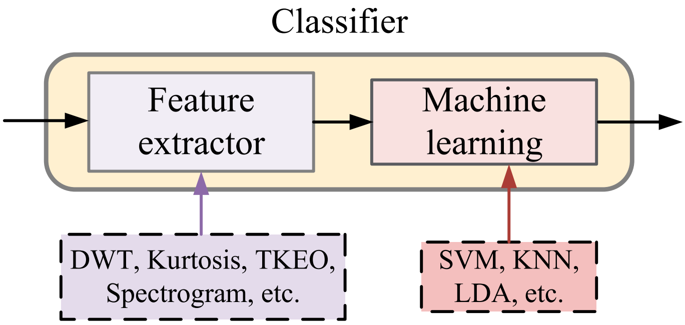


Figure 4.3 The conceptual classifier in pre-correlation methods. Examples of feature extractor are DWT, kurtosis, TKEO and spectrogram; examples of machine learning methods are SVM, KNN and LDA.

4.2.3.1 Feature extractor

Common feature extractors are Discrete Wavelet Transform (DWT) [104], kurtosis [105], Teager–Kaiser Energy Operator (TKEO) [106] and spectrogram [107].

Discrete Wavelet Transform A DWT decomposes the signals into detail and approximation coefficients. The detail coefficients are given by though a high-pass filter and the approximation coefficients through a low-pass filter. In mathematical expression, with an incoming complex signal $r[k]$ (i.e., I/Q raw samples) in discrete form we respectively have approximation and detail coefficients,

$$y_{\text{approx}}[n] = \sum_{k=-\infty}^{+\infty} r[k]h_{\text{low}}[2n-k] \tag{4.1a}$$

$$y_{\text{detail}}[n] = \sum_{k=-\infty}^{+\infty} r[k]h_{\text{high}}[2n-k] \tag{4.1b}$$

where $h_{\text{low}}[\cdot]$ and $h_{\text{high}}[\cdot]$ respectively denote the discrete low-pass filter and high-pass filter, $y_{\text{approx}}[n]$ and $y_{\text{detail}}[n]$ respectively denote the approximation and detail coefficients.

Kurtosis The kurtosis metric is a measure of non-Gaussianity for random variables. If the random variables strictly follow normal distribution, the kurtosis of the random variables is exactly equal to 3. The kurtosis is calculated by,

$$\text{kurtosis}\Big\{r[k]\Big\} = \mathbb{E}\left\{\left[\frac{r[n]-\mathbb{E}(r[n])}{\text{std}(r[n])}\right]^4\right\} \tag{4.2}$$

where std$(\cdot)$ is the standard deviation operator, and $\mathbb{E}(\cdot)$ is the mean operator.

Teager–Kaiser Energy Operator The TKEO is typically used to estimate the instantaneous energy of an incoming signal, in RF fingerprinting it could be a useful tool to reveal the hidden features in the signals power or energy. The TKEO of a complex signal $r[k]$ is defined [108],

$$\text{TKEO}\Big\{r[k]\Big\} = |r[k]|^2 - \frac{1}{2}\Big(r^*[k+1]r[k-1] + r[k+1]r^*[k-1]\Big) \tag{4.3}$$

where $r^*[k]$ is the complex conjugate of $r[k]$.

Spectrogram The spectrogram is a time-frequency analysis of signals, it is usually calculated by applying Short-Time Fourier Transform (STFT). For N_w samples, the STFT is given by,

$$\text{STFT}(f_c, m) = \sum_{k=1}^{N_w} r[k]\text{win}[k-m]\exp(-j2\pi f_c k) \tag{4.4}$$

where win[$\cdot$] is a time window function (e.g., Hann window, etc.). The spectrogram is the squared absolute value of the STFT outputs,

$$\text{spectrogram}(f_c, m) = |\text{STFT}(f_c, m)|^2 \tag{4.5}$$

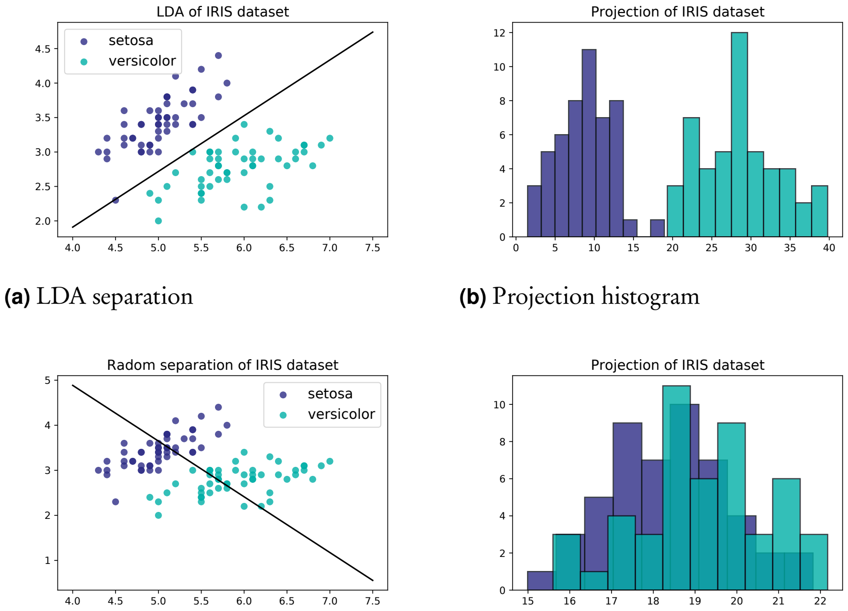
4.2.3.2 Machine-learning methods

The machine-learning methods have largely gotten attentions in the recent years, simple but efficient methods, such as Support Vector Machine (SVM), K-Nearest Neighbours (KNN), Linear Discriminant Analysis (LDA), etc., are candidates in our considerations.

Support Vector Machine The SVM, as a supervised learning method, is deigned to maximise the margin between or among classes. The boundaries between or among classes are determined by the 'support' vectors formed by a few samples. The SVM could be versatile by exploiting the 'kernel trick', details about the 'kernel trick' can be found in publication [P5].

K-Nearest Neighbours The KNN, also as a supervised learning method, is probably the simplest machine learning method in contrast with other existing methods. The principle of KNN is straightforward: for each new sample, a search of k nearest neighbours is implemented, the class of the new sample is then determined by the majority of searched k nearest neighbours. Details and examples of KNN can be found in [P5] as well.

Linear Discriminant Analysis The LDA, another supervised learning method, is a machine learning method with a closed form solution. The basic ideas of this approach is plain: a projection of samples is found such that the separation of classes could be maximised. The formula of LDA could be easily found in literature, for example in [109]. Fig. 4.4 demonstrates the comparisons between LDA separation and random separation using IRIS data [110]. Clearly the LDA tries its best to separate the setosa samples from versicolor samples, the corresponding histogram as well validates that the LDA projects samples into two very separated distributions. The LDA is not included in the simulations in [P5], due to its vulnerability to the non-linear separation of data.



(a) LDA separation

(b) Projection histogram

(c) Random separation

(d) Projection histogram

Figure 4.4 Comparisons between LDA separation and random separation, corresponding projection histogram is on the right side.

Principal Components Analysis In practice, the machine learning methods mentioned above suffers from the curse of dimensionality [111]. To tackle this problem, one feasible way is to pre-process data so that the dimension of samples could be reduced. The Principal Components Analysis (PCA) is a commonly used algorithm to reduce dimension of samples, during PCA process the first few principle components represent the most dominant features inside the samples.

4.2.4 Post-correlation method

In the post-correlation domain, each moderate or higher quality signals within the mixture could be picked out. Theoretically by applying RF fingerprinting techniques one is able to identify which signal/signals in the mixture is/are from the spoofer/spoofers at this stage.

The conceptual classifier for the post-correlation methods has a similar mechanism as in Fig. 4.3, except that the correlator has already acted as the feature extractor. Therefore, the feature extractor in the pre-correlation methods is not needed here, a machine learning method is directly applied on the outputs of the correlator.

4.2.5 Anti-spoofing based PVT solution

We emphasise the capabilities and possible corresponding countermeasures of pre-correlation and post-correlation methods here:

- **pre-correlation:** can identify whether the spoofer signal/signals is/are mixed within the received signals; the countermeasure is to deny receiving incoming signals if spoofing is detected, then to look for alternatives of PVT solution. The main limitation of a pre-correlation method is that it is not able to identify which pseudorandom code comes from a spoofer or not, as all data from all transmitters is available only in a mixed form at pre-correlation stage. Another limitation can be the very low signal-to-noise ratio of the received signal in I/Q domain.
- **post-correlation:** can identify which signal/signals in the mixture of the received signals is/are from the spoofing; the countermeasure is to remove the identified spoofing signal/signals and to continue to form PVT solution with the remaining signals.

Under the different merits of pre-correlation and post-correlation methods, a preliminary RF fingerprinting based anti-spoofing PVT solution is proposed in Fig. 4.5. The prediction results of pre-correlation and post-correlation methods are compared and synthesised to suggest a group of authentic GNSS signals. With these signals, the PVT solution is eventually formed.

Remark. *There exist possibilities that prediction results between pre-correlation and post-correlation methods in Fig. 4.5 contradict to each other. The black box from in Fig. 4.5 is assumed to include a set of strategies that utilise the prediction results to determine the authentic GNSS signals, hence to form the PVT solution and this is still a topic open to research.*

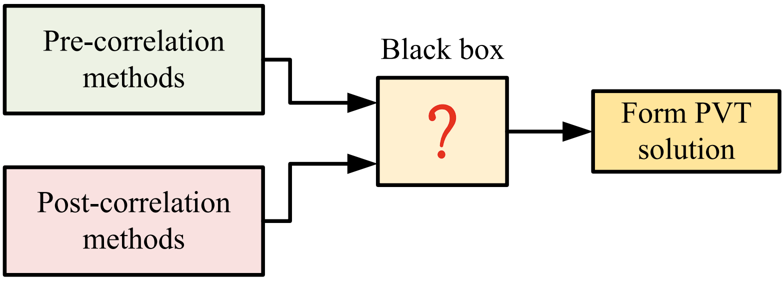


Figure 4.5 The RF fingerprinting based anti-spoofing PVT solution.

4.3 Measurements-based testing

To verify the proposed pre-correlation and post-correlation methods, two measurement campaigns were respectively carried out by project partners in Nottingham, UK and us in Tampere, Finland. Additionally, an open-access measurements from Nuremberg, Germany provided by [112] is as well included for the study.

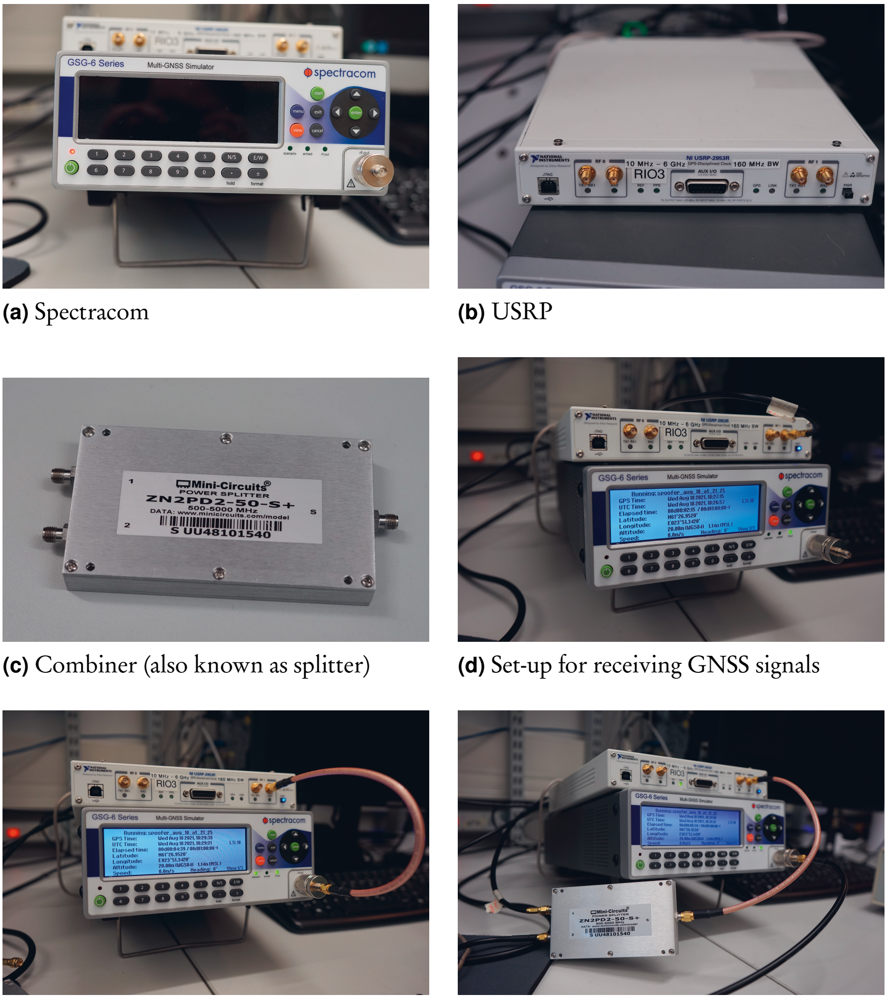
4.3.1 Measurement campaigns

The measurement campaigns aimed at validating the RF fingerprinting techniques on classifications among the following three classes:

1. pure GNSS signals;
2. pure spoofer signals;
3. mixture of GNSS and spoofer signals.

The pure spoofer signals here are ideal cases of spoofing event, which will be hardly possible in real life. However, the pure spoofer signals are necessary measurements to answer the question whether the spoofer signals could be differentiated from the authentic GNSS signals via RF fingerprinting techniques.

In the Tampere measurements we collected in our lab, based on a Spectracom GSG-64 GNSS signal generator shown in Fig. 4.6a acting as the spoofer, a Tallysman TW3972 antenna is mounted above the roof to receive GNSS signals, and a USRP RIO 2954R SDR shown in Fig. 4.6b is used as the receiver to collect samples. In other two measurements (i.e., in Nottingham and Nuremberg), the Spirent signal generator acted as the spoofer. Three different lab setups are corresponding to the above mentioned three classes: the pure GNSS signals samples are collected in the setup shown in Fig. 4.6d; the pure spoofer signals samples are collected in the setup shown in Fig. 4.6e; the mixture of GNSS and spoofer signals samples are combined and collected in the setup shown in Fig. 4.6f.



(a) Spectracom

(b) USRP

(c) Combiner (also known as splitter)

(d) Set-up for receiving GNSS signals

(e) Set-up for receiving spoofer signals

(f) Set-up for receiving GNSS+spoofer signals

Figure 4.6 The lab equipment and setups for measurement campaigns in Tampere, Finland.

Remark. *The transmitting signals power in Spectracom generator is adjusted so that the Carrier-to-Noise Ratio (CNR) of 'spoofing' signals could blend in the CNR of GNSS signals in the air.*

In the post-correlation methods in the mixture (i.e., GNSS+spoofer) class, the number of remaining satellites, which are after the removal of detected spoofer signals, needs to exceed four to perform a proper positioning. This considerations echoes to the design of measurement campaigns in our lab, that the first six strongest signals (i.e., in terms of CNR) are picked up from the incoming signals. The Space Vehicle IDentifier (SV ID) of selected signals are listed in Table 4.1. In the GNSS and spoofer classes, we selected the first four strong signals for classifications; in the mixture class, the first six strong signals were selected. The mixture class is missing in the Nuremberg open-access measurements. In both Nottingham and Tampere measurements, only one spoofer signal is mixed within the ’GNSS+spoofer’ class. We remind readers that Table 4.1 aims at providing information: i) the power of spoofer signals is adjusted to be comparable with the received GNSS signals; ii) no single signal could be picked out in the pre-correlation methods, hence the table is mainly for the post-correlation study.

Table 4.1 SV ID of selected signals (with C/N_0).

		SV ID (corresponding C/N_0 [dB-Hz])
Nottingham	GNSS	2 (45.26), 25 (50.14), 29 (50.45), 31 (48.05)
	spoofer	12 (49.95), 25 (51.72), 29 (51.50), 31 (51.07)
	GNSS+spoofer	2 (42.81), 25 (49.12), 26 (44.54), 27 (49.04), 29 (50.30), 31 (49.87)
Nuremberg	GNSS	1 (47.04), 4 (49.48), 20 (49.53), 23 (49.29)
	spoofer	10 (47.94), 26 (47.51), 27 (48.15), 28 (46.90)
	GNSS+spoofer	not available
Tampere	GNSS	3 (37.82), 19 (35.49), 22 (36.88), 31 (35.81)
	spoofer	3 (35.52), 17 (35.50), 19 (34.85), 31 (36.66)
	GNSS+spoofer	1 (34.60), 3 (36.60), 12 (35.72), 19 (34.18),22 (35.54), 31 (33.92)

* we only list the first four strong signals in GNSS and spoofer classes, the first six strong signals in GNSS+spoofer class;
** we marked the spoofer signal within the mixture using blue colour.
*** we marked the C/N_0 values with red colour.

Additionally, the sampling frequency in Nottingham, Nuremeberg and Tampere measurements were 25 MHz, 20 MHz and 25 MHz respectively; the quantisation in the ADC were 16 bits/sample, 8 bits/sample and 16 bits/sample respectively.

4.3.2 Spoofer identification

With the samples collected in the measurement campaigns, in the following we implement the pre-correlation and post-correlation methods. The classification results of pre-correlation methods are shown in Table 4.2. The feature extractor uses DWT, kurtosis, spectrogram and TKEO, the machine learning method uses SVM with the radial basis function as the kernel. The PCA is always applied before SVM to reduce the dimension of samples, the grid search method helps to find the fine tuning of parameters in the SVM method. From the results, it is clear that a combination of spectrogram and SVM could classify the three classes with the best prediction accuracy, namely mean accuracy 80.06% in Nottingham measurements, 99.99% in Nuremberg measurements, and 97.03% in Tampere measurements. A thorough analysis on the results of pre-correlation methods is presented in [P6].

Table 4.2 Classification results of pre-correlation methods, results are given as accuracy [%].

Feature extraction	**Measurements**								
	Nottingham			Nuremberg			Tampere		
	GNSS	spoofer	G+S	GNSS	spoofer	G+S	GNSS	spoofer	G+S
DWT	69.91%	99.98%	49.37%	95.91%	100.00%	N/A	98.58%	4.15%	74.24%
(mean value [%])		73.09%			97.76%			58.99%	
Kurtosis	33.55%	39.10%	31.14%	48.47%	51.78%	N/A	94.82%	93.45%	99.55%
(mean value [%])		34.60%			50.13%			95.94%	
spg	67.58%	100.00%	72.60%	100.00%	99.99%	N/A	93.50%	99.94%	97.66%
(mean value [%])		80.06%			99.99%			97.03%	
TKEO	8.07%	84.20%	13.70%	96.40%	18.67%	N/A	92.70%	75.13%	40.49%
(mean value [%])		35.32%			57.54%			69.44%	

[*] G+S represents the mixture class (i.e., GNSS plus spoofer signals), spg represents the spectrogram.

The post-correlation methods exploit the hidden features in the outputs of correlator, the SVM together with the PCA is used to perform classifications. The post-correlation methods face a more complicated situation than the pre-correlation methods: i) the 'classifier' could learn from the GNSS and spoofer classes then differentiate them; ii) or learn from the GNSS and spoofer classes then perform classifications in the mixture class. Apparently, in the second scenario after the training phase, the 'classifier' model has only a partial information on the mixture class, and the links between the samples and the labels are not sufficiently known to the 'classifier' training model. In our publication [P6], we spilt the post-correlation methods into two cases: the *benchmark comparison* and *advanced comparison*. The *benchmark comparison* answers the question whether the GNSS and spoofer signals could be differentiated in the post-correlation domain; while the *advanced comparison* helps to explore more practical situation—classifications in the aggregation of GNSS and spoofer signals when partial knowledge on the features of GNSS and spoofer signals are known to the 'classifier' model.

The results of classifications for the *benchmark comparison* is shown in Table 4.3. In all three measurements, the GNSS and spoofer signals are identified with relatively high probability.

Table 4.3 Mean classification accuracy [%] results, benchmark comparison.

	Measurements		
	Nottingham	Nuremberg	Tampere
GNSS	84.38%	87.05%	69.64%
spoofer	91.06%	87.10%	76.34%

The *advanced comparison* is very challenging since its mission is to find each authentic GNSS signal, or to detect the individual spoofer signal then to remove it. We adopt strategies in the *advanced comparison* as described in [P6], however none of them works perfectly, more discussions could be found in [P6].

4.4 Discussion

With the predictable booming integration of GNSS functionalities in the modern electronics, especially the life-critical applications, the assured resilience in GNSS PNT is desired. Many methods to achieve the resilience goal have been proposed, as reviewed at the beginning of this chapter. We particularly study the RF fingerprinting techniques in this regard, due to its excellent performance in other platforms and lacking comprehensive research. Resilience to interferences translates into robust positioning mechanisms and are expected to be some of the main backbones of future RF convergence solutions.

The RF fingerprinting is proved viable—both pre-correlation and post-correlation methods need no extra modifications to the structures and protocols of a typical GNSS receiver, and effective—both pre-correlation and post-correlation methods could differentiate the spoofer signals from the GNSS signals with a good classification accuracy.

The current study establishes the paradigm how the RF fingerprinting techniques could be applied in GNSS area for the physical layer security purpose. Its preliminary results set the ground for the further developments of RF fingerprinting techniques in GNSS. Examples of future possible developments are:

1. The study of the transfer learning or unsupervised learning in post-correlation *advanced comparison*;
2. The implementation of a mature RF fingerprinting based anti-spoofing PVT solution;
3. A combination of data fusion techniques with RF fingerprinting techniques.

Remark. *This chapter focuses the introduction of RF fingerprinting and its feasibility on GNSS anti-spoofing applications. In practice, there are diverse spoofing techniques and the spoofing methods themselves keep evolving, the usage of machine learning methods in RF fingerprinting will need further investigations. The publication [P5] covers more discussions on the different learning methods.*

5 POSITIONING-AIDED COMMUNICATIONS

Nowadays in most wireless communications devices, the location information has become easily acquired via GNSS or cellular/5G technologies. The use of the available location information has large potentials to benefit the wireless communications, in terms of data rate, reliability and latency. The authors in [113] suggest the usage of location information could improve the data rate in IIoT system, the research in [34] shows the advantages of using location-based beamforming comparing with the Channel State Information (CSI) based beamforming, the work in [114] infers that by the assistance of location information the CSI-based beamforming could be improved in the aspect of latency.

Conventionally, many researchers use the CSI-based beamforming techniques. One way to implement the CSI-based beamforming is to use the MUltiple SIgnal Classification (MUSIC) to estimate the AOA, then to steer the antenna radiation angle by considering the channel being reciprocal. In this chapter, based on [P7] the novel location-based beamforming is introduced, discussed and compared with the CSI-based beamforming. Location-enhanced communications tasks are expected to be more and more used in the context of RF convergence in future wireless communications.

5.1 Location-based beamforming

The multiple-antenna system (or MIMO) has been introduced in Chapter 3; one important role of MIMO is to perform beamforming. This section introduces and discusses the location-based beamforming. The location-based beamforming needs a few prerequisites to implement:

- The location information should be always available, or alternatively be estimated in real time;

- The tracking algorithm is able to implement for the prediction of location in the next time instant.

If we assume a simple scenario depicted in Fig. 5.1, a base station transmits to an aerial user with the location-based beamforming technique. The antenna array employed in the based station, at the current time instant, radiates as the red colour lobe; the user moves and, meanwhile, a tracking algorithm at the base station predicts the location of the user at the next time instant and the antenna array steers angle accordingly, i.e., the blue colour lobe. Last but not least, the tracking algorithm adapts the new location information of the user through communications. Due to the inevitable errors in both the tracking algorithms and the location information, the steering angle could be hardly aligned with the ground truth, i.e., the green colour dashed lobe.

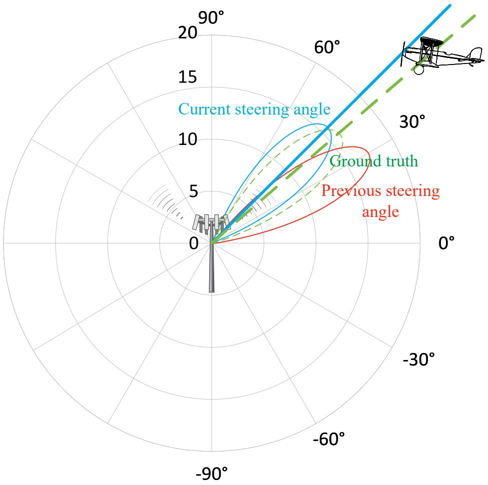
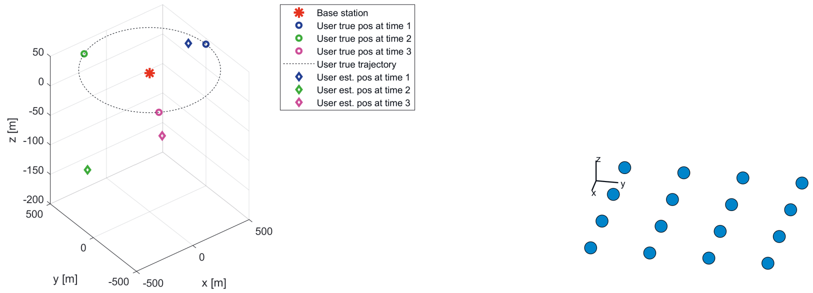


Figure 5.1 An example how the location-based beamforming works. The red lobe denotes the steering angle in last time instant, the blue lobe denotes the current steering angle, the green lobe with dashed line denotes the ground truth, where the antenna should radiate towards in the moment.

The errors, caused by the tracking algorithms and the location information, could be equivalently seen as the angle errors. As shown in Fig. 5.1, the angle error is illustrated by the angle between the blue colour solid line and the green colour dashed line. Obviously, provided a certain antenna array, the angle errors have a major impact on the performance of location-based beamforming. We will demonstrate how the angle errors affects the directivity of an antenna array. The scenarios and an

URA 3D geometry are shown in Fig. 5.2. In Fig. 5.2a, the red star is the base station, the circle markers with different colours represent the true location of the user at various time instants, the diamond markers with different colours represent the predicted location of the user at various time instants.. A 4 × 4 URA is used in the demonstration as shown in Fig. 5.2b.



(a) Scenario

(b) URA

Figure 5.2 The scenarios of demonstration and URA 3D geometry.

The results of the demonstration are shown in Fig. 5.3 and Fig. 5.4, respectively with no angle errors present and angle errors present. Comparing the Fig. 5.3b with Fig. 5.4b, the directivity difference caused by the angles errors could reach 4.4 dB, which infers that the angle errors could cause a large loss in the directivity of antenna array. The optimisation of configuring URA is necessary in the location-based beamforming techniques.

5.1.1 Optimisation of URA

Assuming the URA is configurable, it would be of interest to investigate that given an angle error, how the the directivity behaves with different number of antenna elements. A numerical analysis is performed with the parameters in Table 5.1, the results are shown in Fig. 5.5.

We observe from Fig. 5.5 that, given an angle error, with the growth of antenna element numbers the directivity of the URA increases then declines after a certain point. For a 5° angle error, an 8 × 8 URA could provide the best directivity; for a 2° angle error, an 32 × 32 URA brings the best directivity.

Typically, the angle errors are possibly to be estimated before the design of wire-

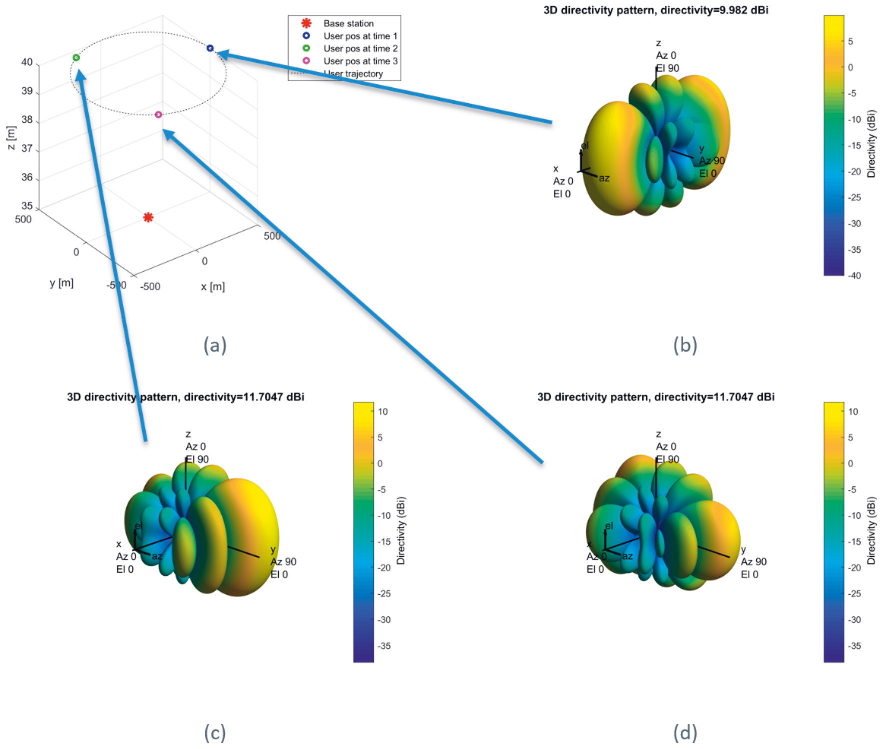
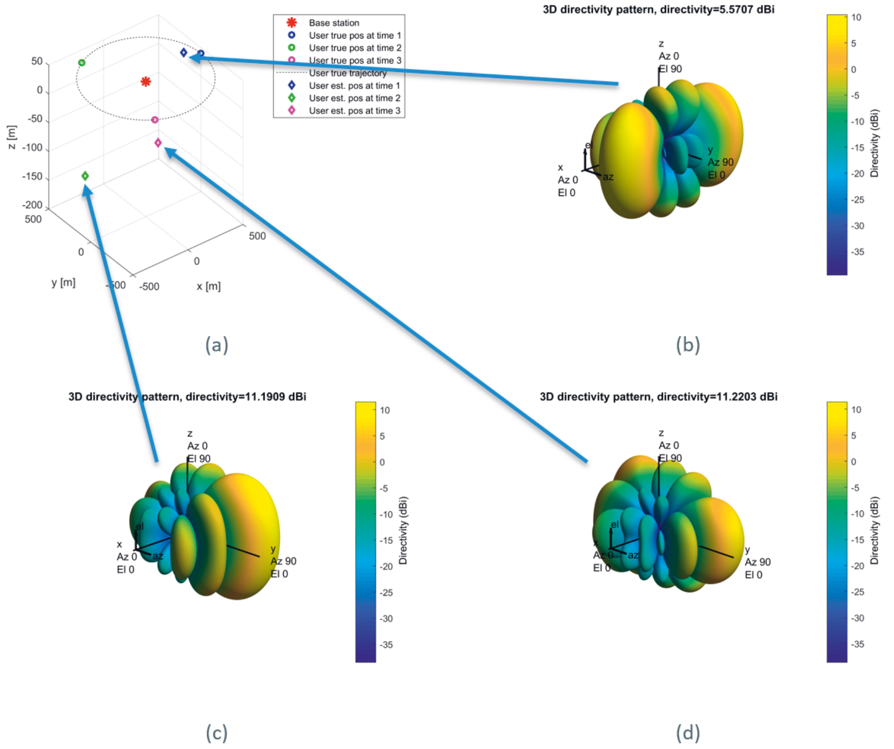


Figure 5.3 The directivity of an 4×4 URA when no angle errors are present.

Table 5.1 Prediction results (mean value), benchmark comparison

Parameters	Values
URA size	$2^n \times 2^n \quad (n = 1, 2, \ldots, 6)$
Angle errors in both elevation and azimuth	2° or 5°
Carrier frequency	1.9 GHz
Inter-element spacing	half wavelength



(a)

(b)

(c)

(d)

Figure 5.4 The directivity of an 4×4 URA when angle errors are present. The location errors follow $\mathcal{N}(0, 50^2)$ (unit: m) in the horizontal direction, and follow $\mathcal{N}(0, 100^2)$ (unit: m) in the vertical direction.

less communications system. The number of antenna elements in URA can then be chosen wisely.

5.1.2 Comparisons of beamforming techniques

Considering the Time Division Duplex (TDD) scheme, [P6] compares the proposed location-based beamforming with CSI-based beamforming techniques. The CSI-based beamforming technique uses MUSIC algorithm to estimate AOA in this study.

A numerical analysis is carried out for the comparisons, details of simulation design, parameters and results could be found in [P6]. Two metrics, namely the Shannon capacity and outage probability, are compared between the CSI-based beamforming and location-based beamforming techniques. To conclude, in 'noise-free' situation, the two beamforming techniques show similar performance in both capac-

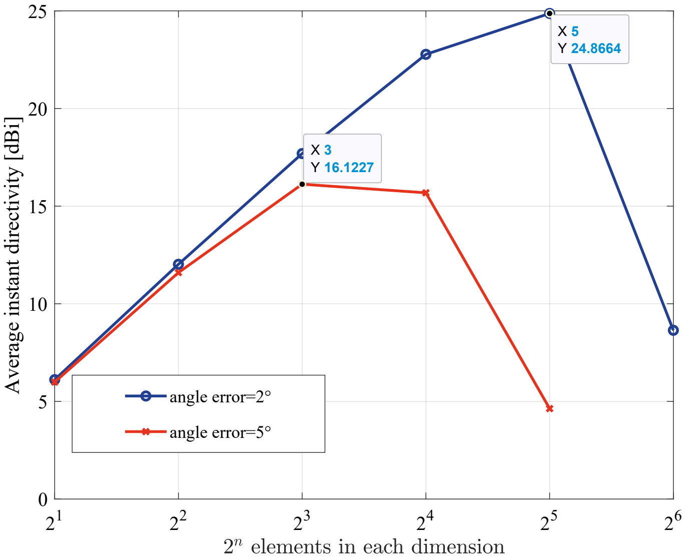


Figure 5.5 The directivity versus the number of antenna elements, under two different angle errors.

ity and reliability (i.e., low outage probability); in 'noisy' environment, the location-based beamforming, with either small angle errors or large angle errors, beats the CSI-based beamforming, in terms of capacity and reliability.

5.2 Discussion

Since the location information becomes accessible in almost every wireless communications device, the utilisation of the location information would benefit the wireless communications. The location-based beamforming was proposed and discussed in this chapter.

The location-based beamforming is heavily influenced by the errors that might be caused by the inaccurate location information and tracking algorithms. As an example, a proper design of URA could alleviate this influence via high directivity provided by antenna array. Moreover, the directivity is related to the beam solid-angle of the main lobe of the radiation. It could be approximated as $D_{\max} = \frac{\pi^2}{\theta_E \times \theta_H}$. If the angle is 0.3 rad, it means that at a distance of 300 meters, the aperture of the main lobe will be about 90 meters by 90 meters.

Comparing with traditional beamforming techniques, for instance the CSI-based beamforming, the location-based beamforming shows better performance in the 'noisy' environment; besides, the location-based beamforming naturally has good performance in the latency metric.

6 JOINT SENSING AND COMMUNICATIONS

Our generation witnesses the fast-paced evolution of cellular-based wireless communications, especially the advance in 5G and beyond in the field of cellular technologies. The operating frequency bands move into the mmWave domain in the spectrum, which engages the heavy congestion of spectrum with existing legacy radar bands. According to a document [115] published by the National Telecommunications and Information Administration, the United States Department of Commerce, most radars operate between 400 MHz and 36 GHz. To tackle the above issue, the joint sensing and communications scheme, also referred to as the Integrated Sensing And Communications (ISAC), recently has drawn intensive attentions in both academia and industrial. The work in [15] points the vast potential use cases for the joint sensing and communications, for examples, the automated vehicles and the medical applications. The authors in [19] explore closely the waveform design and signal processing in joint sensing and communications for Vehicle-to-Vehicle (V2V) scenarios. In medical applications, the research in [116] proposes an architecture of cloud based human body sensing system. The 60 GHz bands are viable for wireless communications [117] as well as the reusing in imaging aspects [118].

Amid the fast evolved joint sensing and communications technologies, the waveform design is one of the most exciting research areas. In the systems that employ the Institute of Electrical and Electronics Engineers (IEEE) 802.11ad protocol, authors in [119] and [120] respectively investigate the preamble in a single-carrier physical layer frame and the signals in beamforming training for sensing purpose, the sensing and communications will then perform in time division fashion. Within the Orthogonal Frequency-Division Multiplexing (OFDM) scheme, the authors in [121] propose a structure that for an OFDM symbol subcarriers are split into communications and sensing parts. In the MIMO system, while the research work in [122] suggests the projection of the sensing signals on the null space for the coexistence of sensing and communications.

In this chapter, a novel proposal for waveform design is introduced and discussed. This Chapter covers [P8].

6.1 Superposition coding scheme

The superposition coding scheme, which could be traced back to the 3GPP standard document [123], is a well developed approach in wireless communications system. We adopt this strategy for the waveform design in the joint sensing and communications system. Let us consider a mono-static radar system illustrated in Fig. 3.9, the resource blocks are allocated in the power domain as shown in Fig. 6.1. As an example in Fig. 6.1, two users share the same time-frequency resources but they are assigned with different levels of power.

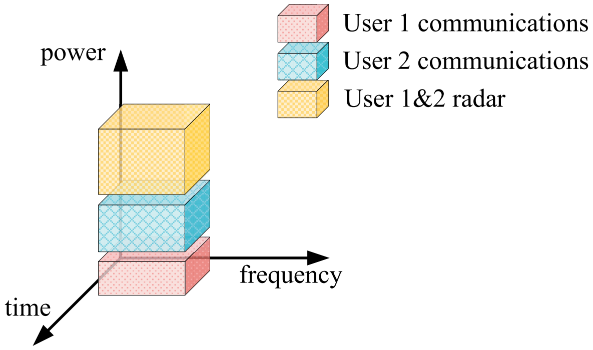


Figure 6.1 The allocation of resource blocks in the superposition coding scheme. This example considers two users with simultaneous sensing and communications.

Under the proposed superposition coding scheme, considering the following hypotheses:

1. the downlink communications;
2. any two users are not collinear with the base station;
3. all nodes are assumed to be SISO;
4. the radar signals are known to all users as well as to the base station.

then, the total transmitted signals $S(t)$ can be modelled as,

$$S(t) = \sum_{k=1}^{K} \alpha_k s_k(t) + \beta x(t) \tag{6.1}$$

where $s_k(t)$ is the communications signals and α_k^2 is the corresponding power allocation coefficient, $x(t)$ is the radar signal and β^2 is the corresponding power coefficient. The coefficients α_k^2 and β^2 abide by the following constraint,

$$\sum_{k=1}^{K} \alpha_k^2 + \beta^2 \leq 1, \quad \alpha_k, \beta \in [0,1], \quad \forall k = 1, \ldots, K \tag{6.2}$$

the above constraint guarantees the sum of assigned power will not exceed the maximum transmitting power.

6.1.1 Signal processing in communications part

During the signal processing in the communications part, the mechanism illustrated in Fig. 6.2 is applied. Using the local radar signal replica to assist the removal of radar signal, the receiver then implements SIC process to boost the SINR of desired communications signals.

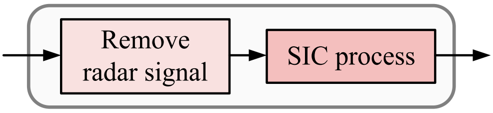


Figure 6.2 The communications signal processing of superposition coding at the user devices.

The instant signal $y(t)$ at the k-th user receiver is,

$$y(t) = |h_k| S(t) + n_k(t) \tag{6.3}$$

where $|h_k|^2$ is the channel gain from the base station to the k-th user and treated as constant during signal transmitting, $n_k(t)$ is the additive white Gaussian noise for the k-th user receiver.

Without loss of generality, let us assume the following order for channel gains,

$$|h_1|^2 > |h_2|^2 > \cdots > |h_k|^2 > \cdots > |h_K|^2 \tag{6.4}$$

to employ SIC at each user receiver, the power allocation coefficients need to follow,

$$\alpha_1^2 < \alpha_2^2 < \cdots < \alpha_k^2 < \cdots < \alpha_K^2 \tag{6.5}$$

Given the assumption $\mathbb{E}(|s_k|^2) = 1$, the SINR γ of the first user is given by,

$$\gamma_1 = \frac{\alpha_1^2 |h_1|^2}{\sigma_1^2} \tag{6.6}$$

the SINR of the k-th user is,

$$\gamma_k = \frac{\alpha_k^2 |h_k|^2}{|h_k|^2 \sum_{i=1}^{k-1} \alpha_i^2 + \sigma_k^2}, \quad 1 < k \leq K \tag{6.7}$$

6.1.2 Signal processing in radar part

As shown in Fig. 6.3, the reflected echoes will first go through the whitening filter to remove clutter[1]. Due to the availability of the SIC functionalities at the base station, the radar signal processing has the degree of freedom to choose either to remove the communications signals components mixed within the received superposed codes, or to treat the communications signals components as the interference. Last, the matched filter will apply to boost the SNR of the received radar signals.

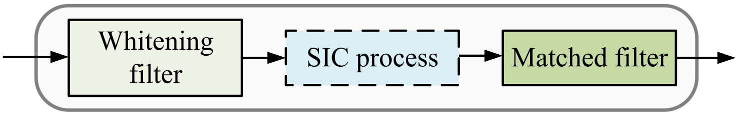


Figure 6.3 The radar signal processing of superposition coding at the base station.

For simplicity and without any loss of generality, the Doppler shift in the reflected echoes is considered as cancelled in advance. Now, the reflected signals $\zeta(t)$ are given by,

$$\zeta(t) = \sum_{k=1}^{K} x(t - \tau_k)\eta_k h_k^2 + \xi S_{\text{int}} + n(t) \tag{6.8}$$

where η_k is the voltage reflectivity, τ_k is the time delay for the k-th user, $n(t)$ is an additive white noise, $n(t) \sim \mathcal{N}(0, \sigma_n^2)$, σ_n^2 is the power of noise.

[1] the clutter usually refers to the unwanted echoes from ground, buildings, etc.

6.1.3 Optimisation problem

The performance of a wireless communications system is often evaluated by the Shannon capacity, whilst the radar system commonly uses the estimation metrics, for example, the CRLB. The parameter estimation of radar system, particularly the time delay, has been discussed in Section 3.3.4; the following will only give the capacity in communications.

For a downlink communications with K users, under the superposition coding scheme, the total capacity R_{sum} is bounded by,

$$R_{\text{sum}} \leq \sum_{k=1}^{K} \log_2(1+\gamma_k) \tag{6.9}$$

In the publication [P8], we proposed to consider the optimisation problem of a joint sensing and communication system as two sub-problems, for the reason that so far there are no existing universal metrics to measure these two systems. In a two users scenario, the above mentioned two sub-problems, as derived from the publication [P8], are listed here,

$$\begin{aligned} \max_{\alpha_1,\alpha_2} \quad & R_{\text{sum}} \\ \text{s.t.} \quad & \alpha_1^2+\alpha_2^2 \leq 1-\beta^2, \\ & R_2 \geq R_{0,2} \end{aligned} \tag{6.10}$$

$$\begin{aligned} \min_{\alpha_1,\alpha_2,\beta} \quad & \sigma_\epsilon^2 \\ \text{s.t.} \quad & \alpha_1^2+\alpha_2^2 \leq 1-\beta^2, \\ & R_2 \geq R_{0,2}, R_1 \geq R_{0,1} \end{aligned} \tag{6.11}$$

where $R_{0,2}, R_{0,1}$ are the minimum rate to guarantee the Quality of Service (QoS) for user 2 and user 1 respectively. σ_ϵ^2 is equivalent to $\mathbb{E}\big[(\hat{\tau}_k - \tau_k)^2\big]$ in Section 3.3.4, β^2 is treated as a parameter, given a certain tolerance of radar estimation error, we would like to achieve the sum rate maximum.

The solution of sub-problems could be found in [P8]. The results imply that superposition coding scheme is suitable for airborne users joint sensing and communications, a moderate QoS for users' wireless communications is recommended.

Remark. *The problems in* (6.10) *and* (6.11) *could be further considered in the context of multi-objective optimisation, i.e.,* $\max(R_{\text{sum}}, -\sigma_\epsilon^2)$*. The solution could be dealt with Pareto optimality.*

6.2 Detection rate comparisons

Let us consider a scenario depicted in Fig. 6.4, a base station implements both the communication and detection tasks. As a possible use case, the detection task could aim at sensing the potential users for communications. In the example shown in Fig. 6.4, there are four targets (i.e., drones) for the detection task, while two of them established the link with the base station for the communications. In the following, we consider K users that need communications, meanwhile M users could be detected. Obviously, the inequality $M \geq K$ always holds.

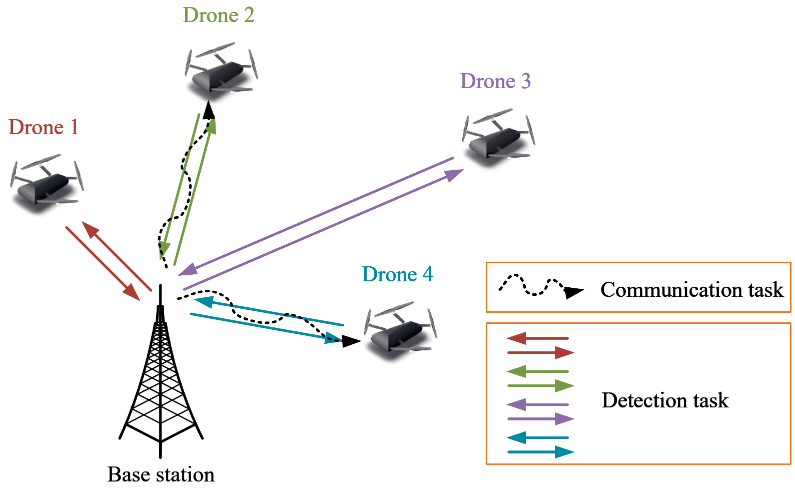


Figure 6.4 An example of a base station simultaneously implementing communications and detection tasks.

Following the principles of matched filter in radar system introduced in Section 3.3.2, we carefully look into the detection rate of targets under two scenarios: SIC at the base station and no SIC at the base station. In the former scenario, the power allocation coefficients need to be reconsidered so that the SIC at the base station is able to remove all communications components during radar receiving; in the latter scenario, the power allocation coefficients only obey the regulations brought up by the communications, all the communications components will be handled as interferences.

To exploit the SIC at the base station, the power allocation coefficients should follow the below,

$$\alpha_{k,\text{SIC}} > \beta_{\text{SIC}}, \quad \forall k = 1, 2, \ldots, K \tag{6.12}$$

with a further manipulation of the inequality, we can get,

$$\beta_{\text{SIC}} < \frac{1}{\sqrt{K}} \tag{6.13}$$

where $\alpha^2_{k,\text{SIC}}$ and β^2_{SIC} are respectively the power allocation coefficients for communications and radar components when the SIC is employed at the base station. The proof of (6.13) is given as follows,

Proof. For K users establishing communications connection, under condition (6.5) we could rewrite (6.1) as,

$$K\alpha^2_{1,\text{SIC}} + o = 1$$

which o is a positive dummy variable.

$$K\alpha^2_{1,\text{SIC}} + o = 1 \implies K\alpha^2_{1,\text{SIC}} < 1$$

provided (6.12), we obtain

$$\beta^2_{\text{SIC}} < \frac{1}{K} \implies \beta_{\text{SIC}} < \frac{1}{\sqrt{K}}$$

■

According to radar signal processing formula in (3.9b), the outputs of matched filter are given under two cases: SIC at the base station and no SIC at the base station.

SIC at the base station: the outputs $g^{(m)}_{\text{SIC}}(t)$ of matched filter for the m-th user, $m = 1, 2, 3, \ldots, M$,

$$g^{(m)}_{\text{SIC}}(t) = \int_0^{\Delta T} \left\{ \beta_{\text{SIC}} x(\tau - \tau_m)\eta_m h^2_m + \left[\xi S_{\text{int}} + n(t) \right] \right\} x^*(\tau - t) \mathrm{d}\tau \tag{6.14}$$

No SIC at the base station: the outputs $g^{(m)}(t)$ of matched filter for the m-th user,

$$g^{(m)}(t) = \int_{0}^{\Delta T} \left\{ S(\tau - \tau_m)\eta_m h_m^2 + \left[\xi S_{\text{int}} + n(t) \right] \right\} x^*(\tau - t) \mathrm{d}\tau \tag{6.15}$$

The hypothesis test is commonly used to determine the detection rate and false alarm rate, and Section 3.3.3 introduced the basic ideas behind. Let $\mathscr{H}_1$ denote the hypothesis that both desired signals and filtered noise are present, $\mathscr{H}_0$ denote the hypothesis that both interference and filtered noise are present. Under both hypotheses, $g^{(m)}(t)$ follows Gaussian distribution, the mean of $g^{(m)}(t)$ are $\mu_g^{(1)}$ and $\mu_g^{(0)}$ respectively,

$$\mathscr{H}_1 : \mu_g^{(1)} = \beta \eta_m h_m^2 \int_{0}^{\Delta T} |x(t)|^2 \, \mathrm{d}t \tag{6.16}$$

$$\mathscr{H}_0 : \mu_g^{(0)} = \eta_m h_m^2 \left| \int_{0}^{\Delta T} \sum_{k=1}^{K} \alpha_k s_k(t) x^*(t) \mathrm{d}t \right| + \xi S_{\text{int}} \left| \int_{0}^{\Delta T} x^*(t) \mathrm{d}t \right| \tag{6.17}$$

$g_{\text{SIC}}^{(m)}(t)$ follows Gaussian distribution as well, the mean of $g_{\text{SIC}}^{(m)}(t)$ are $\mu_{g_{\text{SIC}}}^{(1)}$ and $\mu_{g_{\text{SIC}}}^{(0)}$ respectively,

$$\mathscr{H}_1 : \mu_{g_{\text{SIC}}}^{(1)} = \beta_{\text{SIC}} \eta_m h_m^2 \int_{0}^{\Delta T} |x(t)|^2 \, \mathrm{d}t \tag{6.18}$$

$$\mathscr{H}_0 : \mu_{g_{\text{SIC}}}^{(0)} = \xi S_{\text{int}} \left| \int_{0}^{\Delta T} x^*(t) \mathrm{d}t \right| \tag{6.19}$$

For both $g^{(m)}(t)$ and $g_{\text{SIC}}^{(m)}(t)$, the corresponding variance σ_g^2 and $\sigma_{g_{\text{SIC}}}^2$ are the same, and can be written as,

$$\sigma_g^2 = \sigma_{g_{\text{SIC}}}^2 = \sigma_n^2 \int_{0}^{\Delta T} |x(t)|^2 \, \mathrm{d}t \tag{6.20}$$

Before we further analyse the above hypotheses, we briefly describe how the detection rate could be determined given the false alarm rate tolerance, which is the most encountered problem in practice.

Let us assume two hypotheses,

$$\mathscr{H}_0 : \mathcal{N}(\mu_0, \sigma_0^2) \tag{6.21}$$

$$\mathscr{H}_1 : \mathcal{N}(\mu_1, \sigma_1^2) \tag{6.22}$$

Given the threshold value to the above two hypothesis, λ_{th}, by following the equations in (3.16), (3.18) and the fact that the Q function is invertible, we could have,

$$P_{\text{D}} = Q\Big(\frac{\lambda_{\text{th}} - \mu_1}{\sigma_1}\Big) \tag{6.23a}$$

$$\lambda_{\text{th}} = \sigma_0 Q^{-1}(P_{\text{F}}) + \mu_0 \tag{6.23b}$$

substituting (6.23b) into (6.23a), we get,

$$P_{\text{D}} = Q\Big(\frac{\sigma_0}{\sigma_1} Q^{-1}(P_{\text{F}}) + \frac{\mu_0 - \mu_1}{\sigma_1}\Big) \tag{6.24}$$

Until now we have elaborated the relationship between the detection rate and the false alarm rate tolerance.

In order to compare detection rate under different circumstances, given that:

- the value of $Q^{-1}(P_{\text{F}})$ is a constant;
- Q function is monotonically decreasing;
- σ_0 and σ_1 are equal in our considered scenario, for example, the scenario illustrated in Fig. 6.4.

we could equivalently compare $\frac{\mu_0 - \mu_1}{\sigma_1}$, the greater the value of $\frac{\mu_0 - \mu_1}{\sigma_1}$ is, the smaller the detection rate is.

Now, for the **no SIC at the base station** case, we have $\frac{\mu_g^{(0)} - \mu_g^{(1)}}{\sigma_g^2}$; for the **SIC at**

the base station case, we have $\frac{\mu_{g_{\mathrm{SIC}}}^{(0)}-\mu_{g_{\mathrm{SIC}}}^{(1)}}{\sigma_{g_{\mathrm{SIC}}}^{2}}$. Let us define the following equation,

$$\begin{aligned}\varepsilon_{\mathrm{det}} &= \frac{\mu_{g}^{(0)}-\mu_{g}^{(1)}}{\sigma_{g}^{2}} - \frac{\mu_{g_{\mathrm{SIC}}}^{(0)}-\mu_{g_{\mathrm{SIC}}}^{(1)}}{\sigma_{g_{\mathrm{SIC}}}^{2}} \\ &= \mu_{g}^{(0)} - \mu_{g}^{(1)} - \mu_{g_{\mathrm{SIC}}}^{(0)} + \mu_{g_{\mathrm{SIC}}}^{(1)}\end{aligned} \tag{6.25}$$

clearly, when the value of $\varepsilon_{\mathrm{det}}$ is smaller than 0, the **no SIC at the base station** case outperforms the **SIC at the base station** case, in terms of detection rate.

Substituting (6.17), (6.16), (6.19) and (6.18) into (6.25), we get,

$$\varepsilon_{\mathrm{det}} = \eta_m h_m^2 \left| \int_0^{\Delta T} \sum_{k=1}^{K} \alpha_k s_k(t) x^*(t) \mathrm{d}t \right| + (\beta_{\mathrm{SIC}} - \beta)\eta_m h_m^2 \int_0^{\Delta T} |x(t)|^2 \,\mathrm{d}t \tag{6.26}$$

by applying Cauchy-Schwarz inequality and triangle inequality successively,

$$\varepsilon_{\mathrm{det}} \leq \eta_m h_m^2 \sqrt{\int_0^{\Delta T} \Big[\sum_{k=1}^{K} |\alpha_k s_k(t)|\Big]^2 \mathrm{d}t} \sqrt{\int_0^{\Delta T} |x(t)|^2 \,\mathrm{d}t} + (\beta_{\mathrm{SIC}} - \beta)\eta_m h_m^2 \int_0^{\Delta T} |x(t)|^2 \,\mathrm{d}t \tag{6.27}$$

If the communications components are orthogonal to each other,

$$\int_0^{\Delta T} s_i(t) s_j(t) \mathrm{d}t = 0, \quad i \neq j, \quad \forall i,j = 1,2,\ldots,K \tag{6.28}$$

we could further modify (6.27) to,

$$\varepsilon_{\mathrm{det}} \leq \eta_m h_m^2 \sqrt{\int_0^{\Delta T} \sum_{k=1}^{K} \alpha_k^2 \,|s_k(t)|^2 \,\mathrm{d}t} \sqrt{\int_0^{\Delta T} |x(t)|^2 \,\mathrm{d}t} + (\beta_{\mathrm{SIC}} - \beta)\eta_m h_m^2 \int_0^{\Delta T} |x(t)|^2 \,\mathrm{d}t \tag{6.29}$$

Then we could infer that,

$$\beta > \sqrt{\frac{\int\limits_{0}^{\Delta T} \sum\limits_{k=1}^{K} \alpha_k^2 \left|s_k(t)\right|^2 \mathrm{d}t}{\int\limits_{0}^{\Delta T} \left|x(t)\right|^2 \mathrm{d}t}} + \beta_{\mathrm{SIC}} \Longrightarrow \varepsilon_1 < 0 \tag{6.30}$$

Provided the inequality in (6.13), we get,

$$\beta > \sqrt{\frac{\int\limits_{0}^{\Delta T} \sum\limits_{k=1}^{K} \alpha_k^2 \left|s_k(t)\right|^2 \mathrm{d}t}{\int\limits_{0}^{\Delta T} \left|x(t)\right|^2 \mathrm{d}t}} + \frac{1}{\sqrt{K}} \Longrightarrow \varepsilon_1 < 0 \tag{6.31}$$

The term $\int\limits_{0}^{\Delta T} \sum\limits_{k=1}^{K} \alpha_k^2 \left|s_k(t)\right|^2 \mathrm{d}t$ is equal to the power split for communications tasks, the term $\int\limits_{0}^{\Delta T} \left|x(t)\right|^2 \mathrm{d}t$ is equal to the power of radar signal within ΔT duration.

The results imply that: i) for the scenario with **low** QoS requirements in communications part and relatively **large** number of users that need communications, the **no SIC at the base station** case is recommended; ii) for the scenario with **high** QoS requirements in communications part and relatively **small** number of users that need communications, the **SIC at the base station** case is recommended. The above recommendations are in the context of detection rate.

6.3 Discussion

The RF convergence tends to be a main feature in the 5G an the future cellular networks. Especially, the integrated sensing and communications system draws more and more discussions both in academia and industrial. This chapter reviews newly proposed superposition coding scheme for joint sensing and communications system, the optimisation problem for the joint system and eventually the detection rate comparisons. The main findings are as follows:

1. The superposition coding is suitable for airborne vehicles, particularly for the control & command signals together with the sensing functionalities;
2. The user with a moderate QoS requirements could benefit the most from the superposition coding scheme among all that have different QoS requirements;
3. With respect to the detection rate, 1) the idea of utilising the SIC at the base station, for the purpose of removing communications components during the radar receiving, is suitable for a small number of users in need of communications but with high QoS requirements; 2) without using SIC at the base station, the scenario that a large number of users are in need of communications but with low QoS requirements, is suitable. The base station without using SIC, for example, could provide the control & command signals for drones as the communications services.

7 CONCLUSION AND FUTURE DIRECTIONS

The RF convergence concept has charged in the wireless communications community with its full strength, the turning point emerges that joint systems cover the communications, positioning and sensing. With the evolution of technologies in electronics, communications, positioning and sensing, the modern concepts of wireless networks transcend the old convention on the definition of communications. The boundaries among communications, positioning, and sensing were blurred in the past years, thus, the studies on the interaction, cooperation, compatibility, etc., for the joint systems came to prominence. This thesis is born in the above context, and aims at bringing introductions, developments, and discussions to the joint systems.

The thesis is based on eight publications and consists of four main parts: 1) investigation on state of the art in wireless channel models, challenges and solutions in separated systems of communications, positioning and sensing, publications [P1-P4] and Chapter 2, Chapter 3 are covered in this part; 2) newly developed RF fingerprinting techniques for the resilience of GNSS signal processing, publications [P5, P6] and Chapter 4 are covered in this part; 3) the positioning-aided communications, particularly the location-based beamforming, it covers publication [P7] and Chapter 5; 4) proposed superposition coding scheme for the integrated sensing and communications, this part covers publications [P8] and Chapter 6.

The following concludes the main take-away points in this thesis, furthermore discusses the way ahead.

7.1 The take-away points

To start the summary of this thesis work, we answer the research questions in Chapter 1, then we address the main take-away points.

Q1: "How to model the ground-to-air/air-to-ground channel models when the altitude of users is more than 300 m and the operating frequency of users is at mmWave bands?"

Answer: We found out that expanding the channels above 300 m with free space losses together with incorporated atmospheric effects, such as rain and gas effects, gave good results in the context of general aircraft and UAV communications.

Q2: "How could the innovations in communications, in terms of mmWave and multi-antenna system, benefit the aerial users?"

Answer: Comparing with the 4G operating frequency bands, the usage of mmWave could significantly improve the throughput of aerial users while does not increase the outage probability for aerial users. The MISO techniques was found to increase roughly 10 dB in SIR comparing with the SISO techniques (i.e., techniques are currently used to serve aerial users).

Q3: "How are the predictive abilities of 3GPP models for various IIoT technologies in indoor industrial sites?"

Answer: Based on link budgets of various IIoT technologies, We ran simulations for 3GPP models to estimate metrics such as coverage, spectral efficiency and outage probability. By comparing the prediction results of 3GPP models with the reported results from the literature, we conclude that 3GPP RMa and UMa models showed good abilities to predict parameters for medium-to-long range IIoT technologies, e.g., MIOTY and NB-IoT; 3GPP InH and InF models were suitable to predict parameters for short range IIoT technologies. More discussions could be found in Chapter 3 and publication [P2].

Q4: "What anti-spoofing mechanisms based on machine learning can be used with raw GNSS data to support robust localisation and location-based applications?"

Answer: We proposed the RF fingerprinting based anti-spoofing solution in Chapter 4. The proposed methods are in two classes: pre- and post-correlation methods. In Chapter 4, a thorough introduction was given and the comprehensive real-field-data-based testing is conducted for proof of concept. In the results of the testing, the spoofing detection accuracy of up to 99.99% was obtained with the pre-correlation methods; and the spoofing detection accuracy of up to 97.72% was obtained with the post-correlation methods. The pre-correlation methods were better than post-correlation methods in terms of accuracy, but worse in the capability of distinguishing the exact pseudorandom sequence of the spoofer.

Q5: "To what extent, a location-based beamforming is beneficial towards joint positioning and communications?"

Answer: The location-based beamforming showed better performance than the traditional CSI-based beamforming in the noisy channel. Specifically, the location-based beamforming was shown to be 1 Mbps than CSI-based beamforming in capacity metric; the outage probability of the CSI-based beamforming is on average eight times than that of the location-based beamforming. We provided discussions in Chapter 5.

Q6: "Which scenario is feasible for the newly developed waveform in the joint sensing and communications system, and what is the performance of the new waveform design?"

Answer: The newly developed waveform design is suitable for the drones using the control & command signals for the communications task. With a moderate QoS requirements in the communications task, the new waveform could balance both communications and sensing.

The investigation of channel models was mainly carried out in Chapter 2 and Chapter 3. In Chapter 2, thorough descriptions of FSL, log-distance path loss model and 3GPP models were presented. The 3GPP models imply that: after a certain altitude, the RMa and UMa signals propagation is in purely LOS conditions; both RMa and UMa models predict the FSL at high altitude; in the indoor scenarios, the InH unexpectedly shows less signal strength loss than the FSL under LOS conditions. Additionally, the atmospheric effects on the signals propagation were studied with ITU documents. The results showed that: the 60 GHz bands should be avoided due to the high oxygen absorption; a moist environment or rainfall weather brings more damage to the mmWave signals than the dry air. In Chapter 3, the status quo and new developments in communications, positioning and sensing were introduced and discussed with different focuses. In the communications part, it concluded that: the usage of mmWave bands benefits the aerial users communications, especially the reliability on the control & command signals; the 3GPP models predict the similar results for the IIoT applications on the coverage metrics, in contrast with the reported values from various literature; the multi-antenna system becomes necessary for the aerials users due to the vulnerability of aerial users to the interference, evidences prove that the multi-antenna system is efficient on the interference mitigation.

In the positioning part, the current anti-spoofing techniques in the GNSS were closely reviewed with recommendations on the subcategory of signal processing based method—the RF fingerprinting.

In the sensing part, a framework of the integrated sensing and communications system, based on the mono-static radar, was constructed for the further discussions in Chapter 6.

With the ubiquitous deployment of GNSS functionalities in electronic devices, particularly the life-critical applications, a solution for the trustworthy or assured GNSS PNT is desirable for the market. Chapter 4 described the novel RF fingerprinting techniques for the GNSS resilience against the spoofing. The generic diagram of GNSS signals transmitters was provided, the potential sources of RF fingerprints in the transmitters are identified with analysis in details. Based on the studies carried out on pre- and post-correlation domain in the GNSS receiver, the measurements campaigns were proceeded to validate the feasibility of the RF fingerprinting in GNSS for the cause of anti-spoofing. The results showed that the RF fingerprinting techniques were capable of differentiating the spoofers from the genuine GNSS transmitters (i.e., the satellites). Specifically, the spectrogram plus SVM suits the best for the pre-correlation methods among others; the SVM works as well for the post-correlation methods. We obtained up to 99.99% mean classification accuracy with pre-correlation data and up to 97.72% mean classification accuracy with post-correlation data ; we have seen that, unlike pre-correlation data which can only determine if spoofing is present or not, the post-correlation-data-based RF fingerprinting is also able to identify which transmitters are spoofing transmitters and which ones are genuine transmitters.

The location information is almost available in every wireless communications equipment (e.g., location information provided by the GNSS), it is very plausible to utilise this information to enhance the the performance of communications. Chapter 5 proposes the location-based beamforming technique as a way to exploit the location information at hand. The concept of location-based beamforming is established in this chapter. Furthermore, throughout the studies, we conclude that: i) the location-based beamforming is sensitive to the location errors and the tracking errors, however a sophisticated design of antenna array could suppress the influence of the above errors to the minimum; ii) in contrast with a pure CSI-based beamforming technique, the location-based beamforming shows merits in the performance in 'noisy' environments as well the latency metric. In the noisy channel of our simulations, the location-based beamforming was shown to be 1 Mbps than CSI-based beamforming in capacity metric; the outage probability of the CSI-based beamforming is on average eight times than that of the location-based beamforming.

It is inevitable to step into a time when the integrated sensing and communications becomes an essential feature in the wireless communications standard. Chapter 6 reviews the state of the art techniques and introduces our new proposal, the superposition coding scheme, for the joint sensing and communications systems. To put this chapter into a nutshell, we concludes that: i) the newly proposed superposition coding scheme is particularly suitable for the aerial users when the communications are mainly control & command signals; ii) a moderate QoS requirements in the communications side could balance the performance in both communications and sensing, the fairness in the communications as well benefits from the moderate QoS requirements; iii) through the modelling and mathematical proofs, we prove that using the SIC at the base station—to remove the communications components (i.e., interference to the radar functionality) for the boost of SINR in the radar receiving—actually degenerate the performance of sensing, in terms of the detection rate.

Overall, this thesis comprehensively covers the studies of wireless channel models, innovative technologies in 5G, the security in GNSS PNT, the location-aided communications and the joint sensing and communications system. Attempts in several aspects of RF convergence are put into actions, the results set an optimistic expectation in the future. The concepts, algorithms, models and propositions in this work are validated either by numerical analysis, mathematical proofs or experiments data. We are confident that this work brings many intriguing perspectives in various angles of RF convergence big picture.

7.2 The way ahead

This thesis will soon end here, however the story in the RF convergence continues. There are still many unknowns waiting for exploration, we use this opportunity to ignite the sparks among readers in this very field. We summarise our considerations as following:

1. As a way to reveal the nature of electromagnetic wave propagation, the channel loss models above 300 m altitude need to be further studied and deeper analysed with measurement data, especially concerning the ground-to-air/air-to-ground scenarios for mmWave bands.
2. An open challenge remains to find out in which way, the low altitude airborne vehicles, for example the UAVs, could incorporate their datalinks into the 5G and the beyond networks. Additional open questions are, for example, related to the best allocation of control & command signals, video & entertainment signals, and any other type of data in future unmanned vehicles.
3. Our thesis work showed that RF fingerprinting may improve the resilience to interference of GNSS-based solutions, but an open question remains how to design the RF fingerprinting based anti-spoofing PVT solutions. In addition, it would be interesting to find the feasible data fusion methods, which could make the best use of pre- and post-correlation data, and navigation data.
4. In the superposition coding scheme, there is the remaining question whether there is a universal metric to evaluate the performance of communications and sensing simultaneously. How to exploit the radar signals components and communications signals components to serve the joint system the best is also a worthy open question to investigate further.

REFERENCES

[1] NTIA. *United States frequency allocations chart*. https://www.ntia.doc.gov/files/ntia/publications/2003-allochrt.pdf/. [accessed 10.05.2022].

[2] S. Haykin. Cognitive radio: brain-empowered wireless communications. *IEEE Journal on Selected Areas in Communications* 23.2 (2005), 201–220. DOI: 10.1109/JSAC.2004.839380.

[3] J. Mitola and G. Maguire. Cognitive radio: making software radios more personal. *IEEE Personal Communications* 6.4 (1999), 13–18. DOI: 10.1109/98.788210.

[4] V. Chakravarthy, X. Li, Z. Wu, M. A. Temple, F. Garber, R. Kannan and A. Vasilakos. Novel overlay/underlay cognitive radio waveforms using SD-SMSE framework to enhance spectrum efficiency- part i: theoretical framework and analysis in AWGN channel. *IEEE Transactions on Communications* 57.12 (2009), 3794–3804. DOI: 10.1109/TCOMM.2009.12.080400.

[5] S. Srinivasa and S. A. Jafar. The Throughput Potential of Cognitive Radio: A Theoretical Perspective. *2006 Fortieth Asilomar Conference on Signals, Systems and Computers*. 2006, 221–225. DOI: 10.1109/ACSSC.2006.356619.

[6] J. Poston and W. Horne. Discontiguous OFDM considerations for dynamic spectrum access in idle TV channels. *First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005.* 2005, 607–610. DOI: 10.1109/DYSPAN.2005.1542679.

[7] J. D. Guffey, A. M. Wyglinski and G. J. Minden. Agile Radio Implementation of OFDM Physical Layer for Dynamic Spectrum Access Research. *IEEE GLOBECOM 2007 - IEEE Global Telecommunications Conference*. 2007, 4051–4055. DOI: 10.1109/GLOCOM.2007.770.

[8] Q. Zhao and B. M. Sadler. A Survey of Dynamic Spectrum Access. *IEEE Signal Processing Magazine* 24.3 (2007), 79–89. DOI: `10.1109/MSP.2007.361604`.

[9] Q. Zhao and A. Swami. A Survey of Dynamic Spectrum Access: Signal Processing and Networking Perspectives. *2007 IEEE International Conference on Acoustics, Speech and Signal Processing - ICASSP '07*. Vol. 4. 2007, IV-1349-IV–1352. DOI: `10.1109/ICASSP.2007.367328`.

[10] Q. Zhao, L. Tong, A. Swami and Y. Chen. Decentralized cognitive MAC for opportunistic spectrum access in ad hoc networks: A POMDP framework. *IEEE Journal on Selected Areas in Communications* 25.3 (2007), 589–600. DOI: `10.1109/JSAC.2007.070409`.

[11] Q. Zhao and A. Swami. A Decision-Theoretic Framework for Opportunistic Spectrum Access. *IEEE Wireless Communications* 14.4 (2007), 14–20. DOI: `10.1109/MWC.2007.4300978`.

[12] W. Wang and X. Liu. List-coloring based channel allocation for open-spectrum wireless networks. *VTC-2005-Fall. 2005 IEEE 62nd Vehicular Technology Conference, 2005*. Vol. 1. 2005, 690–694. DOI: `10.1109/VETECF.2005.1558001`.

[13] H. Zheng and C. Peng. Collaboration and fairness in opportunistic spectrum access. *IEEE International Conference on Communications, 2005. ICC 2005. 2005*. Vol. 5. 2005, 3132–3136 Vol. 5. DOI: `10.1109/ICC.2005.1494982`.

[14] H. T. Hayvaci and B. Tavli. Spectrum sharing in radar and wireless communication systems: A review. *2014 International Conference on Electromagnetics in Advanced Applications (ICEAA)*. 2014, 810–813. DOI: `10.1109/ICEAA.2014.6903969`.

[15] B. Paul, A. R. Chiriyath and D. W. Bliss. Survey of RF Communications and Sensing Convergence Research. *IEEE Access* 5 (2017), 252–270. DOI: `10.1109/ACCESS.2016.2639038`.

[16] A. R. Chiriyath, B. Paul and D. W. Bliss. Radar-Communications Convergence: Coexistence, Cooperation, and Co-Design. *IEEE Transactions on Cognitive Communications and Networking* 3.1 (2017), 1–12. DOI: `10.1109/TCCN.2017.2666266`.

[17] F. Liu, C. Masouros, A. P. Petropulu, H. Griffiths and L. Hanzo. Joint Radar and Communication Design: Applications, State-of-the-Art, and the Road Ahead. *IEEE Transactions on Communications* 68.6 (2020), 3834–3862. DOI: 10.1109/TCOMM.2020.2973976.

[18] C. Sturm, T. Zwick and W. Wiesbeck. An OFDM System Concept for Joint Radar and Communications Operations. *VTC Spring 2009 - IEEE 69th Vehicular Technology Conference*. 2009, 1–5. DOI: 10.1109/VETECS.2009.5073387.

[19] C. Sturm and W. Wiesbeck. Waveform Design and Signal Processing Aspects for Fusion of Wireless Communications and Radar Sensing. *Proceedings of the IEEE* 99.7 (2011), 1236–1259. DOI: 10.1109/JPROC.2011.2131110.

[20] S. A. Hassani, A. Guevara, K. Parashar, A. Bourdoux, B. van Liempd and S. Pollin. An In-Band Full-Duplex Transceiver for Simultaneous Communication and Environmental Sensing. *2018 52nd Asilomar Conference on Signals, Systems, and Computers*. 2018, 1389–1394. DOI: 10.1109/ACSSC.2018.8645165.

[21] Y. Zeng, Y. Ma and S. Sun. Joint Radar-Communication: Low Complexity Algorithm and Self-Interference Cancellation. *2018 IEEE Global Communications Conference (GLOBECOM)*. 2018, 1–7. DOI: 10.1109/GLOCOM.2018.8647502.

[22] B. van Liempd, A. Visweswaran, S. Ariumi, S. Hitomi, P. Wambacq and J. Craninckx. Adaptive RF Front-Ends Using Electrical-Balance Duplexers and Tuned SAW Resonators. *IEEE Transactions on Microwave Theory and Techniques* 65.11 (2017), 4621–4628. DOI: 10.1109/TMTT.2017.2728039.

[23] Y. S. Choi, C. S. Cho and Y.-J. Kim. Improved Tx-to-Rx Isolation of Radar Transceivers Using Integrated Full Duplexer with PLL. *2018 International Conference on Radar (RADAR)*. 2018, 1–4. DOI: 10.1109/RADAR.2018.8557219.

[24] K. E. Kolodziej, B. T. Perry and J. S. Herd. In-Band Full-Duplex Technology: Techniques and Systems Survey. *IEEE Transactions on Microwave Theory and Techniques* 67.7 (2019), 3025–3041. DOI: 10.1109/TMTT.2019.2896561.

[25] M. Biedka, Y. E. Wang, Q. M. Xu and Y. Li. Full-Duplex RF Front Ends : From Antennas and Circulators to Leakage Cancellation. *IEEE Microwave Magazine* 20.2 (2019), 44–55. DOI: 10.1109/MMM.2018.2880496.

[26] A. Sabharwal, P. Schniter, D. Guo, D. W. Bliss, S. Rangarajan and R. Wichman. In-Band Full-Duplex Wireless: Challenges and Opportunities. *IEEE Journal on Selected Areas in Communications* 32.9 (2014), 1637–1652. DOI: 10.1109/JSAC.2014.2330193.

[27] E. Everett, A. Sahai and A. Sabharwal. Passive Self-Interference Suppression for Full-Duplex Infrastructure Nodes. *IEEE Transactions on Wireless Communications* 13.2 (2014), 680–694. DOI: 10.1109/TWC.2013.010214.130226.

[28] S. Khaledian, F. Farzami, B. Smida and D. Erricolo. Inherent Self-Interference Cancellation for In-Band Full-Duplex Single-Antenna Systems. *IEEE Transactions on Microwave Theory and Techniques* 66.6 (2018), 2842–2850. DOI: 10.1109/TMTT.2018.2818124.

[29] A. Nagulu and H. Krishnaswamy. Non-Magnetic 60GHz SOI CMOS Circulator Based on Loss/Dispersion-Engineered Switched Bandpass Filters. *2019 IEEE International Solid- State Circuits Conference - (ISSCC)*. 2019, 446–448. DOI: 10.1109/ISSCC.2019.8662467.

[30] T. Dinc and H. Krishnaswamy. A 28GHz magnetic-free non-reciprocal passive CMOS circulator based on spatio-temporal conductance modulation. *2017 IEEE International Solid-State Circuits Conference (ISSCC)*. 2017, 294–295. DOI: 10.1109/ISSCC.2017.7870377.

[31] B. Zhang and H. Mouftah. Position-aided on demand routing protocol for wireless ad hoc networks. *2004 IEEE International Conference on Communications (IEEE Cat. No.04CH37577)*. Vol. 6. 2004, 3764–3768 Vol.6. DOI: 10.1109/ICC.2004.1313245.

[32] M. Mauve, J. Widmer and H. Hartenstein. A survey on position-based routing in mobile ad hoc networks. *IEEE Network* 15.6 (2001), 30–39. DOI: 10.1109/65.967595.

[33] I. Stojmenovic. Position-based routing in ad hoc networks. *IEEE Communications Magazine* 40.7 (2002), 128–134. DOI: 10.1109/MCOM.2002.1018018.

[34] P. Kela, M. Costa, J. Turkka, M. Koivisto, J. Werner, A. Hakkarainen, M. Valkama, R. Jantti and K. Leppanen. Location Based Beamforming in 5G Ultra-Dense Networks. *2016 IEEE 84th Vehicular Technology Conference (VTC-Fall)*. 2016, 1–7. DOI: 10.1109/VTCFall.2016.7881072.

[35] W. Miao, C. Luo, G. Min, L. Wu, T. Zhao and Y. Mi. Position-Based Beamforming Design for UAV Communications in LTE Networks. *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*. 2019, 1–6. DOI: 10.1109/ICC.2019.8761505.

[36] W. Miao, C. Luo, G. Min, Y. Mi and Z. Yu. Location-Based Robust Beamforming Design for Cellular-Enabled UAV Communications. *IEEE Internet of Things Journal* 8.12 (2021), 9934–9944. DOI: 10.1109/JIOT.2020.3028853.

[37] 3GPP. *Technical Specification Group Radio Access Network; Study on Enhanced LTE Support for Aerial Vehicles*. Technical report (TR) 36.777. Version 15.0.0. 3rd Generation Partnership Project (3GPP), Jan. 2018.

[38] 3GPP. *Technical Specification Group Radio Access Network; Study on channel model for frequencies from 0.5 to 100 GHz*. Technical report (TR) 38.901. Version 16.1.0. 3rd Generation Partnership Project (3GPP), Jan. 2020.

[39] W. Khawaja, I. Guvenc, D. W. Matolak, U.-C. Fiebig and N. Schneckenburger. A Survey of Air-to-Ground Propagation Channel Modeling for Unmanned Aerial Vehicles. *IEEE Communications Surveys Tutorials* 21.3 (2019), 2361–2391. DOI: 10.1109/COMST.2019.2915069.

[40] D. Schmidt, K. Radke, S. Camtepe, E. Foo and M. Ren. A Survey and Analysis of the GNSS Spoofing Threat and Countermeasures. *ACM Comput. Surv.* 48.4 (May 2016). ISSN: 0360-0300. DOI: 10.1145/2897166.

[41] R. Morales-Ferre, P. Richter, E. Falletti, A. de la Fuente and E. S. Lohan. A Survey on Coping With Intentional Interference in Satellite Navigation for Manned and Unmanned Aircraft. *IEEE Communications Surveys Tutorials* 22.1 (2020), 249–291. DOI: 10.1109/COMST.2019.2949178.

[42] D. W. Matolak and R. Sun. Air–Ground Channel Characterization for Unmanned Aircraft Systems—Part III: The Suburban and Near-Urban Environments. *IEEE Transactions on Vehicular Technology* 66.8 (2017), 6607–6618. DOI: 10.1109/TVT.2017.2659651.

[43] T. S. Rappaport, S. Sun and M. Shafi. Investigation and Comparison of 3GPP and NYUSIM Channel Models for 5G Wireless Communications. *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)*. 2017, 1–5. DOI: 10.1109/VTCFall.2017.8287877.

[44] S. Kamrul Islam. *Sensors and Low Power Signal Processing*. eng. 1st ed. 2010. New York, NY: Springer US, 2010. ISBN: 1282837915.

[45] R. M. Sandoval, A.-J. Garcia-Sanchez and J. Garcia-Haro. Improving RSSI-Based Path-Loss Models Accuracy for Critical Infrastructures: A Smart Grid Substation Case-Study. *IEEE Transactions on Industrial Informatics* 14.5 (2018), 2230–2240. DOI: 10.1109/TII.2017.2774838.

[46] E. Tanghe, W. Joseph, L. Verloock, L. Martens, H. Capoen, K. V. Herwegen and W. Vantomme. The industrial indoor channel: large-scale and temporal fading at 900, 2400, and 5200 MHz. *IEEE Transactions on Wireless Communications* 7.7 (2008), 2740–2751. DOI: 10.1109/TWC.2008.070143.

[47] K. Wang, R. Zhang, L. Wu, Z. Zhong, L. He, J. Liu and X. Pang. Path Loss Measurement and Modeling for Low-Altitude UAV Access Channels. *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)*. 2017, 1–5. DOI: 10.1109/VTCFall.2017.8288385.

[48] E. Yanmaz, R. Kuschnig and C. Bettstetter. Achieving air-ground communications in 802.11 networks with three-dimensional aerial mobility. *2013 Proceedings IEEE INFOCOM*. 2013, 120–124. DOI: 10.1109/INFCOM.2013.6566747.

[49] D. W. Matolak and R. Sun. Air–Ground Channel Characterization for Unmanned Aircraft Systems—Part I: Methods, Measurements, and Models for Over-Water Settings. *IEEE Transactions on Vehicular Technology* 66.1 (2017), 26–44. DOI: 10.1109/TVT.2016.2530306.

[50] ITU-R. *P Series; Radiowave propagation; Reference standard atmospheres*. Recommendation ITU-R P.835-6. International Telecommunication Union (ITU), Dec. 2017.

[51] ITU-R. *P Series; Radiowave propagation; Attenuation by atmospheric gases and related effects*. Recommendation ITU-R P.676-12. International Telecommunication Union (ITU), Aug. 2019.

[52] ITU-R. *P Series; Radiowave propagation; Attenuation due to clouds and fog*. Recommendation ITU-R P.840-8. International Telecommunication Union (ITU), Aug. 2019.

[53] ITU-R. *P Series; Radiowave propagation; Specific attenuation model for rain for use in prediction methods*. Recommendation ITU-R P.838-3. International Telecommunication Union (ITU), Mar. 2005.

[54] J. S. Seybold. *Introduction to RF propagation*. John Wiley & Sons, 2005.

[55] FAA. FAA Aerospace Forecasts. *FAA Data & Research* (July 6, 2021). URL: `https://www.faa.gov/data_research/aviation/aerospace_forecasts/` (visited on 01/20/2022).

[56] W. Wang and E.-S. Lohan. Interference in heterogeneous aviation networks. *Proceedings of XXXV Finnish URSI Convention on Radio Science*. URSI. 2019.

[57] FAA. FAA Releases Aerospace Forecast. *FAA Newsroom* (Mar. 15, 2018). URL: `https://www.faa.gov/newsroom/faa-releases-aerospace-forecast?newsId=89870` (visited on 01/20/2022).

[58] D. W. Matolak. Hyper-spectral communications, networking amp; ATM as foundation for safe and efficient future flight: Transcending aviation operational limitations with diverse and secure multi-band, multi-mode, and mmWave wireless links: Project overview, aviation communications and new signaling. *2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC)*. 2017, 1–7. DOI: `10.1109/DASC.2017.8102041`.

[59] 3GPP. *Technical Specification Group Radio Access Network; Study on New Radio (NR) to support non-terrestrial networks*. Technical report (TR) 38.811. Version 15.4.0. 3rd Generation Partnership Project (3GPP), Oct. 2020.

[60] T. Sørensen, R. Bruun, R. Marcker and P. E. Mogensen. Comparison of cm- and mm-Wave Channel Characteristics between Autonomous Mobile Robots in a small I4.0 Manufacturing Facility. Symposium on Wireless Personal Multimedia Communications : 5G WAY FORWARD TO 6G, WPMC 2022 ; Conference date: 30-10-2022 Through 02-11-2022. May 2022.

[61] J. Chen, K. Hu, Q. Wang, Y. Sun, Z. Shi and S. He. Narrowband Internet of Things: Implementations and Applications. *IEEE Internet of Things Journal* 4.6 (2017), 2309–2314. DOI: `10.1109/JIOT.2017.2764475`.

[62] A. Augustin, J. Yi, T. Clausen and W. M. Townsley. A Study of LoRa: Long Range & Low Power Networks for the Internet of Things. *Sensors* 16.9 (2016). ISSN: 1424-8220. DOI: `10.3390/s16091466`.

[63] M. Centenaro, L. Vangelista, A. Zanella and M. Zorzi. Long-range communications in unlicensed bands: the rising stars in the IoT and smart city scenarios. *IEEE Wireless Communications* 23.5 (2016), 60–67. DOI: 10.1109/MWC.2016.7721743.

[64] R. Quinnell. Low power wide-area networking alternatives for the IoT. *EDN Network* 43 (2015), 1–6.

[65] D. M. Hernandez, G. Peralta, L. Manero, R. Gomez, J. Bilbao and C. Zubia. Energy and coverage study of LPWAN schemes for Industry 4.0. *2017 IEEE International Workshop of Electronics, Control, Measurement, Signals and their Application to Mechatronics (ECMSM)*. 2017, 1–6. DOI: 10.1109/ECMSM.2017.7945893.

[66] Y. Li, X. Cheng, Y. Cao, D. Wang and L. Yang. Smart Choice for the Smart Grid: Narrowband Internet of Things (NB-IoT). *IEEE Internet of Things Journal* 5.3 (2018), 1505–1515. DOI: 10.1109/JIOT.2017.2781251.

[67] *MIOTY™by BTI Starter Kit 1.0 with Microsoft Azure*. https://behrtechnologies.com/. 2018.

[68] M. Bucur, T. Sorensen, R. Amorim, M. Lopez, I. Z. Kovacs and P. Mogensen. Validation of Large-Scale Propagation Characteristics for UAVs within Urban Environment. *2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall)*. 2019, 1–6. DOI: 10.1109/VTCFall.2019.8891422.

[69] C. A. Balanis. *Antenna theory: analysis and design*. eng. 4th ed. Hoboken: Wiley, 2016. ISBN: 9781118642061.

[70] *5G is NOW, Huawei Field Trial Progress*. https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2018/5GHungary/S2%20Attila%20T%C3%B3th.pdf. 2018.

[71] S. C. Wooh and Y. Shi. Influence of phased array element size on beam steering behavior. *Ultrasonics* 36.6 (1998), 737–749. DOI: https://doi.org/10.1016/S0041-624X(97)00164-9.

[72] Z. B. Tariq, D. M. Cheema, M. Z. Kamran and I. H. Naqvi. Non-GPS Positioning Systems: A Survey. *ACM Comput. Surv.* 50.4 (Aug. 2017). DOI: 10.1145/3098207.

[73] A. Nardin, F. Dovis and J. A. Fraire. Empowering the Tracking Performance of LEO-Based Positioning by Means of Meta-Signals. *IEEE Journal of Radio Frequency Identification* 5.3 (2021), 244–253. DOI: 10.1109/JRFID.2021.3077082.

[74] R. M. Vaghefi and R. M. Buehrer. Improving positioning in LTE through collaboration. *2014 11th Workshop on Positioning, Navigation and Communication (WPNC)*. 2014, 1–6. DOI: 10.1109/WPNC.2014.6843292.

[75] K. Li, J. Bigham, E. L. Bodanese and L. Tokarchuk. Location estimation in large indoor multi-floor buildings using hybrid networks. *2013 IEEE Wireless Communications and Networking Conference (WCNC)*. 2013, 2137–2142. DOI: 10.1109/WCNC.2013.6554893.

[76] Y. Gu, L. Quan, F. Ren and J. Li. Fast Indoor Localization of Smart Hand-Held Devices Using Bluetooth. *2014 10th International Conference on Mobile Ad-hoc and Sensor Networks*. 2014, 186–194. DOI: 10.1109/MSN.2014.32.

[77] P. Meissner, E. Leitinger and K. Witrisal. UWB for Robust Indoor Tracking: Weighting of Multipath Components for Efficient Estimation. *IEEE Wireless Communications Letters* 3.5 (2014), 501–504. DOI: 10.1109/LWC.2014.2341636.

[78] F. Montorsi, F. Pancaldi and G. M. Vitetta. Map-Aware Models for Indoor Wireless Localization Systems: An Experimental Study. *IEEE Transactions on Wireless Communications* 13.5 (2014), 2850–2862. DOI: 10.1109/TWC.2014.040714.130893.

[79] E. D. Kaplan and C. Hegarty. *Understanding GPS/GNSS : principles and applications*. eng. Third edition. GNSS Technology and Applications Series. Artech House, 2017. ISBN: 9781580538947.

[80] M. Säily, O. N. C. Yilmaz, D. S. Michalopoulos, E. Pérez, R. Keating and J. Schaepperle. Positioning Technology Trends and Solutions Toward 6G. *2021 IEEE 32nd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*. 2021, 1–7. DOI: 10.1109/PIMRC50174.2021.9569341.

[81] Peter Gutierrez. *Fleshing Out the LEO PNT Landscape*. https://insidegnss.com/fleshing-out-the-leo-pnt-landscape/. Mar. 2022.

[82] R. Morales-Ferre, E. S. Lohan, G. Falco and E. Falletti. GDOP-based analysis of suitability of LEO constellations for future satellite-based positioning. *2020 IEEE International Conference on Wireless for Space and Extreme Environments (WiSEE)*. 2020, 147–152. DOI: `10.1109/WiSEE44079.2020.9262624`.

[83] Y. Béniguel, M. Angling, E. Banfi, C. Bourga, M. Cueto, R. Fleury, A. Garcia-Rigo, P. Hamel, R. Hartmann, M. Hernández-Pajares, N. Jakowski, K. Kauristie, R. Orus, R. Prieto-Cerdeira, J. J. Valette and M. van de Kamp. Ionospheric Effects on GNSS Performance. *2012 6th ESA Workshop on Satellite Navigation Technologies (Navitec 2012) European Workshop on GNSS Signals and Signal Processing*. 2012, 1–8. DOI: `10.1109/NAVITEC.2012.6423122`.

[84] M. A. Richards, M. A. Richards, J. A. Scheer and W. A. Holm. *Principles of modern radar (Vol. I: basic principles)*. eng. Vol. 1. SciTech Publishing, 2010. ISBN: 9781891121524.

[85] L. Heng, J. J. Makela, A. D. Domínguez-García, R. B. Bobba, W. H. Sanders and G. X. Gao. Reliable GPS-based timing for power systems: A multi-layered multi-receiver architecture. *2014 Power and Energy Conference at Illinois (PECI)*. 2014, 1–7. DOI: `10.1109/PECI.2014.6804565`.

[86] I. Fernández-Hernández and G. Seco-Granados. Galileo NMA signal unpredictability and anti-replay protection. *2016 International Conference on Localization and GNSS (ICL-GNSS)*. 2016, 1–5. DOI: `10.1109/ICL-GNSS.2016.7533686`.

[87] I. Fernández-Hernández, T. Ashur, V. Rijmen, C. Sarto, S. Cancela and D. Calle. Toward an Operational Navigation Message Authentication Service: Proposal and Justification of Additional OSNMA Protocol Features. *2019 European Navigation Conference (ENC)*. 2019, 1–6. DOI: `10.1109/EURONAV.2019.8714151`.

[88] G. Caparra, S. Sturaro, N. Laurenti and C. Wullems. Evaluating the security of one-way key chains in TESLA-based GNSS Navigation Message Authentication schemes. *2016 International Conference on Localization and GNSS (ICL-GNSS)*. 2016, 1–6. DOI: `10.1109/ICL-GNSS.2016.7533685`.

[89] D. Margaria, G. Marucco and M. Nicola. A first-of-a-kind spoofing detection demonstrator exploiting future Galileo E1 OS authentication. *2016 IEEE/ION*

Position, Location and Navigation Symposium (PLANS). 2016, 442–450. DOI: 10.1109/PLANS.2016.7479732.

[90] *Galileo OSNMA tests underway*. https://galileognss.eu/tag/osnma/. 2021.

[91] F. Wang, H. Li and M. Lu. GNSS Spoofing Countermeasure With a Single Rotating Antenna. *IEEE Access* 5 (2017), 8039–8047. DOI: 10.1109/ACCESS.2017.2698070.

[92] F. Wang, H. Li and M. Lu. GNSS Spoofing Detection Based on Unsynchronized Double-Antenna Measurements. *IEEE Access* 6 (2018), 31203–31212. DOI: 10.1109/ACCESS.2018.2845365.

[93] A. Broumandan, A. Jafarnia-Jahromi, S. Daneshmand and G. Lachapelle. Overview of Spatial Processing Approaches for GNSS Structural Interference Detection and Mitigation. *Proceedings of the IEEE* 104.6 (2016), 1246–1257. DOI: 10.1109/JPROC.2016.2529600.

[94] V. Brik, S. Banerjee, M. Gruteser and S. Oh. Wireless Device Identification with Radiometric Signatures. *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking*. MobiCom '08. San Francisco, California, USA: Association for Computing Machinery, 2008, 116–127. ISBN: 9781605580968. DOI: 10.1145/1409944.1409959.

[95] X. Zhou, A. Hu, G. Li, L. Peng, Y. Xing and J. Yu. A Robust Radio-Frequency Fingerprint Extraction Scheme for Practical Device Recognition. *IEEE Internet of Things Journal* 8.14 (2021), 11276–11289. DOI: 10.1109/JIOT.2021.3051402.

[96] A. Ali and G. Fischer. The Phase Noise and Clock Synchronous Carrier Frequency Offset based RF Fingerprinting for the Fake Base Station Detection. *2019 IEEE 20th Wireless and Microwave Technology Conference (WAMICON)*. 2019, 1–6. DOI: 10.1109/WAMICON.2019.8765471.

[97] H. Zha, Q. Tian and Y. Lin. Real-World ADS-B signal recognition based on Radio Frequency Fingerprinting. *2020 IEEE 28th International Conference on Network Protocols (ICNP)*. 2020, 1–6. DOI: 10.1109/ICNP49622.2020.9259404.

[98] M. Ezuma, F. Erden, C. Kumar Anjinappa, O. Ozdemir and I. Guvenc. Detection and Classification of UAVs Using RF Fingerprints in the Presence of Wi-Fi and Bluetooth Interference. *IEEE Open Journal of the Communications Society* 1 (2020), 60–76. DOI: `10.1109/OJCOMS.2019.2955889`.

[99] *OHB System AG Brochures - Galileo -European satellite navigation system (space segment).* `https://www.ohb-system.de/files/images/mediathek/downloads/190603_OHB-System_Galileo_FOC-Satellites_2019-05.pdf`. May 2019.

[100] NI Corp. *Global Synchronization and Clock Disciplining with NI USRP Software Defined Radios.* `https://www.ni.com/fi-fi/innovations/white-papers/20/global-synchronization-and-clock-disciplining-with-ni-usrp-293x-.html`. July 2021.

[101] E. Rebeyrol, C. Macabiau, L. Ries, J.-L. Issler, M. Bousquet and M.-L. Boucheret. Phase noise in GNSS transmission/reception system. *Proceedings of the 2006 National Technical Meeting of the Institute of Navigation*. 2006, 698–708.

[102] G. Caparra, S. Ceccato, N. Laurenti and J. Cramer. Feasibility and Limitations of Self-Spoofing Attacks on GNSS Signals with Message Authentication. *Proceedings of the 30th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2017).* 2017, 3968–3984. DOI: `https://doi.org/10.33012/2017.15402`.

[103] Z. Wu, Y. Zhang, Y. Yang, C. Liang and R. Liu. Spoofing and Anti-Spoofing Technologies of Global Navigation Satellite System: A Survey. *IEEE Access* 8 (2020), 165444–165496. DOI: `10.1109/ACCESS.2020.3022294`.

[104] S. Mallat. A theory for multiresolution signal decomposition: the wavelet representation. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 11.7 (1989), 674–693. DOI: `10.1109/34.192463`.

[105] K. Pearson. "Das Fehlergesetz und Seine Verallgemeinerungen Durch Fechner und Pearson." A Rejoinder. *Biometrika* 4.1/2 (1905), 169–212. ISSN: 00063444.

[106] Y. Préaux and A.-O. Boudraa. Statistical Behavior of Teager-Kaiser Energy Operator in Presence of White Gaussian Noise. *IEEE Signal Processing Letters* 27 (2020), 635–639. DOI: `10.1109/LSP.2020.2988172`.

[107] A. V. Oppenheim. *Discrete-time signal processing*. eng. 3. ed., International ed. Upper Saddle River, N.J. ; Pearson Education, 2010. ISBN: 9780132067096.

[108] R. Hamila, E. Lohan and M. Renfors. Subchip multipath delay estimation for downlink WCDMA system based on Teager-Kaiser operator. *IEEE Communications Letters* 7.1 (2003), 1–3. DOI: 10.1109/LCOMM.2002.807439.

[109] X. Chen and X. Hao. Feature Reduction Method for Cognition and Classification of IoT Devices Based on Artificial Intelligence. *IEEE Access* 7 (2019), 103291–103298. DOI: 10.1109/ACCESS.2019.2929311.

[110] F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, P. Prettenhofer, R. Weiss, V. Dubourg, J. Vanderplas, A. Passos, D. Cournapeau, M. Brucher, M. Perrot and E. Duchesnay. Scikit-learn: Machine Learning in Python. *Journal of Machine Learning Research* 12 (2011), 2825–2830.

[111] R. E. Bellman. *Dynamic Programming*. eng. Princeton: Princeton University Press, 2010. ISBN: 0691146683.

[112] Fraunhofer IIS. *Flexiband USB Front-end*. https://www.iis.fraunhofer.de/de/ff/lv/lok/gnss/simulationtest/flexiband.html/. [accessed 12.04.2022].

[113] E. S. Lohan, M. Koivisto, O. Galinina, S. Andreev, A. Tolli, G. Destino, M. Costa, K. Leppanen, Y. Koucheryavy and M. Valkama. Benefits of Positioning-Aided Communication Technology in High-Frequency Industrial IoT. *IEEE Communications Magazine* 56.12 (2018), 142–148. DOI: 10.1109/MCOM.2018.1701057.

[114] M. Koivisto, A. Hakkarainen, M. Costa, P. Kela, K. Leppanen and M. Valkama. High-Efficiency Device Positioning and Location-Aware Communications in Dense 5G Networks. *IEEE Communications Magazine* 55.8 (2017), 188–195. DOI: 10.1109/MCOM.2017.1600655.

[115] NTIA Special Publication. *Radars and the Electromagnetic Spectrum*. https://www.ntia.doc.gov/legacy/osmhome/reports/ntia00-40/chapt3.htm/. [accessed 22.04.2022].

[116] G. Fortino, M. Pathan and G. Di Fatta. BodyCloud: Integration of Cloud Computing and body sensor networks. *4th IEEE International Conference on Cloud Computing Technology and Science Proceedings*. 2012, 851–856. DOI: 10.1109/CloudCom.2012.6427537.

[117] T. S. Rappaport, J. N. Murdock and F. Gutierrez. State of the Art in 60-GHz Integrated Circuits and Systems for Wireless Communications. *Proceedings of the IEEE* 99.8 (2011), 1390–1436. DOI: 10.1109/JPROC.2011.2143650.

[118] Y. Zhu, Y. Zhu, B. Y. Zhao and H. Zheng. Reusing 60GHz Radios for Mobile Radar Imaging. *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*. MobiCom '15. Paris, France: Association for Computing Machinery, 2015, 103–116. ISBN: 9781450336192. DOI: 10.1145/2789168.2790112.

[119] P. Kumari, J. Choi, N. González-Prelcic and R. W. Heath. IEEE 802.11ad-Based Radar: An Approach to Joint Vehicular Communication-Radar System. *IEEE Transactions on Vehicular Technology* 67.4 (2018), 3012–3027. DOI: 10.1109/TVT.2017.2774762.

[120] E. Grossi, M. Lops, L. Venturino and A. Zappone. Opportunistic Radar in IEEE 802.11ad Networks. *IEEE Transactions on Signal Processing* 66.9 (2018), 2441–2454. DOI: 10.1109/TSP.2018.2813300.

[121] S. D. Liyanaarachchi, C. B. Barneto, T. Riihonen and M. Valkama. Joint OFDM Waveform Design for Communications and Sensing Convergence. *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*. 2020, 1–6. DOI: 10.1109/ICC40277.2020.9149408.

[122] S. Sodagari, A. Khawar, T. C. Clancy and R. McGwier. A projection based approach for radar and telecommunication systems coexistence. *2012 IEEE Global Communications Conference (GLOBECOM)*. 2012, 5010–5014. DOI: 10.1109/GLOCOM.2012.6503914.

[123] 3GPP. *Technical Specification Group Radio Access Network; Study on Downlink Multiuser Superposition Transmission (MUST) for LTE*. Technical report (TR) 36.859. Version 13.0.0. 3rd Generation Partnership Project (3GPP), Jan. 2016.

PUBLICATIONS

PUBLICATION

1

Empowering Heterogeneous Communication Data Links in General Aviation through mmWave Signals

W. Wang, J. Talvitie, E. J. Adamova, T. Fath, L. Korenciak, M. Valkama and E. S. Lohan

IEEE Wireless Communications 26.6 (2019), 164–171
DOI: 10.1109/MWC.0001.1800593

Empowering heterogeneous communication data links in General Aviation through mmWave signals

Wenbo Wang*, Jukka Talvitie*, Eva Jošth Adamová†, Thilo Fath‡, L'uboš Korenčiak†, Mikko Valkama*, and Elena Simona Lohan*,
*Tampere University, Finland, †Honeywell, Czech Republic, ‡Airbus, Germany

Abstract—**We study data transfer links that would enable development of low-cost technologies for increasing safety of general aviation (GA). The solution proposed here is to supplement the existing cmWave solutions with mmWave cellular signals in order to better handle interferences and to reach lower outage probabilities and higher throughputs. Moreover, cellular solutions have the advantage of re-using existing or planned infrastructure, and thus they are expected to require minor additional investments. Our paper aims both at shedding some light on the terminology in GA field and at proposing future viable data-link solutions in GA. We also survey the existing solutions, challenges, and opportunities related to the wireless communication links in GA, and we present several case studies related to the achievable outage probabilities and throughputs under rural and urban scenarios of low-altitude GA vehicles. We conclude that supplementing the existing cmWave wireless links with mmWave wireless connections is a workable solution for affordable communication links for low-altitude GA aircraft.**

I. Introduction and motivation

Currently most of the aircraft operations belong to the *manned aviation* (MA) that refers to operations by aircraft that are piloted by a human on board. At the same time, as the number of operational unmanned aerial vehicles (UAVs) is growing fast, more and more *unmanned aviation* (UA) operations are expected in the future.

The *general aviation* (GA) is defined by International Civil Aviation Organization (ICAO) as all civil aviation operations other than scheduled air services and non-scheduled air transport operations for remuneration or hire. However, this definition is rather broad and it does not classify comprehensively the GA operation class from a research point of view. An essential characteristic of GA which is not reflected in the ICAO definition is that GA is commonly understood as a subclass of the MA class. One important contribution of this paper is to clarify the GA notion in a more detailed manner, as shown in Fig. 1, where categorization of separate aviation classes is visually illustrated.

Nowadays, MA has one of the lowest probability of accidents out of all the means of transport. This was achieved by various systems, technologies, and procedures. In particular, the communication, navigation, and surveillance (CNS) technologies installed on board of aircraft play crucial role to lower the probability of accidents. However, there are still many aircraft that use for example just one piece of communication equipment: the radio (wireless) link for voice communication with air traffic control. Almost all of these aircraft with limited equipment operate under the general aviation category and fly typically only in low altitudes (below 3000 m). GA incorporates also business aviation and it is known that the business jets are among the best equipped aircraft currently flying. Thus, we would like to clarify that for the rest of this paper we use the term *low-altitude GA* (laGA) referring only to a part of GA operations at low altitude and uncontrolled airspace (i.e., explicitly excluding business aviation).

The reason for limited equipment onboard of laGA aircraft is that they are usually used for non-commercial activities (e.g., recreational or philanthropist purposes, research on wild life and climate changes, etc.) and the CNS technologies used for other aviation classes are simply too expensive to be used for these purposes. The UAVs represent another category of aircraft with highly varying level of CNS equipment. Even a small UAV with weight of 2 kg can kill a human when it falls on his/her head or it can seriously damage or even destroy a propeller or a turbofan engine. The rapidly rising number of UAVs, and hence also the risk of potential collisions with other aircraft sharing the same airspace, is a challenge for all of the MA, but mostly for laGA aircraft since they will share the low-altitude airspace with UAVs.

Thus, it is very important to develop affordable CNS technologies for laGA, keeping in mind that many novel solutions that are relevant for laGA, they may become also relevant for UAVs, which in the future will share the same airspace with laGA. These technologies will require a data transfer infrastructure to exchange the information with ground (e.g., traffic management) and with other aircraft that will operate in low altitudes. Such technologies also need to be affordable and quickly deployed. Using the existing and developing cellular infrastructure also for data-link needs of laGA has a large potential to meet all the above requirements.

The use of cellular infrastructure for air traffic at low altitudes has various challenges, e.g., how to decrease the miscommunication errors [1] or how to decrease the outage probabilities. The outages here refer to the situations when the received signal-to-interference-plus-noise ratio (SINR) is below a certain threshold, and thus it is not sufficient to establish and maintain a reliable wireless data link. In addition, both intentional and unintentional wireless interferences are increasing with an increased air traffic, and thus supplementary solutions to the existing ones need to be found. For all of the above reasons, it is highly beneficial to know or to approximate *the path loss* that refers to the deterministic decrease in the signal power due to the wireless propagation over a certain

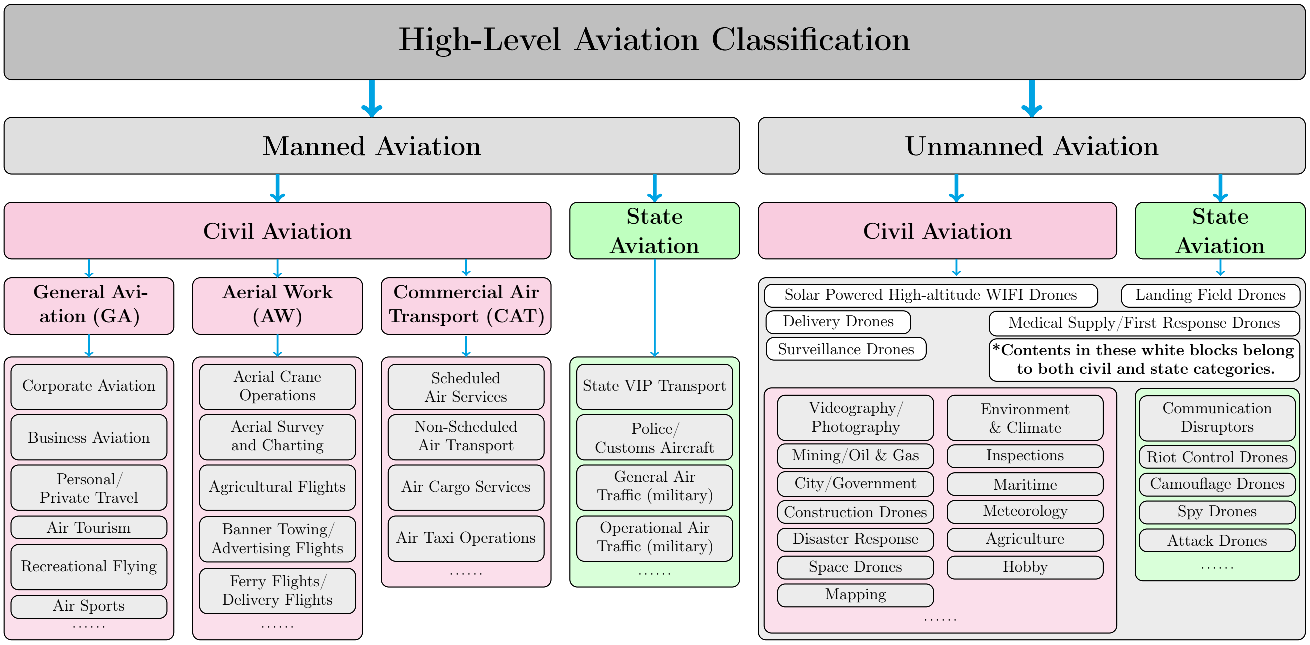


Fig. 1: The main aviation classes.

distance.

The aim of this paper is to promote research in cellular wireless technologies to support low-cost wireless data transfer for aviation purposes, especially for unequipped laGA aircraft and for UAVs sharing the same airspace with laGA aircraft. This will ensure safer future operations, as well as better airspace access for laGA.

We illustrate in a concise manner the existing solutions, the current open challenges, and the opportunities for future laGA data link solutions. We postulate that using the mmWave frequency bands (i.e., data links at carrier frequencies above 30 GHz, that are also to be used for the upcoming 5G cellular communications) can offer viable and robust supplementary solutions to the existing ones, despite their increased path losses. The adoption of mmWave solutions is motivated by the facts that there is currently very low amount of interference in mmWave bands, that beamforming with large or massive multi-antenna processing can boost the wireless channel capacity, and that lower outage probabilities are possible with astute mmWave processing, which would increase the connectivity availability and thus would increase the aircraft safety. More about the mmWave benefits and challenges is discussed in Section IV. In this paper we analyse two concrete case-studies for low-altitude aerial vehicles, namely urban macrocell and rural macrocell cases, and we present the outage probabilities under certain receiver sensitivity requirements, as well as the achievable throughputs (measured in megabits per second or Mbps).

Related Work: Some major trends in wireless communications nowadays, which are likely to affect also the laGA domain in the future, are towards automation, remote controlling, cloud-based processing, and software-defined networking. The communications in the aviation domain, and in particular in laGA domain, make no exception from these trends, but their developments move at a much slower pace than the developments in the terrestrial wireless architectures. This slower-paced development is most likely due to the fact that there are more stringent safety and reliability targets involved. Other emerging trends in aviation, not addressed here, are the Aeronautical Ad-Hoc Networks (AANET) [2], aiming at improved and more reliable communications both between aerial vehicles and between an aerial vehicle and the ground networks, such as cellular (e.g., 5G [3]) and Internet of Things (IoT) networks. The need for enhanced surveillance, communication, and flight management capabilities in MA has been recently emphasized in [4].

As shown in Fig. 1, according to the usage, the aviation domain is typically categorized into manned and unmanned aviation. Each category (i.e., MA and UA) can be further divided into civil aviation and state aviation. While GA aircraft and UAVs fall in different categories as illustrated in Fig. 1 (MA versus UA), they often share the same airspace. Thus, wireless communication solutions for GA are also relevant for UAVs. The GA category is a sub-category of manned civil aviation and laGA is sub-category of GA. The laGA aircraft include utility aircraft (e.g., Cessna 172), sailplanes, aerobatic aeroplanes, research helicopters, etc.

II. Key existing technologies, challenges, and opportunities for the data links in laGA

In this section, we provide a short description of few MA data-transfer technologies that are or might be relevant to the laGA aircraft in the future. The first two technologies listed here are the only ones currently in use for laGA aircraft:

- The *VHF Data (or Digital) Link mode 2 (VDLm2)* is the main version of VHF Data Link and it is currently the primary mode used in the wireless communications links for MA. The VDLm2 uses a differential 8-PSK modulation and transmits at carrier frequency of around 136 MHz with signal bandwidths of 25 kHz. Typical throughputs in VDLm2 are around 31.5 kbps at physical layer.

- Another data-link solution in MA is the *High Frequency Data Link (HFDL)*, reaching low throughputs of up to 1.8 kbps.

VDLm2 and HFDL are air-to-ground (A/G) technologies. In addition, few more expensive solutions, based on satellite communications such as Inmarsat and Iridium, exist and they are mostly used by high-cost GA aircraft. We would like to emphasize the fact that currently, Inmarsat and Iridium technologies and the other experimental solutions described below are not used for laGA, but they are listed here for the sake of completeness and as the focus is on technologies that might be relevant also to laGA in the future:

- *Inmarsat* is both a wireless communication solution and a company focusing on satellite-based communications; their broadband connectivity solutions rely on air-to-satellite (A/S) wireless transmissions, mostly in L-band (i.e., 1–2 GHz). In downlink high throughputs of 50 Mbps are achievable via Inmarsat Global Xpress solutions.
- *Iridium*, like Inmarsat, is another solution, named after a company offering broadband connectivity to passengers of business GA aircraft and commercial airlines, based on satellite communications technologies in L bands. Iridium has its own constellation of 66 operational units. Achievable throughputs are lower than with Inmarsat, and in downlink they can go up to 1.5 Mbps in Iridium NEXT.

Additional solutions discussed in the next bullet points are either in experimental phase or in research phase.

- *European Aviation Network (EAN)* is an experimental communication data link for aviation, built by Inmarsat and Deutsche Telekom and scheduled to become fully operational in 2019. EAN integrates satellites and A/G connectivity networks, using cellular Long Term Evolution (LTE) ground base stations, operating also in L and S cmWave frequency bands. The applicability of EAN solution in laGA is still questionable, as the current EAN business model is focused mainly on the high-altitude commercial aircraft for on-board passenger entertaining broadband services.
- *L-band Digital Aeronautical Communications System* (L-DACS) is another experimental communication data link A/G solution under standardization since Dec 2016. It is based on orthogonal frequency division multiplexing (OFDM) and sharing many concepts with the 4G/LTE cellular communications. L-DACS currently uses L band (cmWave), which interferes with Distance Measuring Equipment (DME) systems used for localizing the aircraft with respect to a benchmark station. Achievable throughputs in L-DACS are up to 1.3 Mbps.
- *Broadband Aeronautical Multi-Carrier system (B-AMC)* is one L-DACS variant. B-AMC currently supports A/G mode, but extensions to A/A mode are currently under investigation. Achievable throughputs in B-AMC are around 300 kbps.
- *Aeronautical Mobile Airport Communication System (AeroMacs)* has also been proposed by Eurocontrol and Federal Aviation Administration (FAA) as a solution to modernize the aircraft communication links. It is based on the commercial 4G WiMAX specifications and it is meant for operation in C-bands, at around 5 GHz, for short-range high data-rate communications, with throughputs up to 10 Mbps.

As seen so far, most of the existing wireless solutions for communication data links use sub-GHz and GHz cmWave signals below 7 GHz and are typically affected by unintentional interference from other aviation signals or ground communication networks (e.g., LTE, FM broadcasting, etc.) In addition, the current spectrum below 7 GHz is very congested not only with other CNS signals used in aviation, but also with signal used in non-aviation systems. Therefore, to increase the robustness, and to be able to offer broader frequency diversity, a complementary solutions should move to higher than 7 GHz frequencies, in particular towards mmWave spectrum, namely frequency bands above 30 GHz.

Supplementing currently existing solutions with mmWave-based solutions can bring several benefits, as described in Section IV.

Table I summarizes the existing data links in MA, by pointing out the current usage of frequency bands, and the challenges and opportunities brought by each of these frequency bands. As seen in Table I, there is a large number of various communication solutions currently available, spanning over multiple frequency bands, but even such a significant number seems not to be sufficient for the future dense and complex airspace [5]. This is because each of the current solutions has its limitations, as illustrated in the fourth column in Table I. As seen in the previous section, the sub-GHz and GHz microwave solutions (i.e., the so-called cmWave solutions) are currently mostly deployed in crowded frequency spectra, namely below 7 GHz, where they have to deal with various inter-system interferences.

We postulate that, in order to solve the current limitations, the future communications for laGA should rely on multi-link capabilities, mmWave communications with localized interferences to supplement the cmWave communications, and multi-aircraft collaborations. The advantages of the communications above 8.7 GHz are illustrated in the last column and last row of the Table I. The mmWave bands according to the definition accepted by the wireless communication community refers to frequencies above 30 GHz. As the bands above 8.7 GHz are currently used very little or unused, there is a low amount of inter-system interference in these bands. In addition, as the carrier frequency increases, the path losses are also higher, meaning that only the transmitters in a vicinity of a communication link would interfere with that communication link (i.e., we have a localized interference, where interference management becomes easier [3]). In addition, larger contiguous bandwidths are available at mmWave bands, e.g., even 100 MHz of contiguous bandwidths, enabling higher throughputs in communication and higher positioning accuracy in navigation applications.

Band	Frequency ranges	Example use in aviation	Challenges	Opportunities

HF	3–30 MHz	2850–22000 kHz:
		A/G communication (HF voice and data)
		3023&5680 kHz:
		Search and Rescue
			Possible interferences from FM broadcasting;
			Many sub-bands here reserved for military aviation applications
				Low path losses;
				Large coverage areas;
				Well-established/traditional aviation solutions

VHF	30–300 MHz	117.975–137 MHz: A/G (voice and data) and A/A communication (voice) 129.15–136.9 MHz: VDLm2, ACARS/HFDL	Crowded frequency bands and interferences from other systems; Low throughputs	Path losses slightly larger than in HF band; Coverage areas still high; Well-established/traditional aviation solutions
UHF or L	0.3–3 GHz	960–1164 MHz: C2 terrestrial link 1.61–1.62 GHz: Iridium 1–4 GHz: Inmarsat	Most crowded frequency bands for aviation are between 1 and 4 GHz; High interferences up to 4 GHz; Current use in GA limited to business jets	Enhanced capacity compared to sub GHz bands; Potential to use existing cellular and IoT infrastructure
SHF or C	3–7 GHz	5.03–5.09 GHz: C2 satellite link AeroMACS	Interferences from other systems, as C band is also used for satellite communications and some synthetic aperture radars (SARs)	High capacity/high throughputs achievable; C band suffers of lower interferences than HF and L bands
SHF (X, Ku, K, Ka bands), V and W	7–110 GHz	Used very little in wireless links for aviation systems (e.g., JetWave)	Very high path losses; Short range; Gaseous absorption above 60 GHz	Very high throughputs achievable; Low and localized interferences; Miniaturized antenna arrays; Efficient beamforming solutions possible

TABLE I: Existing and potential communication data-link technologies in manned aviation.

III. Modelling the low-altitude general aviation channels

A path-loss model of a wireless data link (i.e., A/A, A/G, or A/S) has typically three components: i) a deterministic path-loss component that is distance and frequency dependent; ii) a random shadowing component, modelling the large-scale fluctuations in the path losses, and iii) a random fading component, modelling the small-scale (rapid) fluctuations in the received signal strength. In addition, most of these models are split into a line of sight (LOS) part and a non line of sight (NLOS) part, with an associated LOS probability to define the transition between the two parts. Channel models in aviation were studied for example in [6]–[13], and a summary of the most encountered models for laGA links is shown in Table II.

a) Path losses in A/G channels: The A/G channels (sometimes referred to as A2G or G2A to also illustrate uplink/downlink connectivity) differ from the ground propagation channels in typically higher elevation angles, higher LOS probability and less multipath to deal with [14]. One of the most encompassing A/G channels in the current literature are the recent 3GPP channels [6] covering carrier frequencies up to 100 GHz and aircraft altitudes up to 300 m. The 3GPP aerial channel models [6] expand the urban macrocell (UMa), rural macrocell (RMa) and urban microcell (UMi) terrestrial channel models to aerial operations. The most relevant 3GPP channel models, in the context of laGA, are UMa and RMa, as the base station antenna in UMi is below the roof-top level, and thus unable to serve with adequate quality in-flight aerial vehicles. Aerial channel models could be considered in two parts, namely below 300 m part and above 300 m part. The one above 300 m altitude typically is Free Space Loss (FSL) [9], possibly with some correction parameters, such as those used in the IF-77 FAA channel model, recently re-published by ITU under the name of ITU-R P.2345-0 channel model [7].

b) Path losses in A/A channels: The A/A models assume a base station installed in the moving aircraft and a receiver also installed in another moving aircraft. The A/A models existing in the literature assume 100% LOS and they rely either on a modified FSL model (e.g., by changing slightly the path loss coefficient) or on a simplified path-loss model which is frequency independent (it depends only on the distance between the aircraft). A/A path loss modelling is quite limited in the existing literature.

c) Path losses in A/S channels: A/S channel models are even scarcer in the current literature than A/A models and they typically assume FSL and LOS scenarios.

d) Shadowing and fading: The path-loss models described so far depend on the link type, e.g., A/G, A/A, or A/S. The shadowing and fading models are typically modelled by similar distributions, independently of the link type (i.e., the same statistical distributions with different parameters). The vast majority of papers reporting measurement-based shadowing and fading distributions for aerial vehicles specify a Gaussian distribution in logarithmic scale (i.e., log-normal distribution) for the shadowing effects (i.e., the received signal strength large-scale fluctuations in dB scale obey a Gaussian zero-mean distribution) and a Rician distribution (typically with a strong Rician factor) for the fading effects.

The 3GPP UMa and RMa models [6] are frequently regarded as the benchmark in various literature studies. The Huawei UMa and RMa models [11] are derived from 3GPP models with additional measurements fitting at cmWave bands. The measurements-based fitting is treated as a correction figure to be added to the 3GPP models.

IV. Benefits of mmWave bands and case studies in rural and urban areas

We start first by describing the potential benefits of using mmWave bands for laGA wireless communications.

1. **Better interference rejection capability**: If the interference affects only some of the available frequency

Model	Main parameters	Component	Link type	Observations	Reference
Free Space Loss (FSL)	3D distance, carrier frequency	Path loss	A/G A/A, A/S	Aircraft heights above 300 m	[9], [13]
3GPP	Horizontal distance, carrier frequency, aircraft altitude	Path loss, shadowing, fading	A/G	Aircraft heights up to 300 m; Carrier frequencies below 100 GHz	[6]
FAA IF-77/ ITU-R P.2345-0	3D distance, carrier frequency, mean surface refractivity, antenna heights, elevation angle, surface conductivity, etc.	Combined path loss, shadowing, fading, atmospheric effects	A/G, A/A, A/S	Carrier frequencies below 20 GHz; Based on FSL path loss; Many empirical parameters needed as inputs	[7]
Huawei A/G	Horizontal distance, carrier frequency, aircraft altitude	Path Loss	A/G	These are 3GPP UMa and RMa models with a correction factor	[11]
Gaussian in log scale	-	Shadowing	A/G, A/A, A/S	Shadowing variance varies according to LOS/NLOS profile	[8], [10]
Rician	-	Fading	A/G, A/A, A/S	Rician factor varies according to the link type	[8], [12], [13]

TABLE II: Summary of main channel models suitable for laGA.

bands, an optimally combined solution can choose to operate in the frequency band with the higher SINR. As mmWave signals have higher path losses (as the path losses are inversely proportional with the square of the carrier frequencies), long-distance interferer has lower effects in the mmWave than in the cmWave bands.

2. **Coherent combining gain**, namely a system operating on N frequency bands and combining the N signals in a coherent manner has a theoretical $10\log_{10}(N)$ gain in the signal-to-noise ratio compared to the single-frequency system. Thus combining the existing cmWave solutions with mmWave solutions would enhance the operational SINR.
3. **Higher throughput is theoretically achievable**, due to the higher available contiguous bandwidths as we move at higher frequencies, above $30\,\text{GHz}$.
4. **Lower outage probabilities** are a result of better operational SINR. Indeed, a better operational SINR is achievable due to a lower interference in mmWave than in cmWave at the moment, due to the possibility of using beamforming and massive multiple-input multiple-output (MIMO) to enhance the SINR, as well as due to the diversity gains achievable by combining several carrier frequencies, as mentioned above.

Secondly, we would also like to point out that the use of mmWave bands raises the following challenges which need to be addressed:

1. **Limited ranges**: the higher the carrier frequency, the weaker the received signal power is, and the distance-based losses (called path losses) are major factors limiting the achievable communication ranges and the coverage areas of the ground base station. A high density ground infrastructure can increase the range, but this would also increase the infrastructure deployment costs for mmWave-band transmission.
2. **Need for antenna up-tilting**: in order to communicate with the flying aircraft, the future cellular networks, such as 5G, must support also up-tilted antennas with associated additional components.
3. **Mobility**: to compensate the path losses in mmWave bands and to mitigate the interference in wireless links, the MIMO techniques are applied. The beam alignment for the high mobility user is challenging.

Thirdly, we present two case studies in rural and urban areas, by focusing on outage probabilities and throughputs as performance metrics, respectively. Outage probabilities are generally important metrics in studying the performance of wireless channels [15] and they are particularly relevant in aviation since the reliability of a communication link is directly related to the safety of people on-board of aircraft. We define the outage probability as the probability that the instantaneous SINR drops below a target SINR. The target SINR is related to the receiver sensitivity needed for the receiver to operate correctly, according to target metrics (e.g., bit error rates, symbol error rates, coverage area, etc.). For example, current LTE specifications specify a target minimum SINR $= -5\,\text{dB}$. Future 5G receivers are likely to go down to operational SINR $\leq -30\,\text{dB}$ [3], by taking advantage of beamforming and MIMO gains. Throughputs are obvious performance metrics when the target is to have some broadband services, such as on-board passenger entertainment. The second case study focuses on achievable throughputs under a more futuristic hypothesis, when broadband connectivity will also be available on laGA aircraft.

In the **first case study**, we compare cmWave performance with mmWave performance in terms of outage probabilities. We study the situation where the cmWave-based solutions are affected by interference (e.g., operational SINR $= -5\,\text{dB}$), while the mmWave are in an interference-free case (e.g., operational SINR $= -30\,\text{dB}$). The results are shown in Fig. 2. A receiver bandwidth of $5\,\text{MHz}$ was considered for a fair comparison at all carrier frequencies. Five channel path models were selected among those in Table II, namely the FSL, UMa and RMa from 3GPP specifications [6], and UMa and RMa from Huawei model [11]. UMa cases correspond to urban scenarios, while RMa cases correspond to rural scenarios. The FAA model [8] was not included in our studies, as it depends on many unknown parameters, such as the geometry of the environment, the permittivity of the obstacles between the access nodes (or base stations) and aircraft, etc. The log-

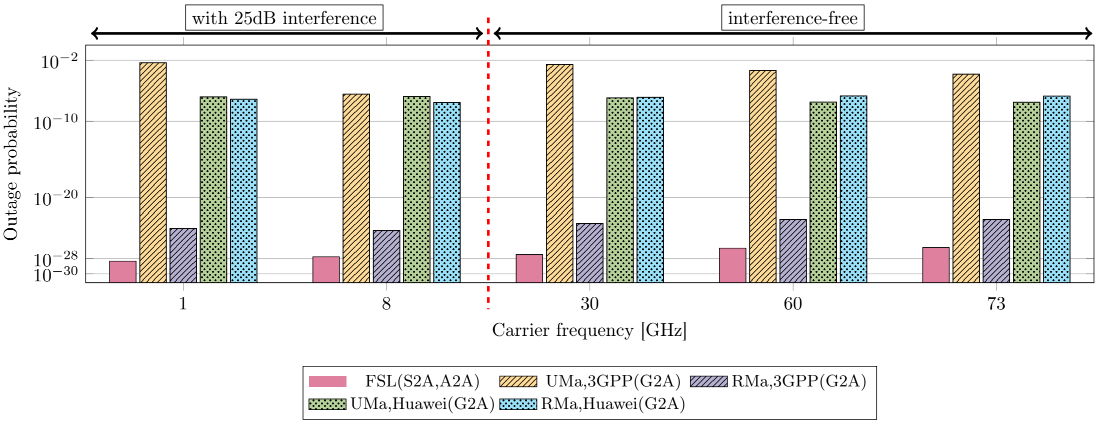


Fig. 2: Outage probabilities in interference-affected scenario in cmWave bands and interference-free scenario for mmWave frequency bands.

normal shadowing and Rician fading were also modelled for all these five channels. When the shadowing is specified in the model (i.e., the 3GPP models), the shadowing parameters from the models were used. In Huawei channel model, we used shadowing parameters from 3GPP for the Huawei UMa and RMa scenarios respectively. This means that in some cases the shadowing was stronger than in the others (e.g., RMa and UMa have slightly different shadowing parameters for both 3GPP and Huawei models). The fading was modelled similarly for all the five channels, according to a Rician distribution with Rician factor varying randomly between 7 and 9 dB. For FSL, a shadowing variance similar with 3GPP RMa LOS shadowing variance was used. In the simulations we used the quasi-LTE signal parameters for the parts including link budget calculations. We also assumed constant antenna gains. The full details on the technical parameters are available at [1] and are not included here due to lack of space. The outage probabilities shown in Fig. 2 range between 4.7×10^{-29} and 4.8×10^{-3} at cmWave bands (i.e., interference prone environment) and between 3.4×10^{-28} and 2.8×10^{-3} at mmWave bands (i.e., interference-free environment), according to the used channel model. FSL gives the lowest outage probabilities at each frequency bands, but they likely are quite unrealistic, as seen from the comparison with the other used channel models. If we compare the different channels considered in Fig. 2 we see that the 3GPP UMa model is the most pessimistic one. We can also see in Fig. 2 that the both Huawei channel models (RMa and UMa) give rather similar results in terms of outage probabilities. This probably happens because Huawei channel models were derived according to UAV-based measurement campaigns at two specific sites (classified as urban and rural), which might not have had sufficient feature to characterize comprehensively urban and rural areas. These results indicate that Huawei models seem to be less suitable than 3GPP models for a good analysis of path losses and outage probabilities for low-altitude GA aircraft.

Our **second case study** focuses on mmWave only, assuming two different receiver bandwidths and taking throughput as the performance metrics. The throughput is a critical criterion in wireless communications, that indicates what kind of operations could be implemented in the channel. We simulated the throughput values based on the five above-mentioned channel models, at 30 GHz carrier frequency, corresponding to the lower bound of the mmWave bands. Both small and large bandwidths were considered (5 MHz in Fig. 3 and 100 MHz in Fig. 4) with a capacity efficiency factor of 0.7. The small-bandwidth case was selected for a fairer comparison to the cmWave bands and in order to provide the lower bounds on the achievable throughputs, while the large-bandwidth case reflects the future trends in wireless communications. The height of aircraft was uniformly varied from 50 m to 3 km, which corresponds to airspace G where most of the flying laGA

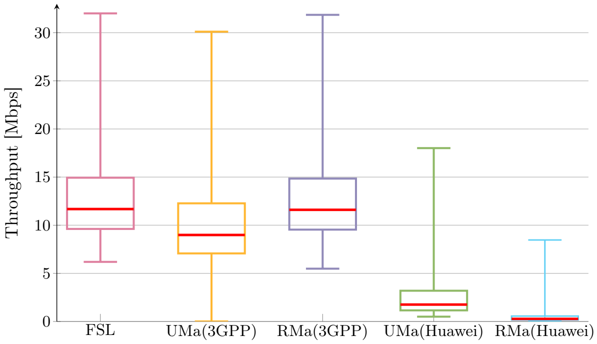


Fig. 3: Throughputs at 30 GHz frequency with 5 MHz bandwidth according to five channel models.

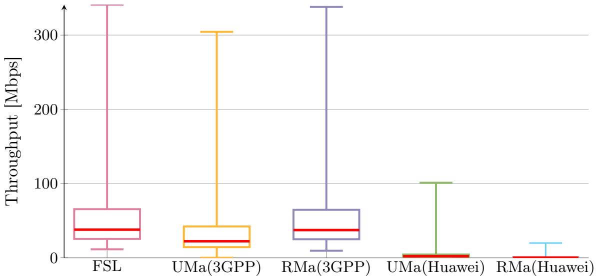


Fig. 4: Throughputs at 30 GHz frequency with 100 MHz bandwidth according to five channel models.

[1] https://bit.ly/2Qg3vC3

aircraft operate. We focus on the **downlink** transmission (i.e., ground-to-air mode), with a base-station transmit power of 43 dBm and a receiver noise figure of 8 dB, in accordance with current LTE specifications (the parameters for simulations of the second use case are available at [1]). The term downlink here is used according to the wireless communication terminology, meaning the link from the (ground) base station towards the aircraft, by distinction with the uplink transmissions, which are from the mobile or aircraft towards the base station.

In the box plots (i.e., Fig. 3 and Fig. 4), we assumed the upper whisker as the 99.7th percentile, the lower whisker as the 0.3th percentile, the upper quartile as the 75th percentile and the lower quartile as the 25th percentile. As expected, the throughput under FSL channel model gives the most promising results, its median is around 12 Mbps with 5 MHz bandwidth and around 38 Mbps with 100 MHz bandwidth. However, such a value is unlikely to be achieved in practice, as FSL is a rather idealistic channel model. Under the 3GPP channel models, with 5 MHz bandwidth, the median values of throughput are about 9 Mbps and 12 Mbps in UMa and RMa scenarios, respectively. Meanwhile, with 100 MHz bandwidth the median values are 22 Mbps and 37 Mbps in 3GPP UMa and RMa scenarios, respectively. 3GPP RMa scenario converges in fact to FSL scenario for altitudes above 300 m. According to the Huawei channel model, the median values of both UMa and RMa scenarios are below 3 Mbps with both 5 MHz and 100 MHz bandwidth, which shows that this model is the most pessimistic among the considered models and can be considered as a lower bound on the performance.

V. Conclusions

In this work, we have reviewed the major challenges and potential technology solutions in the communication data links used in laGA and we have pointed out low interference level, reasonable outage probability and high achievable throughputs of the use of future mmWave signals to supplement the existing cmWave aviation links. The discussion was focused mostly on the physical layer aspects of laGA, as this physical layer design is one of the most critical ones when designing new communication solutions. The advantages of a mmWave-based approach have been shown in terms of achievable outage probabilities and throughputs under five different channel models and for different available channel bandwidths. The predicted values highly depend on the underlying path-loss modelling, with FSL giving overly optimistic upper bounds and with Huawei channel models giving the lower bounds in throughput performance. We recommend the use of 3GPP channel models in the context of laGA data links, as they not only provide an average performance among various considered models, but they are also widely accepted by the research community. Despite the higher path losses at increased carrier frequency, it could be seen that the outage probability of mmWave signals was close to the one for cmWave signals. Therefore the usage of mmWave signals is a promising supplementary solution in addition to the existing ones. Open research directions are the impact of the antenna radiation patterns on the outages and throughputs, modelling more accurately the link budgets according to the upcoming 5G specifications, and investigation of navigation, tracking, and positioning capabilities of the wireless signals for laGA.

Acknowledgement

This work was supported by SESAR Joint Undertaking (SJU) in project EMPHASIS (grant 783198). The opinions expressed herein reflect the authors' view only. Under no circumstances shall the SJU be responsible for any use that may be made of the information contained herein. This work has been also partially supported by the Academy of Finland (grant 313039).

References

[1] B. Molesworth and D. Estival, "Miscommunication in general aviation: The influence of external factors on communication errors," *Safety Science*, vol. 73, pp. 73–79, March 2015.

[2] Q. Luo and J. Wang, "Multiple QoS parameters-based routing for civil aeronautical ad hoc networks," *IEEE Internet of Things Journal*, vol. 4, pp. 804–814, June 2017.

[3] A. Gupta and R. K. Jha, "A survey of 5G network: Architecture and emerging technologies," *IEEE Access*, vol. 3, pp. 1206–1232, July 2015.

[4] Y. Lim, V. Bassien-Capsa, S. Ramasamy, J. Liu, and R. Sabatini, "Commercial airline single-pilot operations: System design and pathways to certification," *IEEE Aerospace and Electronic Systems Magazine*, vol. 32, pp. 4–21, July 2017.

[5] D. W. Matolak, "Hyper-spectral communications, networking ATM as foundation for safe and efficient future flight: Transcending aviation operational limitations with diverse and secure multi-band, multi-mode, and mmWave wireless links: Project overview, aviation communications and new signaling," in *2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC)*, pp. 1–7, September 2017.

[6] "3GPP - 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Study on enhanced LTE support for aerial vehicles (release 15)." 3GPP TR 36.777 V15.0.0, http://www.3gpp.org/DynaReport/36-series.htm, January 2017.

[7] "ITU - Report ITU-R P.2345-0 (08/2015), Defining propagation model for Recommendation ITU-R P.528-3." P Series, Radiowave propagation, August 2015.

[8] D. W. Matolak and R. Sun, "Air-ground channel characterization for unmanned aircraft systems; part i: Methods, measurements, and models for over-water settings," *IEEE Transactions on Vehicular Technology*, vol. 66, pp. 26–44, January 2017.

[9] J. Naganawa, J. Honda, T. Otsuyama, H. Tajima, and H. Miyazaki, "Evaluating path loss by extended squitter signals for aeronautical surveillance," *IEEE Antennas and Wireless Propagation Letters*, vol. 16, pp. 1353–1356, December 2017.

[10] R. Amorim, P. Mogensen, T. Sorensen, I. Z. Kovacs, and J. Wigard, "Pathloss measurements and modeling for UAVs connected to cellular networks," in *2017 IEEE 85th Vehicular Technology Conference (VTC Spring)*, pp. 1–6, June 2017.

[11] K. Wang, R. Zhang, L. Wu, Z. Zhong, L. He, J. Liu, and X. Pang, "Path loss measurement and modeling for low-altitude UAV access channels," in *2017 IEEE 86th Vehicular Technology Conference*, pp. 1–5, Sep 2017.

[12] E. Yanmaz, R. Kuschnig, and C. Bettstetter, "Achieving air-ground communications in 802.11 networks with three-dimensional aerial mobility," in *2013 IEEE 32nd Conference on Computer Communications (INFOCOM)*, pp. 120–124, April 2013.

[13] R. Sun and D. W. Matolak, "Air-ground channel characterization for unmanned aircraft systems; part ii: Hilly and mountainous settings," *IEEE Trans. on Veh. Technology*, vol. 66, pp. 1913–1925, Mar 2017.

[14] N. Ahmed, S. S. Kanhere, and S. Jha, "On the importance of link characterization for aerial wireless sensor networks," *IEEE Communications Magazine*, vol. 54, pp. 52–57, May 2016.

[15] T. D. Cola and M. Mongelli, "Adaptive time window linear regression for outage prediction in Q/V band satellite systems," *IEEE Wireless Communications Letters*, pp. 1–1, April 2018.

PUBLICATION

2

Comparative Analysis of Channel Models for Industrial IoT Wireless Communication

W. Wang, S. L. Capitaneanu, D. Marinca and E. S. Lohan

IEEE Access 7.(2019), 91627–91640
DOI: 10.1109/ACCESS.2019.2927217

Received May 23, 2019, accepted June 22, 2019, date of publication July 8, 2019, date of current version July 25, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2927217

Comparative Analysis of Channel Models for Industrial IoT Wireless Communication

WENBO WANG[1], (Student Member, IEEE), STEFAN L. CAPITANEANU[2], (Member, IEEE), DANA MARINCA[3], (Member, IEEE), AND ELENA-SIMONA LOHAN[1], (Senior Member, IEEE)

[1]Electrical Engineering Unit, Tampere University, 33210 Tampere, Finland
[2]Schneider Electric, 75002 Rueil-Malmaison, France
[3]PRISM Unit, University Paris Saclay, 78035 Saint-Aubin, France

Corresponding author: Wenbo Wang (wenbo.wang@tuni.fi)

This work was supported by the Academy of Finland under Project PRISMA, project number 313039.

ABSTRACT In the industrial environments of the future, robots, sensors, and other industrial devices will have to communicate autonomously and in a robust and efficient manner with each other, relying on a large extent on wireless communication links, which will expand and supplement the existing wired/Ethernet connections. The wireless communication links suffer from various channel impairments, such as attenuations due to path losses, random fluctuations due to shadowing and fading effects over the channel and the non line-of-sight (NLoS) due to obstacles on the communication path. Several channel models exist to model the industrial environments in indoor, urban, or rural areas, but a comprehensive comparison of their characteristics is still missing from the current literature. Moreover, several IoT technologies are already on the market, many competing with each other for future possible services and applications in Industrial IoT (IIoT) environments. This paper aims at giving a survey of existing wireless channel models applicable to the IIoT context and to compare them for the first time in terms of worst-case, median-case, and best-case predictive behaviors. Performance metrics, such as cell radius, spectral efficiency, and outage probability, are investigated with a focus on three long-range IoT technologies, one medium-range, and one short-range IoT technology as selected case studies. A summary of popular IoT technologies and their applicability to industrial scenarios is addressed as well.

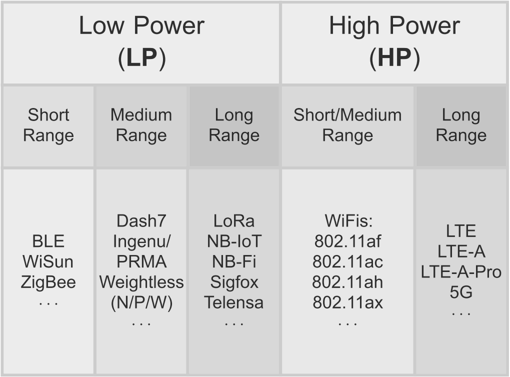
INDEX TERMS 3GPP channel loss models, cell radius, industrial IoT, outage probability, spectral efficiency.

I. INTRODUCTION AND MOTIVATION

Sensors and devices inter-connected through various Internet of Things (IoT) protocols can improve the production steering and ensure a more efficient end-to-end traceability and surveillance along the production chain, provided that the IoT wireless communication links are properly designed to support the target spectral efficiency with minimal interruption levels and limited bandwidth. The IoT wireless communication links span over a wide area of carrier frequencies, from existing centimeter-wave (cmWave) links to future millimetre-wave (mmWave) connections and support a wide area of bandwidths, from Ultra Narrow Band (UNB) communications (such as Sigfox, Telensa, and Weightless-N standards) to spread spectrum (e.g., LoRa, ZigBee, WirelessHART, Ingenu, WAVIoT) and even wideband communications (e.g., WiFi-based IoTs) [1].

The IoT devices can also be classified according to their power consumption. A classification of IoT technologies which can be used in industrial applications is shown in Fig. 1. The IoT solutions can be grouped into low-power (LP) or battery-operated solutions, and high-power (HP) solutions. Each of these two categories can be further grouped according to the communication ranges, into short (e.g., few meters to few tens of meters), medium (e.g., few tens of meters to few kilometers), and long ranges (e.g., ranges up to few tens of km). The vast majority of IoT standards nowadays fall under the LP category (several IoT standards names are enumerated in Fig. 1; details on each standard can be found for example in [1]). The high-power/high-throughput

The associate editor coordinating the review of this manuscript and approving it for publication was Qing Yang.



Low Power (**LP**)			High Power (**HP**)	
Short Range	Medium Range	Long Range	Short/Medium Range	Long Range
BLE WiSun ZigBee ...	Dash7 Ingenu/ PRMA Weightless (N/P/W) ...	LoRa NB-IoT NB-Fi Sigfox Telensa ...	WiFis: 802.11af 802.11ac 802.11ah 802.11ax ...	LTE LTE-A LTE-A-Pro 5G ...

FIGURE 1. Classifications of the connectivity solutions for industrial applications.

solutions are covered by current and emerging Wireless Local Area Networks (WLAN) standards, popularly known as WiFis, and by the cellular communications, such as the existing 4G/Long Term Evolution (LTE) standards and the emerging 5G standard [2], [3].

Industrial IoT market will form a significant part of the future Information, Communication and Technology (ICT) markets [4]. Communications links in IIoT will have to trade the high spectral efficiency for low battery consumption and long-range support [5]. Thus, there will be no winning IIoT technology for all possible applications. Wireless IIoT solutions are meant to enable a predictive management of wireless equipment used at various industrial sites, to increase the workers' safety and production capacity [6], to increase the savings of stakeholders involved in the industrial chain [7], to enable wireless self-localization of electronic devices and components in 3D industrial space [8], etc.

Examples of potential industrial applications for existing IoT technology are summarized in Table 1 for 18 of the most encountered IoT solutions. The communication range is specified for each of these technologies, together with existing uses in IIoT. A 'not available' (n/a) input does not mean that such technology cannot be used in that particular scenario, but rather that, to the best of the authors' knowledge, no industrial solutions have been tested so far under that particular scenario. The considered scenarios are divided into: rural, urban, and indoor, according to the typical classification of channel models [9], but it is worth mentioning that the boundaries between these three scenarios are not very strict.

No prevalent IoT technology for industrial applications exist, as the choice of a good technology should rely on a multi-criterion decision making process [10], [11], which takes into account the ease of installation and maintenance of a certain technology, its scalability and robustness, its privacy, its power consumption, and its range.

Three widely encountered long-range IoT technologies in industrial applications are LoRa (e.g., flower industry [12], chemical emission monitoring [13], etc.), Sigfox, and NB-IoT. One novel medium-range industrial IoT technology is MIOTY, claiming that it is the first technology following the European Telecommunications Standards Institute (ETSI) low throughput networks standard [14]. One widely encountered short-range technology in industrial IoT is ZigBee. These five technologies, namely NB-IoT, LoRa, Sigfox, MIOTY, and ZigBee, are selected as case studies in our paper, but we remark that similar studies for additional IoT technologies are straightforward to implement based on the methodology presented here.

In order to accurately model the wireless communication links between any two IoT devices, one acting as a transmitter and the other one as a receiver, a link budget analysis is always necessary and it needs to rely on a specific channel model. Link budget refers to balancing the received powers in uplink and downlink directions, by taking into accounts the transmission powers, the antenna gains, and the losses encountered over the wireless propagation channel. The channel modeling typically includes the distance-dependent and deterministic path losses, and the spatio-temporal random effects due to shadowing, multipath, and Doppler effect.

To the best of the authors' knowledge, no comprehensive analysis of existing channel models and their applicability to industrial IoT environments exist and this is the gap we plan to address in our paper. The authors' main contributions are: (1) the analysis of the benefits of the path-loss channel modeling for IIoT applications, (2) the comprehensive description of path-loss channel models for various IIoT technologies (as the formulas presented in here cannot be found in an unified form elsewhere, to the best of the authors' knowledge), (3) the derivation of best-case, median-case, and worst-case bounds for rural, urban, and indoor scenarios for IIoT applications based on existing path-loss models, and (4) the analysis of five IIoT case studies, relying on five different IoT technologies, in terms of cell radius, spectral efficiency, and outage probabilities.

The rest of the paper is organized as follows. In Section II, we briefly discuss the importance of channel modeling in designing an IIoT system. An comprehensive description and discussion of channel loss models are given in Section III. Section IV lists the link budget and other information of selected IoT technologies, NB-IoT, LoRa, Sigfox, Zigbee and MIOTY. In Section V, VI and VII, three metrics, namely the coverage area, spectral efficiency and outage probability, are studied based the selected IoT technologies in Section IV. Section VIII concludes this work and provides some insights of open research in IIoT.

II. THE BENEFITS OF ADEQUATE PATH-LOSS CHANNEL MODELING FOR THE IIOT APPLICATIONS

As already mentioned in the first section, the wireless channel modeling part plays an essential role in choosing the right IIoT technology and building efficient IIoT solutions. An adequate channel modeling allows a designer to estimate and forecast the losses and random fluctuations over the signal power when sent information over a wireless link.

TABLE 1. Visions of industrial applications per IoT technology type according to the channel scenario.

	Technology	Range	Rural (forest industry, agriculture, etc.)	Urban	Indoor (warehouses, mines, industrial halls, etc.)
Low power	BLE/BLE mesh	short	n/a	Smart metering	Smart warehouses with fully automated 3D storage system
	Dash 7	medium	Food monitoring and tracking		
	EC GSM-IOT	long	Monitoring temperature fluctuations in the cold chain or other supply chains; predictive maintenance of goods in a supply chain		n/a
	Ingenu/RPMA	long	Utility monitoring and management (street lightening, hot-water heaters, cool pumps, etc.)		n/a
	LoRa	long	Remote control of industrial sensors in harsh environments (indoor air quality monitoring, liquid presence detectors, industrial temperature monitoring, etc.); smart asset management; waste management		
	NB-Fi (WAVIoT)	long	Remote temperature control in stored food; smart metering; environmental sensing for worker safety (CO2 level, moisture level, etc.)		
	NB-IoT	long	Utility management, asset tracking	Security control	Factory lightening
	Sigfox	long	Tracking workers for safety/geofencing alerts		
	Telensa	long	Utility monitoring		
	Weightless N/P/W	medium	n/a	Smart metering	Shelf autonomous updating
	WeightlessHART	short	n/a	Industrial process control and asset management	
	WiSUN	short	n/a	Smart utility network	
	ZigBee/ZigBee-NaN	short	n/a	Industrial control and sensing applications	
	MIOTY	medium	Mining, gas and oil	Smart metering and industrial sensing applications	
	Wirepass Mesh	long	n/a	Smart metering, factory lighting and asset tracking	
High power	WiFi	long	n/a	Remote control and monitoring of industrial equipment, electronic instrumentation	
	LTE/LTE-A/LTE-A-Pro	long	Industrial gateways in harsh environments	Remote control and monitoring	
	5G	long	Smart manufacturing, smart utility networks, remote energy control, augmented and virtual reality-based industrial solutions, etc.		

The designer could also use the channel models to approximate the cell radius or coverage areas for a particular technology, the outage probabilities under a certain network topology or Access Node (AN) density, the required dimensions of the infrastructure (e.g. number and placement of ANs), etc. Being able to model accurately the wireless channel effects is an important step towards a reliable and efficient design of a wireless IIoT solution. With the help of the channel models, a designer is able to:

- Estimate the operational Signal-to-Noise Ratio (SNR) for a particular industrial application in a particular environment;
- Estimate the density of access nodes required to cover a certain industrial area;
- Estimate the uplink (UL) and downlink (DL) coverage areas and balance the link budgets (i.e., the received powers in UL and DL directions);
- Understand if a certain IoT technology is suitable only in a specific scenario (e.g., rural versus urban) or can be easily scaled to various scenarios;
- Estimate the spectral efficiency of a certain network in terms of supported number of sensors or nodes and achievable throughput under limited bandwidth;
- Allow an efficient network planning in IIoT and reduce the installation and maintenance costs;
- Enable a predictive management of equipment, e.g., predicting failures in various electronic components and ensure their timely replacement;

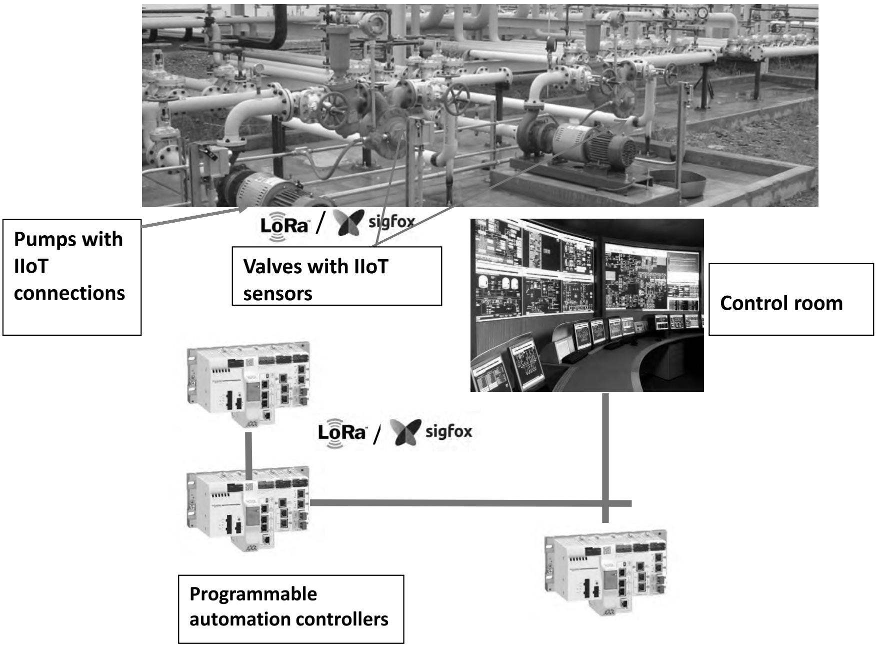

Pumps with IIoT connections
LoRa / sigfox
Valves with IIoT sensors
Control room
LoRa / sigfox
Programmable automation controllers

FIGURE 2. Example of an outdoor IIoT application: Pumps with IoT sensors.

- Permit cost savings through remote control and updating of various components and devices in the industrial chain (e.g., yard and asset management, fleet tracking, etc.);
- Facilitate the wireless geo-localization of captor industrial sensors and other measurement sensors.

Different IIoT applications may operate in different scenarios, such as rural versus urban, or outdoor versus indoor. Thus, it makes sense that the channel models to be used will also be adapted to the scenario targeted by a particular application.

An example of outdoor IIoT application, for both urban and rural cases, is illustrated in Fig. 2: the distribution pumps (e.g., for water, gas, or petrol) can be equipped with IoT sensors, e.g., based on a long-range IoT technology such as LoRa or Sigfox, and the sensors can transmit in a timely manner anomalies in the distribution chain to a control center, as well as they can enable an optimization of the distribution and they can control the pressure and flow in the pipes.

Another IIoT example, this time for an indoor scenario, is illustrated in Fig. 3 for a building management system based on ZigBee (or other short-range IoT) sensors. The IoT sensors would permit to remotely monitor the installation at every level, from the incoming circuit breaker to the final electrical load. The IoT sensors would also ensure real-time alarms and email notifications for voltage loss and overload trips, pre-alarm notifications in the event of an overload, etc.

The channel modeling for IIoT applications has yet to be addressed in detail in the existing literature. From the state-of-the-art in this field it is worth mentioning that a channel model for industrial applications based on LoRa technology has previously been studied in [12]. It was shown in [12] that up to 6000 nodes can be served with a single access node (or gateway) in an indoor industrial area with a surface of 34000 m^2, assuming a simplified single-slope path-loss channel model with measurement-fit coefficients, as described in [15]. No comparison between various channel models was given in [12]. Another path-loss model based on LoRa was studied in [16] for indoor IIoT applications. The channel model in there relied on a two-slope simplified path-loss model and was not validated by measurements. Other channel models proposed in the literature for IIoT applications are variants of the simplified single-path model, e.g., a single-slope path loss model for ZigBee indoor IIoT applications [17], a single-slope path loss model for generic Received Signal Strength (RSS) estimation, with parameters adjustable according to the temperatures [18].

In addition to the literature dedicated to IoT applications, 3GPP has been developing more general channel models, covering various 5G applications scenarios, from terrestrial to aerial communications and from LP to HP applications and they have been grouping them under three main categories: rural, urban, and indoor [9]. The 3GPP models will be discussed in Section III. The applicability of the 3GPP indoor

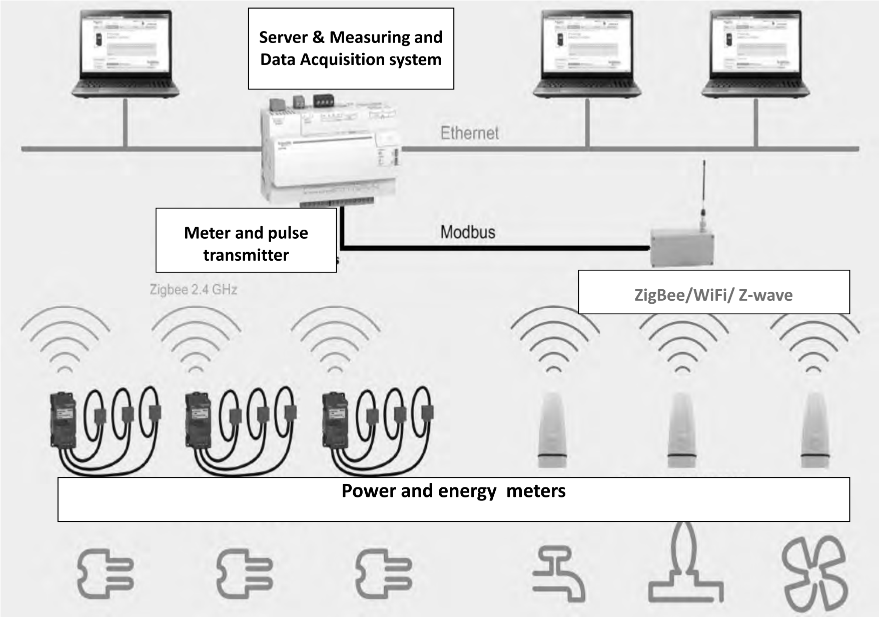

Server & Measuring and Data Acquisition system
Ethernet
Meter and pulse transmitter
Modbus
Zigbee 2.4 GHz
ZigBee/WiFi/ Z-wave
Power and energy meters

FIGURE 3. Example of an indoor IIoT application: Building management system with energy and power metering.

hotspot channel model to IIoT scenarios has been also studied previously by the authors in [19]. However, only the indoor propagation models were analyzed in [19] and the conclusion was that outage probabilities constraints in industrial IoT can be reached with cmWave propagation, but more research is needed to improve the achievable spectral efficiency and outage probabilities in mmWave ranges under the considered indoor scenarios.

As seen above, there is only a limited coverage of the path-loss channel modeling applicable to IIoT scenarios in the existing literature and a comparison between the existing models under both outdoor and indoor scenarios is still lacking. In addition, most of the reported models rely on a single-slope path loss model with environment-dependent parameters (i.e., apparent transmit power and path-loss coefficient) and they require scenario-specific measurement campaigns to estimate the model parameters. In what follows we describe several path-loss models developed in the existing literature for rural, urban, and indoor scenarios and we will look at the worst-case, median-case, and best-case predicted values under different metrics in order to be able to pinpoint the most relevant models in the context of IIoT.

III. ANALYSED CHANNEL MODELS

A variety of wireless terrestrial channel models has been developed in the literature and a designer has typically a wide pool to choose from. However, in the context of IIoT, a comparison between the main features of these different channel models is hard to find in the existing literature. The next sub-sections present seven identified wireless channel models from the literature and discuss their applicability in an IIoT context: the free space loss model, the single-slope model, the 3GPP models (four variants, according to target scenario, detailed in Table 4 and 6), and the industrial indoor channel models (two variants, detailed in Table 4). Additionally, the industrial environment is complex, and usually featured by large obstacles, multiple reflections and frequent movements. To tackle with these issues, the shadowing is used to model the effect caused by the large obstructions in the propagation path and the small-scale fading is used to model the effect caused by the multipath and the movement of subjects in the environment. The discussion of shadowing and small-scale fading follows the descriptions of the channel loss models in each sub-section. In Sections V, VI and VII, we will analyze and compare numerically the channel models with fixed parameters (i.e., by dropping out the single-slope channel model, which is a generic model, with an infinity of possible parameters), in terms of various metrics relevant to industrial environments.

A. FREE SPACE LOSS MODEL

The **Free Space Loss (FSL)** model is often used as a theoretical lower bound and a performance benchmark in all wireless channel modeling studies. Its advantages stay in its low complexity, its low number of parameters, and its easy mathematical tractability. Its main drawback is the fact that it is usually too idealistic to measure practical industrial environments and can offer only a very loose bound in performance, as it will be also obvious from our studies in Sections V, VI and VII. FSL has been used as a bound also in other IoT-related studies, for example for wireless propagation over sandy terrains [20] or in oil rigs [21].

In a FSL, the received power P_R (in dB) at a distance d_3D (in m) from the transmitter is given by,

$$P_\mathrm{R} = P_\mathrm{T} - PL_\mathrm{FSL}(d_\mathrm{3D}) \tag{1}$$

where P_T is the transmit power and PL_FSL is the free space path loss in dB scale defined in Table 4.

The shadowing and small-scale fading is not applicable in FSL model.

B. SINGLE-SLOPE SIMPLIFIED PATH LOSS MODEL

The generic single-slope path loss model is encountered in a vast majority of papers [17], [18], [22] related to wireless communications. This model is given in terms of received signal strength P_R according to two parameters: an apparent transmit power and a path-loss (or slope) coefficient:

$$P_\mathrm{R} = P_{\mathrm{T_a}} - 10n\log_{10}(d_\mathrm{3D}) \tag{2}$$

where n is the path loss coefficient, $P_{\mathrm{T_a}}$ is the apparent transmit power, typically measured as the power at 1 m away from the transmitter. The carrier frequency effect is implicitly included in the $P_{\mathrm{T_a}}$, but it does not appear any more as a model parameter.

In this simplified (and generic) model, the path loss coefficient n and $P_{\mathrm{T_a}}$ are typically derived based on measurements and are valid only for a particular scenario. The shadowing and small-scale fading are usually modeled as additive random variables following the log-normal distribution and Rician distribution respectively. The simplicity of the model makes it widely adopted by many research papers [17], [18], but the fact that n and $P_{\mathrm{T_a}}$ do not have unique values makes it unsuitable to be included in a comparison as such. Indeed, FSL can be seen as particular case of this simplified single-scope model.

C. 3GPP OUTDOOR AND INDOOR CHANNEL MODELS

3GPP standardization has been recently dedicated a significant amount of work for modeling the terrestrial wireless channels for a variety of applications, in particular related to the New Radio (NR) and 5G developments. The 3GPP channel models are built on a multitude of parameters determined empirically from various measurement campaigns and they have been grouped into three main categories: rural, urban, and indoor. In [9], terrestrial channel models that could be widely applied from 0.5 GHz to 100 GHz carrier frequency were proposed. In [3] the extension of models up to 300 m (300 m altitude is usually considered as the low altitude) is presented.

All 3GPP channel loss models describe the shadowing effects as additive random variables following zero-mean log-normal distribution $\mathcal{N}(0, \sigma^2)$ (details see Appendix A Table 4). The small-scale fading is modeled as additive random variables following Rician distribution Rice(K) (details see Appendix A Table 5).

1) 3GPP RMA

The **Rural Macrocell (RMa)** model of 3GPP [9] characterizes the channel loss of rural areas with a base station height h_BS (in meter), a robot height h_UT (in meter), an average street width W (in meter), and an average building height h (in meter). In 3GPP RMa model, the height of base station is assumed to range from 10 m to 50 m, the height of robot is from 1 m to 10 m, the street width is from 5 m to 50 m, the building height is from 5 m to 50 m. The model uses a breakpoint distance d_BP (in meter) concept to divide the path loss calculation into two parts: i) one with the horizontal distance d_2D (in meter) smaller than breakpoint distance and ii) the other with the horizontal distance greater than breakpoint distance.

In Appendix A Table 4, eq. (12) and (13) are path loss in RMa line-of-sight (LoS) and non-line-of-sight (NLoS) scenarios, respectively. Table 6, eq. (22) gives the LoS probability for 3GPP RMa scenario.

2) 3GPP UMA

The **Urban Macrocell (UMa)** model of 3GPP [9] characterizes the channel losses of urban areas in the situation when the base station antenna is above rooftops. 3GPP UMa model is constructed also taking into account the base station height and robot height. The height of base station ranges from 10 m to 50 m, the height of robot ranges from 1.5 m to 22.5 m. Similarly with the 3GPP RMa model, 3GPP UMa model also uses the breakpoint distance concept d'_BP (in meter) to divide the path loss calculation into two parts. However, unlike the 3GPP RMa model, it approximates the breakpoint distance by taking into account the effective environment height h_E (in meter) rather than only considering base station height and robot height as in 3GPP RMa model.

In Appendix A Table 4, eq. (14) and (15) show the path loss in UMa LoS and NLoS scenarios, respectively. Table 6, eq. (23) gives the LoS probability in UMa scenario. The effective environment height yields to eq. (3a), the effective antenna height of robot h'_UT (in meter) and the effective antenna height of base station h'_BS (in meter) are given in eq. (3b) and (3c),

$$h_\mathrm{E} = \begin{cases} h_\mathrm{UT} \leq 13\text{ m} \quad \text{or} \quad d_\mathrm{2D} \leq 18\text{ m}, \\ 1; \\ 13\text{ m} < h_\mathrm{UT} \leq 22.5\text{ m} \quad \text{and} \quad d_\mathrm{2D} > 18\text{ m}, \\ \frac{5}{4}\left(\frac{h_\mathrm{UT} - 13}{10}\right)^{1.5}\left(\frac{d_\mathrm{2D}}{100}\right)^{3} e^{\left(-\frac{d_\mathrm{2D}}{150}\right)}. \end{cases} \tag{3a}$$

$$h'_\mathrm{UT} = h_\mathrm{UT} - h_\mathrm{E} \tag{3b}$$

$$h'_\mathrm{BS} = h_\mathrm{BS} - h_\mathrm{E} \tag{3c}$$

3) 3GPP UMI

The **Urban Microcell (UMi)** model of 3GPP [9] characterizes channel loss of urban areas in the situation when the base station antenna is below rooftops. 3GPP UMi model also takes into account the base station height and robot height. The height of base station is set to 10 m in the 3GPP UMi and the height of robot is from 1.5 m to 22.5 m. Like 3GPP RMa and UMa models, 3GPP UMi model uses a breakpoint distance d'_{BP} concept as well and applies the exact breakpoint distance calculation as the UMa model. However, in UMi model the effective environment height is defined as 1 m.

In Appendix A Table 4, eq. (16) and (17) are path loss in UMi LoS and NLoS scenarios, respectively, in Table 6, eq. (24) gives LoS probability in UMi scenario.

4) 3GPP INH

The Indoor Hotspot (InH) model of 3GPP [9] characterizes channel loss in indoor areas where low mobility of objects, strong reflection of signals and many obstacle of path are existed. InH model is categorized into two cases: i) **the mixed office (InHm)** and ii) **the open office (InHo)**. The difference in the two categories stays in the LoS probability calculation, which allows higher probability of LoS situation in open office than in mixed office. In Appendix A Table 4, eq. (18) and (19) are path loss in InH LoS and NLoS scenarios respectively, in Table 6, eq. (25) gives LoS probability in mixed office case, eq. (26) gives LoS probability in open office case.

D. INDUSTRIAL INDOOR CHANNEL LOSS MODEL

In [23], an industrial indoor channel loss model is proposed according to an extensive measurement campaign. The channel loss model focuses on the Industrial Scientific Medical (ISM) band, namely 900 MHz, 2400 MHz and 5200 MHz. In the paper, our interest is the channel characteristics in 900 MHz and 2400 MHz, whose path loss models are given in Appendix A Table 4, eq. (20) and eq. (21).

The model gives considerations of two scenarios: the low multi-path effect scene and the high multi-path effect scene. Moreover, the movements of obstacles in the environment and the movements of receivers/transmitters are also taken into account.

The shadowing effect is characterized as additive random variables following zero-mean log-normal distribution $\mathcal{N}(0, \sigma^2)$ (details see Appendix A Table 4). The small-scale fading is modeled as additive random variables following Rician distribution Rice(K) (details see Appendix A Table 5).

E. OVERALL PATH-LOSS MODEL USED IN OUR STUDIES

In some channel models (e.g., 3GPP models in section III-C), channel loss is investigated in LoS and NLoS situations, while others (e.g., the industrial indoor model in section III-D), channel loss is given without distinguishing LoS and NLoS situations. In order to use the channel loss models reviewed in this section to evaluate different IoT technologies in Section V, VI and VII, here we define an overall path loss model as follows,

$$PL_{\text{overall}} = \Pr_{\text{LOS}}(L_{\text{LOS}}) + (1 - \Pr_{\text{LOS}})(L_{\text{NLOS}}) + \zeta \quad (4)$$

where PL_{overall} denotes the overall path loss, $\Pr_{\text{LOS}}$ denotes the LoS probability, ζ denotes the small-scale loss, L is defined as the total large-scale loss,

$$L_{\text{LOS/NLOS}} = PL_{\text{LOS/NLOS}} + \xi_{\text{LOS/NLOS}} \quad (5)$$

where $PL_{\text{LOS/NLOS}}$ denotes the path loss median value in the LoS or NLoS situation, $\xi_{\text{LOS/NLOS}}$ denotes the shadowing loss in the LoS or NLoS situation.

TABLE 2. Link budgets for various IoT solutions (Downlink).

Parameters	NB-IoT (standalone)	LoRa (*SF=12)	Sigfox	Zigbee	MIOTY [27]
Modulation	**OFDM	**CSS	**UNB	**DSSS	**TS-UNB
Transmit power [dBm]	43	14	27	20	14
Bandwidth (B) [kHz]	180	125	0.6	2000	25
Receiver Noise Figure [dB]	5	5	5	5	8
Maximum Coupling loss (MCL) [dB]	164	151	161	118	154
Receiver Sensitivity [dBm]	-121	-137	-134	-98	-140
Carrier Frequency [MHz]	900	868	868	2400	868

*SF denotes spreading factor. In LoRa technology, the receiver sensitivity is −137 dBm when the SF is 12;
**OFDM denotes Orthogonal Frequency Division Multiplexing, CSS denotes Chirp Spread Spectrum, UNB denotes Ultra Narrow-Band, DSSS denotes Direct Sequence Spread Spectrum, TS-UNB denotes Telegram-Splitting-Ultra-Narrow-Band [14].

IV. LINK BUDGETS USED IN OUR ANALYSES

The link budget of a system reflects many aspects in the transmitter-receiver chain, for example, the maximum coupling loss, the trade-off between bandwidth and transmitted power. As motivated in the introductory sections, we select five technologies, namely NB-IoT, LoRa, Sigfox, Zigbee and MIOTY, to present and compare their link budget. Based on [14], [24]–[27], the link budget is shown in Table 2.

Among NB-IoT, LoRa, Sigfox, Zigbee and MIOTY technologies, NB-IoT promises the best tolerance of coupling loss (i.e., 164 dB) in the transmitter-receiver chain, Zigbee has the highest bandwidth (i.e., 2 MHz), and MIOTY with TS-UNB modulation provides the best receiver sensitivity (i.e., −140 dBm).

V. COVERAGE AREAS

In this section, we applied both the reviewed channel loss models from Section III and the link budgets from Section IV

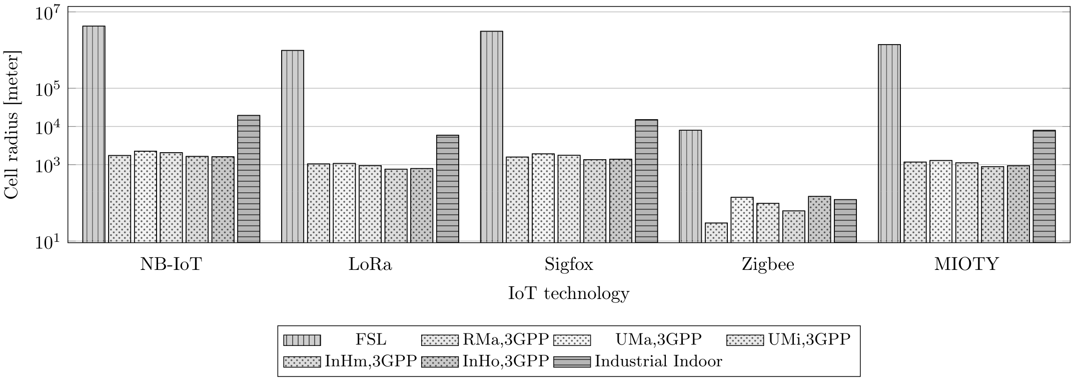


FIGURE 4. Cell radius of different technologies under different channel loss models at 1% outage probability. (FSL denotes Free Space Loss; RMa,3GPP denotes 3GPP Rural Macrocell; UMa, 3GPP denotes 3GPP Urban Macrocell; UMi, 3GPP denotes 3GPP Urban Microcell; InHm, 3GPP denotes 3GPP Indoor hotspot mixed office; InHo, 3GPP denotes 3GPP Indoor Hotspot open office; Industrial Indoor denotes Industrial Indoor channel loss model.).

to estimate the radius of a cell coverage area according to a target outage probability at cell edges. With a specific target metric, for example the target bit rate or the target outage probability, we could find the boundary of a cell service coverage area.

The outage probability is defined as the probability that overall path loss in (4) is greater or equal to maximum coupling loss. This is the minimum requirement that maintains connection of a wireless link. The mathematical expression is,

$$P_{\text{out}} = \Pr(PL_{\text{overall}} \geq \text{MCL}) \tag{6}$$

We set the outage probability P_{out} equal to 1% and find the appropriate horizontal distance (i.e., the cell radius). In this estimation, we assumed that the height of robot is 2 m, the height of access node (AN) is 10 m, the average height of buildings is 5 m and the average width of street is 20 m. The cell radius predicted by different channel models at 1% outage probability are shown in Fig. 4. The best-case is clearly predicted by FSL, but it is overly optimistic. The worst-case and median-case are also numerically shown in Table 3, and compared with other values reported in the literature.

In Table 3 we also presented the reported or measured cell range for comparison purposes. For example, in Sigfox technology, reported range from [31] is from 3000–10000 m, however in [32] the authors measured 600 m cell range in urban area. Our median-case predictors, obtained with 3GPP channel modeling, seem to predict quite close the average reported values for these technologies from other researchers. From Fig. 4 and Table 3, based on the models we reviewed, NB-IoT clearly beats the other four technologies with a median cell range 2061 m. Sigfox also has a good coverage with a median cell range 1754 m. Zigbee has the worst coverage, as expected, since it is targeting for short-range IoT applications.

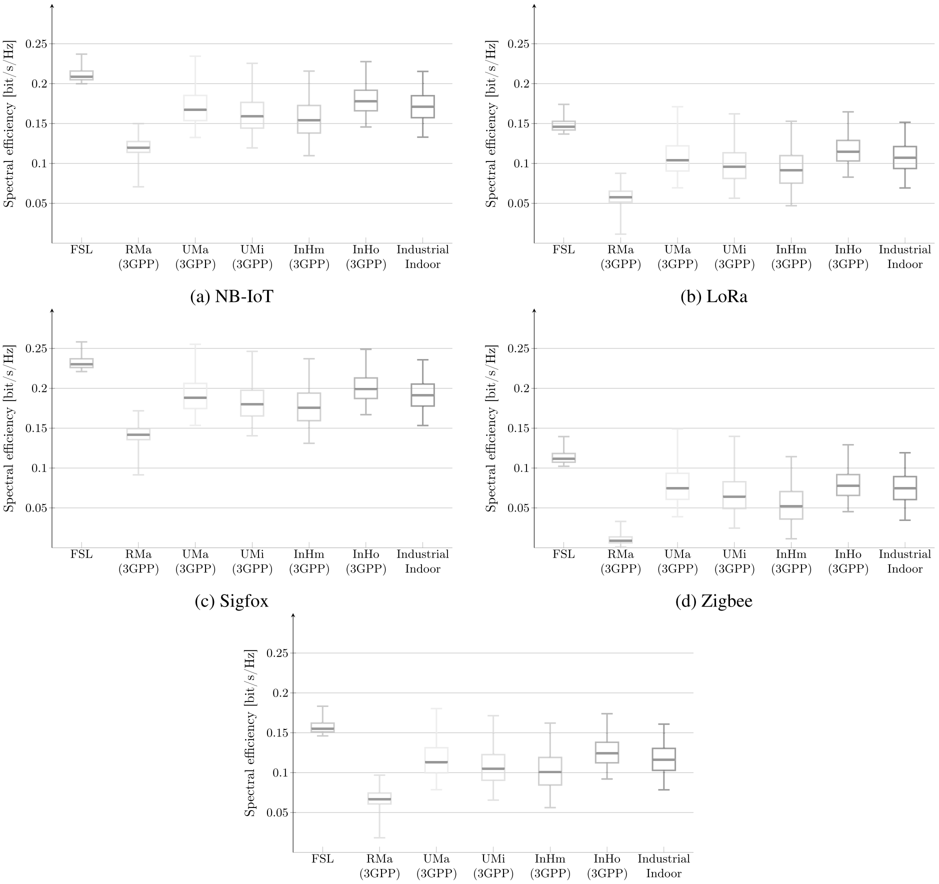
Last but not the least, we would like to highlight that from the point of view of the cell radius study, the 3GPP models seem the most reasonable models to approximate the channel path losses. From Fig. 4, the FSL usually gives an upper bound of cell radius; the industrial indoor model fails to predict the cell radius when the MCL is large, due to the unbelievable large predicted cell radius. The NB-IoT, LoRa, Sigfox and MIOTY are assumed to be candidates in the industrial indoor applications, however according to the cell radius estimated by the industrial indoor model, the above four technologies have better coverage in indoor rather than in outdoor (e.g., the results from 3GPP UMa), which is unlikely to be true. The industrial indoor model, nevertheless, provides some insight in the Zigbee technology, according to its prediction of cell radius, the industrial indoor environment is in between indoor open office and mixed office.

TABLE 3. Cell range of different technologies.

Technology	Predicted cell range from studied models		Cell range measured or reported from literatures
	worst value [m]	median value [m]	reported value [m]
NB-IoT	1609	2061	1000–8000 in [28]
LoRa	765	1046	3400 in [29], 2000 in [30]
Sigfox	1356	1754	3000–10000 in [31], 600 in [32]
Zigbee	29.7	122	30–50 in [33]
MIOTY	890	1712	claimed 5 km urban/ 15 km flat terrains [27]

VI. SPECTRAL EFFICIENCY

In most of the IoT technologies which can be applied to various industrial sites, the achievable spectral efficiency may



(a) NB-IoT

(b) LoRa

(c) Sigfox

(d) Zigbee

(e) MIOTY

FIGURE 5. Spectral efficiency comparisons among NB-IoT, LoRa, Sigfox, Zigbee and MIOTY technologies. The result is based on 100 Monte Carlo runs (the Monte Carlo method is a statistical sampling technique [34], [35]).

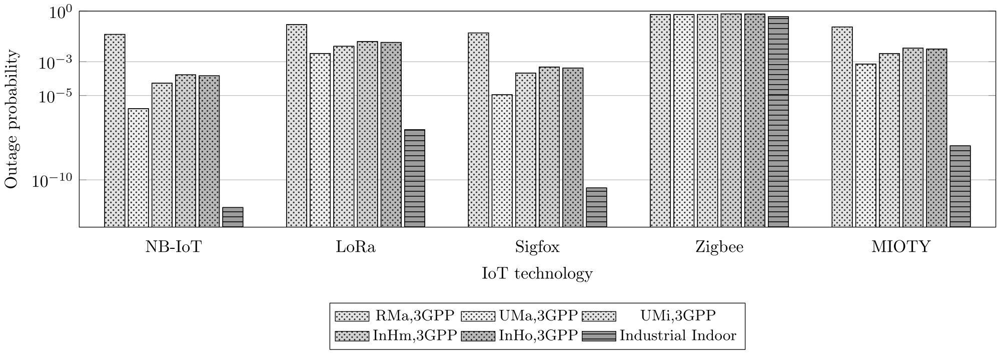


FIGURE 6. Outage probability of different technologies under different channel loss models.

vary in a large extent due to different industrial environments. This section analyses the five selected IoT technologies in terms of spectral efficiency.

The spectral efficiency C (in bits per second per Hz or bit/s/Hz) is limited by the duty cycle of certain devices [36], in the downlink, the spectral efficiency is

TABLE 4. Channel loss models with shadowing.

		Path loss in decibel, d_{3D} in meter, f_c in GHz	**Parameters**
FSL	n/a	$PL_{\mathrm{FSL}} = 32.45 + 20\log_{10}(d_{\mathrm{3D}}) + 20\log_{10}(f_c)$ (11)	n/a
3GPP RMa [9]	LOS	$\begin{cases} 10\,\mathrm{m} \le d_{\mathrm{2D}} \le d_{\mathrm{BP}}, \quad \sigma_{\mathrm{LOS1}} = 4 \\ PL_{\mathrm{LOS1}} = 20\log_{10}(\frac{40\pi d_{\mathrm{3D}} f_c}{3}) + \min(0.03h^{1.72}, 10)\log_{10}(d_{\mathrm{3D}}) \\ \qquad - \min(0.044h^{1.72}, 14.77) + 0.002\log_{10}(h)d_{\mathrm{3D}} \\ d_{\mathrm{BP}} < d_{\mathrm{2D}} \le 10\,\mathrm{km}, \quad \sigma_{\mathrm{LOS2}} = 6 \\ PL_{\mathrm{LOS2}} = PL_{\mathrm{LOS1}}(d_{\mathrm{BP}}) + 40\log_{10}(\frac{d_{\mathrm{3D}}}{d_{\mathrm{BP}}}) \end{cases}$ (12)	$d_{\mathrm{BP}} = 2\pi h_{\mathrm{BS}} h_{\mathrm{UT}} f_c/C$, $C = 3 \times 10^8$ m/s, $10\,\mathrm{m} \le h_{\mathrm{BS}} \le 150\,\mathrm{m}$, $1\,\mathrm{m} \le h_{\mathrm{UT}} \le 10\,\mathrm{m}$, $5\,\mathrm{m} \le W \le 50\,\mathrm{m}$, $5\,\mathrm{m} \le h \le 50\,\mathrm{m}$, f_c is carrier frequency in Hz, d_{2D} is horizontal distance, d_{3D} is 3D distance C is speed of light, d_{BP} or d'_{BP} is breakpoint distance in meter, h_{BS} is height of base station, h_{UT} is height of robot, W is average street width, h is average building height, σ is standard deviation of Gaussian variables, which are used to model shadowing effect.
	NLOS	$PL_{\mathrm{NLOS}} = \max(PL_{\mathrm{LOS}}, PL'_{\mathrm{NLOS}}), \quad \sigma_{\mathrm{NLOS}} = 8$ $PL'_{\mathrm{NLOS}} = 161.04 - 7.1\log_{10}(W) + 7.5\log_{10}(h) - \big(24.37 - 3.7(h/h_{\mathrm{BS}})^2\big)\log_{10}(h_{\mathrm{BS}}) + \big(43.42 - 3.1\log_{10}(h_{\mathrm{BS}})\big)\big(\log_{10}(d_{\mathrm{3D}}) - 3\big) + 20\log_{10}(f_c) - \Big(3.2\big(\log_{10}(11.75h_{\mathrm{UT}})\big)^2 - 4.97\Big)$ (13)	
3GPP UMa [9]	LOS	$\begin{cases} 10\,\mathrm{m} \le d_{\mathrm{2D}} \le d'_{\mathrm{BP}}, \quad \sigma_{\mathrm{LOS1}} = 4 \\ PL_{\mathrm{LOS1}} = 28.0 + 22\log_{10}(d_{\mathrm{3D}}) + 20\log_{10}(f_c) \\ d'_{\mathrm{BP}} < d_{\mathrm{2D}} \le 5\,\mathrm{km}, \quad \sigma_{\mathrm{LOS2}} = 4 \\ PL_{\mathrm{LOS2}} = 28.0 + 40\log_{10}(d_{\mathrm{3D}}) + 20\log_{10}(f_c) - 9\log_{10}\big((d'_{\mathrm{BP}})^2 + (h_{\mathrm{BS}} - h_{\mathrm{UT}})^2\big) \end{cases}$ (14)	$d'_{\mathrm{BP}} = 2\pi h'_{\mathrm{BS}} h'_{\mathrm{UT}} f_c/C$, h'_{BS} and h'_{UT} are effective antenna height, $h'_{\mathrm{BS}} = h_{\mathrm{BS}} - h_{\mathrm{E}}$, $h'_{\mathrm{UT}} = h_{\mathrm{UT}} - h_{\mathrm{E}}$, h_{E} is effective environment height, $1.5\,\mathrm{m} \le h_{\mathrm{UT}} \le 22.5\,\mathrm{m}$, $h_{\mathrm{BS}} = 25\,\mathrm{m}$, *in d_{BP} or d'_{BP}, the f_c is in Hz, in other places, f_c is in GHz.
	NLOS	$PL_{\mathrm{NLOS}} = \max(PL_{\mathrm{LOS}}, PL'_{\mathrm{NLOS}}), \quad \sigma_{\mathrm{NLOS}} = 6$ $PL'_{\mathrm{NLOS}} = 13.54 + 39.08\log_{10}(d_{\mathrm{3D}}) + 20\log_{10}(f_c) - 0.6(h_{\mathrm{UT}} - 1.5)$ (15)	
3GPP UMi [9]	LOS	$\begin{cases} 10\,\mathrm{m} \le d_{\mathrm{2D}} \le d'_{\mathrm{BP}}, \quad \sigma_{\mathrm{LOS1}} = 4 \\ PL_{\mathrm{LOS1}} = 32.4 + 21\log_{10}(d_{\mathrm{3D}}) + 20\log_{10}(f_c) \\ d'_{\mathrm{BP}} < d_{\mathrm{2D}} \le 5\,\mathrm{km}, \quad \sigma_{\mathrm{LOS2}} = 4 \\ PL_{\mathrm{LOS2}} = 32.4 + 40\log_{10}(d_{\mathrm{3D}}) + 20\log_{10}(f_c) - 9.5\log_{10}\big((d'_{\mathrm{BP}})^2 + (h_{\mathrm{BS}} - h_{\mathrm{UT}})^2\big) \end{cases}$ (16)	$h_{\mathrm{E}} = 1\,\mathrm{m}$, $1.5\,\mathrm{m} \le h_{\mathrm{UT}} \le 22.5\,\mathrm{m}$, $h_{\mathrm{BS}} = 10\,\mathrm{m}$.
	NLOS	$PL_{\mathrm{NLOS}} = \max(PL_{\mathrm{LOS}}, PL'_{\mathrm{NLOS}}), \quad \sigma_{\mathrm{NLOS}} = 7.82$ $PL'_{\mathrm{NLOS}} = 22.4 + 35.3\log_{10}(d_{\mathrm{3D}}) + 21.3\log_{10}(f_c) - 0.3(h_{\mathrm{UT}} - 1.5)$ (17)	
3GPP InH [9]	LOS	$PL_{\mathrm{LOS}} = 32.4 + 17.3\log_{10}(d_{\mathrm{3D}}) + 20\log_{10}(f_c), \quad \sigma_{\mathrm{LOS}} = 3$ (18)	$1\,\mathrm{m} \le d_{\mathrm{3D}} \le 150\,\mathrm{m}$.
	NLOS	$PL_{\mathrm{NLOS}} = \max(PL_{\mathrm{LOS}}, PL'_{\mathrm{NLOS}}), \quad \sigma_{\mathrm{NLOS}} = 8.03$ $PL'_{\mathrm{NLOS}} = 17.3 + 38.3\log_{10}(d_{\mathrm{3D}}) + 24.9\log_{10}(f_c)$ (19)	
Industrial indoor [23]	900 MHz	$PL = 61.65 + 24.9\log_{10}(d_{\mathrm{3D}}/15), \quad \sigma = 7.35$ (20)	n/a
	2400 MHz	$PL = 71.84 + 21.6\log_{10}(d_{\mathrm{3D}}/15), \quad \sigma = 8.13$ (21)	

given by,

$$C = \eta D_{\mathrm{d}} \log_2(1 + \mathrm{SNR}) \tag{7}$$

where SNR denotes signal-to-noise-ratio in linear scale, D_{d} denotes duty cycle, η denotes channel efficiency, in this section η was taken equal to 0.7. The duty cycle D_{d} is regulated in [37] in Europe, 1% duty cycle is maximum that can be used in 868 MHz ISM band. Here, we remark that the NB-IoT uses legacy band, no duty cycle restriction has been put on to it. However, in order to compare spectral efficiency metrics of all selected IoT technologies in Section IV, we use 1% duty cycle for NB-IoT as well.

Fig. 5 compares achievable spectral efficiency under different channel path-loss models and under five different IoT technologies. The high spectral efficiency is more relevant at short ranges (i.e., indoor applications), than at large ranges, thus our example here focuses on a 200 × 200 m^2 square indoor industrial site. Here we consider 5% outliers, which the ends of the whiskers are represented by the 2.5th percentile and the 97.5th percentile respectively.

The height of robot remains 2 m, the height of AN remains 10 m as in section V. We note that in this scenario, 3GPP UMi, InHm, InHo and industrial indoor channel loss models are more relevant to the indoor applications than the others, thus the results discussion will focus more on these four models. In NB-IoT technology, InHo model predicts the highest median value 0.178 bit/s/Hz; InHm model with almost 0.154 bit/s/Hz median value gives the lower bound of NB-IoT spectral efficiency. In LoRa, Sigfox, Zigbee and MIOTY technologies, a similar situation occurs to them as well, in the sense that InHo model predicts the highest median value of spectral efficiency while InHm model gives the lowest median value. Among these five technologies, the Sigfox is most spectral efficient technology in the indoor scenarios, the Zigbee is the worst technology from the spectral efficiency aspect. However, the Zigbee at 2.4 GHz frequency band has 2 MHz bandwidth resource and it could provide the highest throughput among these five technologies in indoor scenarios.

VII. OUTAGE PROBABILITY

IIoT technologies could also serve many kinds of outdoor applications, as discussed in Section I. In a large outdoor area, the outage probability metric (i.e., one dimension of reliability) usually has priority over spectral efficiency. Therefore, in this section, we define a 2000 × 2000 m^2 simulation area to compare different IIoT services. The height of robot and base station are still 2 m and 10 m, respectively. From Table 1, we remark that Zigbee is a short range IoT technology, thus the main discuss of this section focuses on NB-IoT, LoRa, Sigfox and MIOTY only. Besides, we will pay more attentions to the outdoor channel loss models, for example, the 3GPP RMa, UMa and UMi models.

In this section, we calculate the average outage probability over the entire simulation space. Let the set $\mathcal{S}$ denote all positions of a robot in simulation space, a position of a robot is $\mathbf{s}_i \in \mathcal{S}$, in Cartesian coordinate system $\mathbf{s}_i$ is defined as,

$$\mathbf{s}_i = \{x_i, y_i, z_i : x_i, y_i \in (-10^3, 10^3), z_i \in (0, 2)\} \tag{8}$$

TABLE 5. K-factor for small-scale fading.

Model	K-factor [dB]
3GPP RMa [9]	$K \sim \mathcal{N}(7, 4^2)$
3GPP UMa [9]	$K \sim \mathcal{N}(9, 3.5^2)$
3GPP UMi [9]	$K \sim \mathcal{N}(9, 5^2)$
3GPP InH [9]	$K \sim \mathcal{N}(7, 4^2)$
Industrial Indoor [23]	$900\,\text{MHz}\ K = 11.5$ $2400\,\text{MHz}\ K = 11.6$

where $i = 1, 2, 3, \cdots$, the average outage probability $\overline{P}_{\text{out}}$ is defined as,

$$\overline{P}_{\text{out}} = \frac{\sum\limits_{\mathbf{s}_i \in \mathcal{S}} P_{\text{out}}^{(\mathbf{s}_i)}}{|\mathcal{S}|} \tag{9}$$

where $P_{\text{out}}^{(\mathbf{s}_i)}$ denotes eq. (6) at $\mathbf{s}_i$.

Under the considerations of shadowing and small-scale fading effects, the analytic solutions of $P_{\text{out}}^{(\mathbf{s}_i)}$ are hard to find. The shadowing effects are usually modeled as random variables (in dB) following Gaussian distribution, while the small-scale fading effects are modeled as random variables (in linear scale) following Rician distribution. In this paper, we estimate $P_{\text{out}}^{(\mathbf{s}_i)}$ by treating its solution as the tail probability estimation in *sum of non-identically distributed random variables situation* [35]. The algorithm 10.6 in [35] is applied, the $P_{\text{out}}^{(\mathbf{s}_i)}$ is estimated by,

$$P_{\text{out}}^{(\mathbf{s}_i)} = \Pr(\mathcal{X}^{(\mathbf{s}_i)} \geq \text{MCL} - PL^{(\mathbf{s}_i)}) \tag{10}$$

where $PL^{(\mathbf{s}_i)}$ is the deterministic part of the path loss, $\mathcal{X}^{(\mathbf{s}_i)}$ denotes the sum of shadowing and small-scale fading effects at $\mathbf{s}_i$, $\text{MCL} - PL^{(\mathbf{s}_i)}$ is the threshold in the algorithm 10.6 in [35].

As seen in Fig. 6, NB-IoT outperforms LoRa, Sigfox and MIOTY IoT technologies in terms of outages. The worst case for NB-IoT is predicted by the 3GPP RMa model with 3.76×10^{-2} outage probability. Generally speaking, NB-IoT, LoRa, Sigfox and MIOTY has their most outages events in the RMa scenarios from the results. Among 3GPP RMa, UMa and UMi models, the predictions of UMa model are always the best cases, for example, 1.42×10^{-6} outage probability in NB-IoT, 2.67×10^{-3} outage probability in LoRa, 9.40×10^{-6} outage probability in Sigfox, 6.46×10^{-4} outage probability in MIOTY.

VIII. CONCLUSIONS AND OPEN RESEARCH DIRECTIONS

In this work, we addressed the problem of wireless channel modeling in the context of IIoT technologies. We described

TABLE 6. Line-of-sight probability for 3GPP models.

Model	Line-of-sight probability	
3GPP RMa [9]	$\mathrm{Pr} = \begin{cases} 1 & , \quad d_{\mathrm{2D}} \leq 10\,\mathrm{m} \\ e^{-\frac{d_{\mathrm{2D}}-10}{1000}} & , \quad 10\,\mathrm{m} < d_{\mathrm{2D}} \end{cases}$	(22)
3GPP UMa [9]	$\mathrm{Pr} = \begin{cases} 1 & , \quad d_{\mathrm{2D}} \leq 18\,\mathrm{m} \\ \Big(\frac{18}{d_{\mathrm{2D}}} + \big(1 - \frac{18}{d_{\mathrm{2D}}}\big)e^{-\frac{d_{\mathrm{2D}}}{63}}\Big)\Big(1 + \frac{5}{4}C'(h_{\mathrm{UT}})(\frac{d_{\mathrm{2D}}}{100})^3 e^{-\frac{d_{\mathrm{2D}}}{150}}\Big) & , \quad 18\,\mathrm{m} < d_{\mathrm{2D}} \end{cases}$ where $C'(h_{\mathrm{UT}}) = \begin{cases} 0 & , \quad h_{\mathrm{UT}} \leq 13\,\mathrm{m} \\ (\frac{h_{\mathrm{UT}} - 13}{10})^{1.5} & , \quad 13\,\mathrm{m} < h_{\mathrm{UT}} \leq 23\,\mathrm{m} \end{cases}$	(23)
3GPP UMi [9]	$\mathrm{Pr} = \begin{cases} 1 & , \quad d_{\mathrm{2D}} \leq 18\,\mathrm{m} \\ \frac{18}{d_{\mathrm{2D}}} + \big(1 - \frac{18}{d_{\mathrm{2D}}}\big)e^{-\frac{d_{\mathrm{2D}}}{36}} & , \quad 18\,\mathrm{m} < d_{\mathrm{2D}} \end{cases}$	(24)
3GPP InH [9]	Mixed office: $\mathrm{Pr} = \begin{cases} 1 & , \quad d_{\mathrm{2D}} \leq 1.2\,\mathrm{m} \\ e^{-\frac{d_{\mathrm{2D}}-1.2}{4.7}} & , \quad 1.2\,\mathrm{m} \leq d_{\mathrm{2D}} < 6.5\,\mathrm{m} \\ 0.32e^{-\frac{d_{\mathrm{2D}}-6.5}{32.6}} & , \quad 6.5\,\mathrm{m} \leq d_{\mathrm{2D}} \end{cases}$	(25)
	Open office: $\mathrm{Pr} = \begin{cases} 1 & , \quad d_{\mathrm{2D}} \leq 5\,\mathrm{m} \\ e^{-\frac{d_{\mathrm{2D}}-5}{70.8}} & , \quad 5\,\mathrm{m} \leq d_{\mathrm{2D}} < 49\,\mathrm{m} \\ 0.54e^{-\frac{d_{\mathrm{2D}}-49}{211.7}} & , \quad 49\,\mathrm{m} \leq d_{\mathrm{2D}} \end{cases}$	(26)

in details seven channel models, namely the free space loss, the 3GPP channel models with its five variants (indoor open and mixed hotspots, outdoor urban micro- and micro-cell, and outdoor rural), and the industrial indoor channel loss model for ISM bands. We also described the generic single-slope model, which is a generalization of FSL. We compared the predicted performance based on the above-mentioned seven channel models in terms of three important wireless communications metrics, namely the cell radius, the spectral efficiency, and the outage probability in both indoor and outdoor scenarios. We selected four potential IIoT technologies, namely NB-IoT, Sigfox, LoRA, ZigBee and MIOTY, to evaluate their performance in terms of cell radius at 1% outage probability, their spectral efficiency within 200×200 m^2 area, and their outage probabilities within 2000×2000 m^2 area.

Among these five potential IIoT technologies, NB-IoT has the longest cell radius and the best outage probability in outdoor scenarios, while Sigfox has the best spectral efficiency in indoor scenarios and Zigbee has the largest operating bandwidth. We have also shown that the median-case predictors among these studied channel models are not far from the values reported or measured in practice for the selected IIoT technologies. We would like to emphasize that 3GPP channel loss models are so far the best suitable models to estimate the studied communication metrics, as they often offer an estimate close to the median-predicted behavior by many other channel models. Considering the average of a certain metric over a space (i.e., the average spectral efficiency or outage probability over the simulation space), the worst-case scenario can be studied based on 3GPP RMa channel models, while the best-case scenario is given by the free-space loss channel model (i.e., overly optimistic bound).

In terms of future research work in IIoT environments, in our opinion, three key axes are: i) the wireless connection reliability, ii) the wireless geo-localization, and iii) the predictive maintenance. In our paper, the wireless connection reliability is thoroughly studied based on the channel loss models. The geo-localization and the predictive maintenance aspects will be investigated in the future work.

Regarding the reliability factor, extremely reliable wireless communication will be more and more needed in order to avoid heavy cabling in zones with difficult access.

For example, if we have a high furnace chimney where a quality air measurement device is to be installed, a wireless IoT sensor mounted on the top of the chimney may be 100 times less expensive than deploying an Ethernet cable from the top to the bottom of the tower. But a one hour stop of the IoT communication link may be 100 million times more expensive than the installation cost: NOx, SOx, or CO emission overrun during one hour may produce the closure of the plant.

Regarding the geo-localization needs, it is well-known that high expenses are engaged every time when a new person has to be trained for process operating in a plant. These expenses are increased by the turnover due to tedious working conditions. The wireless geo-localization of the devices from a specific installation may save lot of time and money and the autonomy of the new hired person would be dramatically improved.

Last, but not least, the predictive maintenance for large surface scattered installations may be easily deployed using precise reliable IIoT communication. The uploaded analytics from the field may predict dangerous increase or overrun of key indicators using low rate communicating systems at very low cost, much simpler to install than cabling.

APPENDIX A
CHANNEL LOSS MODELS AND LINE-OF-SIGHT PROBABILITY

See Table 4–6.

REFERENCES

[1] P. F. E. Silva, V. Kaseva, and E. S. Lohan, "Wireless positioning in IoT: A look at current and future trends," *Sensors*, vol. 18, no. 8, p. 2470, 2018.

[2] A. Gupta and E. R. K. Jha, "A survey of 5G network: Architecture and emerging technologies," *IEEE Access*, vol. 3, pp. 1206–1232, Jul. 2015.

[3] *Study on Enhanced LTE Support for Aerial Vehicles (Release 15)*, document 3GPP TR 36.777 v15.0.0, 3GPP-Technical Specification Group Radio Access Network, 2017. Accessed: Mar. 2018. [Online]. Available: http://www.3gpp.org/DynaReport/36-series.htm

[4] D. Miller, "Blockchain and the Internet of Things in the industrial sector," *IT Prof.*, vol. 20, no. 3, pp. 15–18, 2018.

[5] Y.-W. Kuo, C.-L. Li, J.-H. Jhang, and S. Lin, "Design of a wireless sensor network-based IoT platform for wide area and heterogeneous applications," *IEEE Sensors J.*, vol. 18, no. 12, pp. 5187–5197, Jun. 2018.

[6] S. Mayer, J. Hodges, D. Yu, M. Kritzler, and F. Michahelles, "An open semantic framework for the industrial Internet of Things," *IEEE Intell. Syst.*, vol. 32, no. 1, pp. 96–101, Jan./Feb. 2017.

[7] J. Wan, S. Tang, Q. Hua, D. Li, C. Liu, and J. Lloret, "Context-aware cloud robotics for material handling in cognitive industrial Internet of Things," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2272–2281, Aug. 2018.

[8] G. Han, L. Wan, L. Shu, and N. Feng, "Two novel DOA estimation approaches for real-time assistant calibration systems in future vehicle industrial," *IEEE Syst. J.*, vol. 11, no. 3, pp. 1361–1372, Sep. 2017.

[9] *Study on Channel Model for Frequencies From 0.5 to 100 GHz*, document 3GPP TR 38.901 V14.3.0 (2017-12), 3GPP-Technical Specification Group Radio Access Network, 2017.

[10] Y. Kondratenko, G. Kondratenko, and I. Sidenko, "Multi-criteria decision making for selecting a rational IoT platform," in *Proc. IEEE 9th Int. Conf. Dependable Syst., Services Technol. (DESSERT)*, May 2018, pp. 147–152.

[11] E. M. Silva, C. Agostinho, and R. Jardim-Goncalves, "A multi-criteria decision model for the selection of a more suitable Internet-of-Things device," in *Proc. Int. Conf. Eng., Technol. Innov. (ICE/ITMC)*, Jun. 2017, pp. 1268–1276.

[12] J. Haxhibeqiri, A. Karaagac, F. Van den Abeele, W. Joseph, I. Moerman, and J. Hoebeke, "LoRa indoor coverage and performance in an industrial environment: Case study," in *Proc. 22nd IEEE Int. Conf. Emerg. Technol. Factory Autom. (ETFA)*, Sep. 2017, pp. 1–8.

[13] T. Addabbo, A. Fort, M. Mugnaini, L. Parri, S. Parrino, A. Pozzebon, and V. Vignoli, "An IoT framework for the pervasive monitoring of chemical emissions in industrial plants," in *Proc. Workshop Metrol. Ind. 4.0 IoT*, Apr. 2018, pp. 269–273.

[14] *Short Range Devices; Low Throughput Networks (LTN); Protocols for Radio Interface A*, document ETSI TS 103 357 V1.1.1 (2018-06), 2018. Accessed: Mar. 2019.

[15] J. Petajajarvi, K. Mikhaylov, A. Roivainen, T. Hanninen, and M. Pettissalo, "On the coverage of LPWANs: Range evaluation and channel attenuation model for LoRa technology," in *Proc. 14th Int. Conf. ITS Telecommun. (ITST)*, Dec. 2015, pp. 55–59.

[16] M. Luvisotto, F. Tramarin, L. Vangelista, and S. Vitturi, "On the use of LoRaWAN for indoor industrial IoT applications," *Wireless Commun. Mobile Comput.*, vol. 2018, May 2018, Art. no. 3982646.

[17] M. Damsaz, D. Guo, J. Peil, W. Stark, N. Moayeri, and R. Candell, "Channel modeling and performance of Zigbee radios in an industrial environment," in *Proc. IEEE 13th Int. Workshop Factory Commun. Syst. (WFCS)*, May/Jun. 2017, pp. 1–10.

[18] R. M. Sandoval, A.-J. Garcia-Sanchez, and J. Garcia-Haro, "Improving RSSI-based path-loss models accuracy for critical infrastructures: A smart grid substation case-study," *IEEE Trans. Ind. Informat.*, vol. 14, no. 5, pp. 2230–2240, May 2018.

[19] W. Wang and E. S. Lohan, "Applicability of 3GPP indoor hotspot models to the industrial environments," in *Proc. 8th Int. Conf. Localization GNSS (ICL-GNSS)*, Jun. 2018, pp. 1–5.

[20] A. Alsayyari, I. Kostanic, C. Otero, M. Almeer, and K. Rukieh, "An empirical path loss model for wireless sensor network deployment in a sand terrain environment," in *Proc. IEEE World Forum Internet Things (WF-IoT)*, Mar. 2014, pp. 218–223.

[21] M. Soleimani, M. M. Bhuiyan, M. H. MacGregor, R. Kerslake, and P. Mousavi, "RF channel modelling and multi-hop routing for wireless sensor networks located on oil rigs," *IET Wireless Sensor Syst.*, vol. 6, no. 5, pp. 173–179, Oct. 2016.

[22] S. Shrestha, J. Talvitie, and E. S. Lohan, "Deconvolution-based indoor localization with WLAN signals and unknown access point locations," in *Proc. Int. Conf. Localization GNSS (ICL-GNSS)*, Jun. 2013, pp. 1–6.

[23] E. Tanghe, W. Joseph, L. Verloock, L. Martens, H. Capoen, K. Van Herwegen, and W. Vantomme, "The industrial indoor channel: Large-scale and temporal fading at 900, 2400, and 5200 MHz," *IEEE Trans. Wireless Commun.*, vol. 7, no. 7, pp. 2740–2751, Jul. 2008.

[24] M. Lauridsen, H. Nguyen, B. Vejlgaard, I. Z. Kovács, P. Mogensen, and M. Sorensen, "Coverage comparison of GPRS, NB-IoT, LoRa, and SigFox in a 7800 km^2 area," in *Proc. IEEE 85th Veh. Technol. Conf. (VTC Spring)*, Jun. 2017, pp. 1–5.

[25] B. Vejlgaard, M. Lauridsen, H. Nguyen, I. Z. Kovács, P. Mogensen, and M. Sorensen, "Interference impact on coverage and capacity for low power wide area IoT networks," in *Proc. Wireless Commun. Netw. Conf. (WCNC)*, Mar. 2017, pp. 1–6.

[26] *Semtech SX1276-7-8-9 Datasheet*. Accessed: Oct. 2018. [Online]. Available: https://www.semtech.com/uploads/documents/DS_SX1276-7-8-9_W_APP_V5.pdf

[27] (2018). *MIOTY^{TM} by BehrTech Starter Kit 1.0 with Microsoft Azure*. Accessed: Apr. 2019. [Online]. Available: https://cdn2.hubspot.net/hubfs/4739964/Data%20Sheets/BTI%20_%20Data%20Sheet%20Mioty%20Starter%20Kit%20v1.5%20(Print-Ready)%20April%2023.pdf?utm_campaign=Use%20Case%20-%20Downloads&utm_source=Website&utm_medium=Data%20Sheet

[28] J. Chen, K. Hu, Q. Wang, Y. Sun, Z. Shi, and S. He, "Narrowband Internet of Things: Implementations and applications," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 2309–2314, Dec. 2017.

[29] A. Augustin, J. Yi, T. Clausen, and W. M. Townsley, "A study of LoRa: Long range & low power networks for the Internet of Things," *Sensors*, vol. 16, no. 9, p. 1466, 2016.

[30] M. Centenaro, L. Vangelista, A. Zanella, and M. Zorzi, "Long-range communications in unlicensed bands: The rising stars in the IoT and smart city scenarios," *IEEE Wireless Commun.*, vol. 23, no. 5, pp. 60–67, Oct. 2016.

[31] R. Quinnell, ‘‘Low power wide-area networking alternatives for the IoT,’’ *EDN Netw.*, 2015. [Online]. Available: https://www.edn.com/design/systems-design/4440343/Low-power-wide-area-networking-alternatives-for-the-IoT

[32] D. M. Hernandez, G. Peralta, L. Manero, R. Gomez, J. Bilbao, and C. Zubia, ‘‘Energy and coverage study of LPWAN schemes for industry 4.0,’’ in *Proc. IEEE Int. Workshop Electron., Control, Meas., Signals Appl. Mechatronics (ECMSM)*, May 2017, pp. 1–6.

[33] Y. Li, X. Cheng, Y. Cao, D. Wang, and L. Yang, ‘‘Smart choice for the smart grid: Narrowband Internet of Things (NB-IoT),’’ *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1505–1515, Jun. 2018.

[34] R. E. Rider, ‘‘From cardinals to chaos: Reflections on the life and legacy of stanislaw Ulam,’’ *Science*, vol. 246, no. 4926, pp. 134, 1989.

[35] D. P. Kroese, T. Taimre, and Z. I. Botev, *Handbook of Monte Carlo Methods*, vol. 706. Hoboken, NJ, USA: Wiley, 2013.

[36] O. Liberg, M. Sundberg, E. Wang, J. Bergman, and J. Sachs, *Cellular Internet of Things: Technologies, Standards, and Performance*. New York, NY, USA: Academic, 2017.

[37] *Spectrum Requirements for Short Range Device, Metropolitan Mesh Machine Networks (M3N) and Smart Metering (SM) Applications*, document ETSI TR 103 055 V1.1.1 (2011-09), 2011. Accessed: Mar. 2019.

WENBO WANG received the M.Sc. degree in electrical engineering from the Tampere University of Technology, Tampere, Finland, in 2016. He is currently pursuing the Ph.D. degree in wireless communication with Tampere University, Tampere. From 2016 to 2017, he was a Marie Curie Early Stage Researcher with the University of Twente, Enschede, The Netherlands. The research work focused on the efficient estimation of parameters in high-dimensional state space. His current research interests include the non-terrestrial networks, mmWave channel models, the industrial Internet-of-Things, and non-linear filtering algorithms. He has served as a Reviewer for the International Conference on Information Fusion, in 2018 and 2019, and as both a TPC member and a reviewer for the IEEE/CIC International Conference on Communications in China, in 2019.

STEFAN L. CAPITANEANU born in Bucharest, Romania, in 1976. He has received the Ph.D. degree in electrical engineering from the Institut National Polytechnique de Toulouse (INPT), France, in 2002. Since then, he has been with Schneider Electric. He is currently the Advanced Control Team Leader for the Industry Automation Department based near Paris, France. From milk drying to Eiffel hydraulic lift optimization, his work is used directly by big actors on European or world market as Sanofi, Lactalis, Agrial, Eiffel Tower Society, Areva, and Schlumberger. His main research interests include advanced process control, energy efficiency in industry by using process optimization, intelligent automation, and motor drives.

DANA MARINCA is currently an Associate Professor with the ALMOST Team (Algorithms and Stochastic Models), DAVID Laboratory (Data and Algorithms for Smart and Sustainable City), University of Versailles Saint-Quentin (UVSQ), University Paris Saclay. She has participated in four research projects funded by national and international institutions (EU FP7). Her research interests include recommendation systems, learning and prediction mechanism, and content delivery networks. She has coauthored more than 20 international peer-reviewed publications, has served as a TPC Member for several international conferences in networking, and has co-supervised so far five M.Sc. theses and two Ph.D. theses.

ELENA-SIMONA LOHAN received the M.Sc. degree in electrical engineering from the Polytechnics University of Bucharest, in 1997, the D.E.A. degree in econometrics from École Polytechnique, Paris, in 1998, and the Ph.D. degree in telecommunications from the Tampere University of Technology, in 2003. She is currently an Associate Professor with the Electrical Engineering Unit, Tampere University (formerly Tampere University of Technology) and a Visiting Professor with the Universitat Autonoma de Barcelona (UAB), Spain. She is leading a Research Group on Signal Processing for Wireless Positioning. She has co-edited the first book on galileo satellite system *Galileo Positioning Technology* (Springer), has co-edited a Springer book on multi-technology positioning, and has authored or coauthored more than 185 international peer-reviewed publications, six patents, and inventions. She has supervised more than 40 B.Sc./M.Sc. students and more than 13 Ph.D. students, ten of which completed their Ph.D. In the past four years, she has been a Principal Investigator in five national projects and four EU projects. She is also an Associate Editor for the *RIN Journal of Navigation* and for the *IET Journal on Radar, Sonar, and Navigation.*

PUBLICATION

3

Applicability of 3GPP Indoor Hotspot Models to the Industrial Environments

W. Wang and E. S. Lohan

*2018 8th International Conference on Localization and GNSS (ICL-GNSS)*2018, 1–5

DOI: 10.1109/ICL-GNSS.2018.8440893

Applicability of 3GPP Indoor Hotspot Models to the Industrial Environments

Wenbo Wang and Elena Simona Lohan
Tampere University of Technology, Finland
{wenbo.wang, elena-simona.lohan}@tut.fi

***Abstract*—In this paper we study the applicability of the 3GPP Indoor Hotspot model (InH from TR38.901 document) to the indoor industrial environments with moving robots. We will show the impact of carrier frequencies on the expected path losses as we move from cmWave to the mmWave bands, we will present the upper bounds on the capacity expected at different available carrier frequencies and different 3D distances, and we will also discuss the results in the context of receiver sensitivities of various Internet-of-Things solutions for industrial environments, such as Sigfox, LoRa, BLE or Wi-SUN.**

***Index Terms*—3GPP Indoor hotspot channels (InH), open office, mixed office, cmWave, mmWave, industrial environments**

I. Introduction

Industrial environments refer to those scenarios where an industrial activity takes place, such as manufacturing factories, oil and mining fields, chemical plants, etc. The two major targets in an industrial environment are to improve work safety and to increase the production efficiency. Factory automation is one of the top applications envisioned by the researchers in 5G communications areas [1].

In a factory automation environment, the hotspot areas refers to areas with a high density of industrial nodes, such as robots, sensors, human controllers, etc., which need both uplink and downlink connections to the access network. The reliability of such connections should be very high; the researchers usually talk about ”ultra-reliable connections” in such scenarios [1], [2] and they measure the reliability for example, in terms of diversity (spatial, time or frequency diversity) or outage probabilities [1], [3].

Traditionally, the wireless connections in industrial environments have been covered by industrial-specific standards such as ISA 101.11a or WirelessHART. In recent years however, more and more focused has shifted towards cellular wireless communications such as 4G (LTE) and 5G (next generation of wireless communications). The research efforts related to 4G and 5G communications are led by 3GPP standardization body, which has already published various channel models to support a wide range of carrier frequency bands, basically anything between 0 GHz and 100 GHz [4].

One of these channel models is the he 3GPP indoor hotspot (InH) path-loss channel model, defined in [4], [5] as an indoor scenario with small cells, a Base Station (BS) or Access Node (AN) mounted below the ceilings and the users (or robots) moving inside the building. The key characteristics of InH, as defined in [4] are high user throughput and indoor coverage. The path-loss and shadowing models characterizing InH environments can be found in [5] and they form the basis of our research work in this paper. The goal is to analyse the receiver performance at different carrier frequencies, ranging from sub-GHz cmWaves to mmWaves, and different bandwidths. Performance metrics such as capacity and outage probabilities are investigated and they are discussed in terms of industrial environment constraints. The received signal strength predicted by the maximum link budgets, according to the 3GPP InH model, will also be compared with several commercial receiver sensitivities of various Internet-of-Things solutions for industrial environments, such as Sigfox, LoRa, BLE or Wi-SUN.

Related work can be found in [6], [7]. For example, modified 3GPP channel models can be found in [6] (LTE indoor topology, dynamic case), but used in a different context (smart home environment) and looking only at fixed carrier frequency (3.5 GHz). Moreover, no comparison with the original 3GPP channel models was provided in [6]. In [7], the authors compare the 3GPP Urban Microcell (UMi) and Urban Macrocell (UMa) with the NYUSIM channel models for 5G wireless communications and draw the conclusion that NYUSIM channel model is more optimistic than the 3GPP ones, as it provides better spectral efficiencies. Our work is complementary to the work in [7], as we focus on a different 3GPP channel, namely the InH channel.

To the best of the Authors' knowledge, there is currently of lack of research papers investigating the InH indoor channel model of 3GPP under concrete case studies, such as industrial environments. Our study here aims to address this gap.

II. 3GPP Indoor Hotspot model (InH)

The 3GPP InH model, as found in [5], defines the path losses via a deterministic part (distance dependent) and a random part (due to shadowing) and under two situations: i) Line of Sight (LOS) and ii) Non Line of Sight (NLOS), by giving also the LOS probability. The path loss, including shadowing, under LOS case PL_{LOS} is given by

$$\begin{aligned} PL_{LOS} &= 32.4 + 17.3\log_{10}(d_{3D}) + 20\log_{10}(f_c) \\ &+ \xi_{LOS} \end{aligned} \tag{1}$$

where d_{3D} is the 3D distance between the access node and the robot (given in meter), f_c is the carrier frequency (given in GHz) and ξ_{LOS} is the shadowing under LOS conditions, modelled as a Gaussian variable of zero mean and standard deviation $\sigma_{SF_{LOS}}$, and $\sigma_{SF_{LOS}} = 3, 1m \leq d_{3D} \leq 150m$.

Similarly, the path loss, including shadowing, under NLOS case PL_{NLOS} is given by

$$\begin{aligned} PL_{NLOS} &= \max(PL_{LOS}, 38.3\log_{10}(d_{3D}) \\ &+ 17.30 + 24.9\log_{10}(f_c)) + \xi_{NLOS} \end{aligned} \tag{2}$$

where ξ_{NLOS} is the shadowing under NLOS conditions, modelled as a Gaussian variable of zero mean and standard deviation $\sigma_{SF_{NLOS}}$ and $\sigma_{SF_{NLOS}} = 8.03, 1m \leq d_{3D} \leq 150m$.

The LOS probability is defined under two cases:

1) Mixed indoor

$$Pr_{LOS} = \begin{cases} 1, & d_{2D} \leq 1.2m \\ e^{(-\frac{d_{2D}-1.2}{4.7})}, & 1.2m \ < d_{2D} \leq 6.5m \\ 0.32e^{-\frac{d_{2D}-6.5}{32.6}}, & 6.5m < d_{2D} \end{cases} \tag{3}$$

2) Open indoor

$$Pr_{LOS} = \begin{cases} 1, & d_{2D} \leq 5m \\ e^{(-\frac{d_{2D}-5}{70.8})}, & 5m \ < d_{2D} \leq 49m \\ 0.54e^{-\frac{d_{2D}-49}{211.7}}, & 49m < d_{2D} \end{cases} \tag{4}$$

Thus, in one d_{2D} interval the path losses plus shadowing PL_{InH} under the 3GPP InH model are given by

$$\begin{aligned} PL_{InH} =& Pr_{LOS}(PL_{LOS} + \xi_{LOS}) \\ &+ (1 - Pr_{LOS})(PL_{NLOS} + \xi_{NLOS}) \end{aligned} \tag{5}$$

III. 3GPP MODEL ANALYSIS

If we only consider the shadowing effect on the calculation of InH path loss, in the context of 3GPP TR38.901 document, we could derive the below form for the expected overall path loss,

$$\begin{aligned} PL = \sum_{n=1}^{N} & P(Pr_{LOS}^{(n)}|\cdot)\Big[Pr_{LOS}^{(n)}(PL_{LOS} + \xi_{LOS}) \\ &+ (1 - Pr_{LOS}^{(n)})(PL_{NLOS} + \xi_{NLOS})\Big] \end{aligned} \tag{6}$$

where $P(Pr_{LOS}^{(n)}|\cdot)$ is the $n-th$ posterior given by the $n-th$ d_{2D} segment in either the mixed office or the open office scenario, $Pr_{LOS}^{(n)}$ is Pr_{LOS} in the $n-th$ d_{2D} segment, N is the total number of d_{2D} segments in one scenario.

It is obvious that the overall path loss in eq. (6) follows a Gaussian distribution$PL \sim \mathcal{N}(\mu_{PL}, \sigma_{PL}^2)$. The shadowing ξ_{LOS} and ξ_{NLOS} are modelled as Gaussian variables, the linear summation of Gaussian variables follows a Gaussian distribution. The mean value (μ_{PL}) and variance value (σ_{PL}^2) are given as below,

$$\begin{cases} \mu_{PL} = \sum_{n=1}^{N} P(Pr_{LOS}^{(n)}|\cdot)\Big[Pr_{LOS}^{(n)}PL_{LOS} \\ \qquad + (1 - Pr_{LOS}^{(n)})PL_{NLOS}\Big] \\ \sigma_{PL}^2 = \sum_{n=1}^{N}\Big[P(Pr_{LOS}^{(n)}|\cdot)Pr_{LOS}^{(n)}\sigma_{SF_{LOS}}\Big]^2 \\ \qquad + \Big[P(Pr_{LOS}^{(n)}|\cdot)(1 - Pr_{LOS}^{(n)})\sigma_{SF_{NLOS}}\Big]^2 \end{cases} \tag{7}$$

A. Calculation of the posterior

The posterior in eq. (7) is determined by the segments, the lower and upper bound of d_{2D} and the distribution of robots. In 3GPP TR38.901, the corresponding parameters are given, we select relevant ones and present in Table I.

TABLE I
PARAMETERS OF INDOOR SCENARIOS

Parameters	Indoor open office (mixed office)
Layout	$120m \times 50m \times 3m$
Hotspot antenna height	3m (ceiling)
Robot location height	1m
Min. hotspot-robot distance (d_{2D})	0m
Max. d_{3D} distance	150m
Robot distribution (horizontal)	uniform

We calculate the $\max(d_{2D}) \approx 149.9967(m)$, since in the Table I it mentions that the robot follows the uniform distribution horizontally, thus $d_{2D} \sim \mathcal{U}(0, 149.9967)$, now we could derive the posterior as the below,

$$P(Pr_{LOS}^{(n)}|\cdot) = \int_{d_1}^{d_2} \frac{1}{149.9967} d_{d_{2D}} \tag{8}$$

where d_1 and d_2 are the lower and upper bound of d_{2D} in one segment respectively.

The value of posterior $P(Pr_{LOS}^{(n)}|\cdot)$ is given in the Table .

TABLE II
POSTERIOR $P(Pr_{LOS}^{(n)}|\cdot)$

Posterior	Value
Indoor Mixed office	
$P(d_{2D} \leq 1.2m)$	0.008
$P(1.2m \ < d_{2D} \leq 6.5m)$	0.035
$P(6.5m < d_{2D})$	0.957
Indoor open office	
$P(d_{2D} \leq 5m)$	0.033
$P(5m \ < d_{2D} \leq 49m)$	0.293
$P(49m < d_{2D})$	0.674

IV. Industrial environment constraints

The performance criteria regarding the (indoor) industrial environments are typically related to the reliability of the communications links, end-to-end latency, and workers safety. In our simulations, we will focus on several communication-related performance criteria, namely capacity and outage probabilities. These summarize in Table III. An N/A values means that the target criterion was not given in the considered reference.

TABLE III
Industrial (indoor) environment targets and constraints

Reference	Outage probability constraint	SNR targets [dB]	Capacity targets
[3]	$< 10^{-2}$	20	N/A
[8]	$< 10^{-2}$	-20 (LoRa) 7 (Sigfox)	N/A
[9]	N/A	$4.5 - 15$	5 bits/s/Hz
[10]	N/A	20 [1]	18.9 bits/s/Hz
[11]	$= 10^{-9}$	$15 - 20$	N/A

V. Link budget, receiver sensitivity, outage probabilities, and capacity

The received signal power P_R is given by

$$P_R = P_T + G_T - L_T - PL_{InH} + G_R - L_R, \tag{9}$$

where P_T is the transmit power, G_T and G_R are the antenna gains at the transmitter and receiver sides, respectively, L_T and L_R are the cable losses at the transmitter and receiver sides, respectively, and the path loss PL_{InH} is given by the eq. (5).

Assuming a receiver sensitivity $P_{R_{min}}$, the outage probability p_{out} is defined here as the probability that the received signal strength from eq. (9) is smaller or equal to $P_{R_{min}}$, i.e.

$$p_{out} = proba(PL_{InH} \geq P_T + G_T - L_T + G_R - L_R - P_{R_{min}}) \tag{10}$$

The PL_{InH} term is a randomly distributed variable, which depends on the shadowing under LOS and NLOS conditions. In addition, the SNR (in dB scale) is related to the received signal power P_R via

$$SNR = P_R + 174 - 10log_{10}(B_W) - N_F \tag{11}$$

where B_W is the receiver bandwidth in Hz, N_F is the receiver noise figure (in dB), and P_R is given in eq. (9). We remark that some authors define the outage probability as the probability that SNR falls below a certain threshold.

The data capacity or throughput C assuming an efficiency $\eta < 1$ (typically between 0.4 and 0.7 [10]) with respect to the Shannon capacity is given by

$$C = \eta B_W log_2 (1 + SNR) \tag{12}$$

with SNR given in eq. (11). Several examples of typical receiver sensitivities $P_{R_{min}}$ for different chipsets and various IoT technologies are shown in Table IV.

TABLE IV
Receiver sensitivities in commercial IoT chipsets

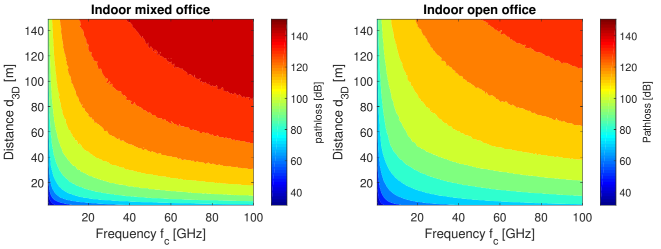
Chipset	IoT technology	$P_{R_{min}}$ [dBm]
Semtech SX1257	LoRa	-142
Microchip RN2483	LoRa	-146
BP35A1	Wi-SUN	-103
CC2541	BLE	-90
CC2520	ZigBee	-98
Telit LE51-868 S	Sigfox	-126

VI. Simulation results

This section focuses on path-loss-related results with 3GPP InH models (open and mixed offices) for an LTE-like signal. The main simulation parameters are shown in Table V.

A. Path loss versus 3D distance and carrier frequency

In this simulation scenario, we assume that the coordinate of access node is $(0, 0, 3)$ m and the height of robot is 1m. The horizontal coordinate of robot is randomly generated under the constrain $d_{3D} \leq 150$. The path loss is calculated according to eq. (5), which considers both the LOS and NLOS cases.



(a) InH Mixed office

(b) InH Open office

Fig. 1. The path loss of InH mixed office and open office model. The result is based on 1000 Monte Carlo runs.

Figure 1 shows that at equal carrier frequencies and 3D distances, the indoor mixed office suffers higher path loss compared to the indoor open office. In addition, the value of path loss in indoor mixed office ascends faster than that in indoor open office, along with either the carrier frequency or the 3D distance. The maximum path losses at the considered 3D distances (i.e., maximum 150 m) of the indoor mixed office and the indoor open office are close to 160 dB and 140 dB, respectively.

B. Capacity versus 3D distance and carrier frequency

In this simulation scenario, we use the same settings as the Section VI-A for some assumptions. Other assumptions are given in the Table V.

The discussion of capacity falls into two cases. In the simulation scenario of capacity versus carrier frequency, we choose two 3D distances, namely 6.1347 meters and 50.7163 meters, in order to test the performance of InH indoor model

[1] It is the reference SNR in the MIMO system.

TABLE V
PARAMETERS OF THE CAPACITY SIMULATION

Parameters	Value	Value
LTE-like signal	**Downlink case**	**Uplink case**
Transmitted power $P_T(P_t)$	43dBm	23dBm
Transmitter antenna gain $G_T(G_t)$	18dBi	0dBi
Transmitter feeder loss $L_T(L_t)$	4dB	0dBi
Receiver antenna gain $G_R(G_r)$	0dBi	18dBi
Receiver feeder loss $L_R(L_r)$	0dB	4dB
Receiver noise figure $N_{FR}(N_{Fr})$	7dB	5dB
Downlink bandwidth B_W	2MHz	1MHz
Efficiency η	0.6	0.6

in the near and far area along with the carrier frequency. In the simulation scenario of capacity versus 3D distance, we choose two carrier frequencies, namely 4.48 GHz and 78.11 GHz, in order to test the performance of InH indoor model in the cmWave and mmWave carrier along with the 3D distance.

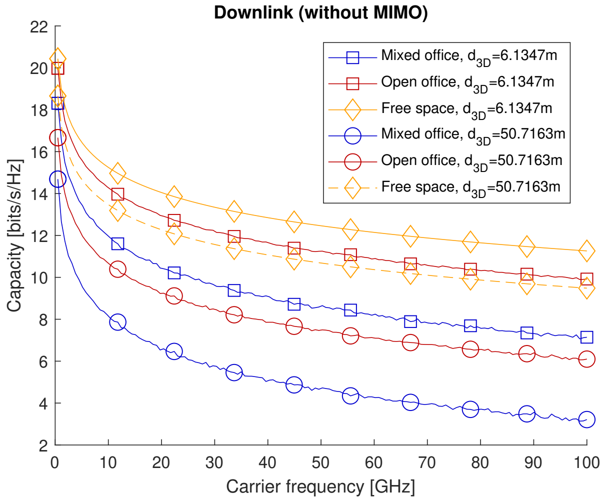


Fig. 2. Capacity versus the carrier frequency in both indoor mixed office and open office scenarios. The result is based on 1000 Monte Carlo runs.

The capacity results from Fig. 2 show that a high capacity above 18 bits/s/Hz, as targeted by some studies in Table III is achievable mostly at sub-GHz carrier frequencies. The more moderate target of 5 bits/s/Hz from Table III is achievable at all carrier frequencies up to 100 GHz for the open office InH model, but only at carrier frequencies below 50 GHz for mixed office InH model. We also notice from Fig. 2 that the open office InH model at small distances between the access node and the robot is only about 1 bit/s/Hz worse than the free space model.

In Fig. 3, likewise it indicates that the possibility of reaching 18 bits/s/Hz at high carrier frequency (i.e.,78.11GHz) does not exist, no matter under what scenarios. Discussing the capacity from the angle of the 3D distance, we notice that high capacity could only be achieved in the near area for both the open office and mixed office InH models.

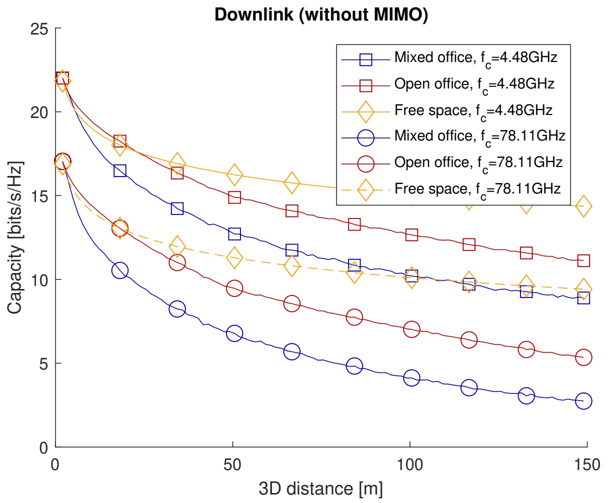


Fig. 3. Capacity versus the 3-D distance in both indoor mixed office and open office scenarios.The result is based on 1000 Monte Carlo runs.

C. Outage probability

The rejection sampling method is applied as a numerical approach to compute the outage probability. The results of numerical approach are shown in Fig. 4. The figure is given along with the carrier frequency, and the total Monte Carlo runs are 100000 times. The sampling algorithm is given as below,

```
Algorithm 1 Outage probability of a specific carrier frequency
Require: shadowing $\xi_{LOS}$ and $\xi_{NLOS}$, link budget from
    Table V, receiver sensitivity $P_{R_{min}}$ from Table IV, carrier
    frequency $f_c$, iterations $R$.
Draw $d_{3D}^{(i)} \sim \mathcal{U}(2,150)$, set variable $count = 1$
for $i = 1 : R$ do
    Calculate path loss $PL_{InH}$ according to eq. (5)
    if $PL_{InH} \geq P_T + G_T - L_T + G_R - L_R - P_{R_{min}}$ then
        $count = count + 1$
    else
        Continue to the next for loop
    end if
end for
Outage probability $p_{out} = \frac{count}{R}$
```

The theoretic analysis of outage probability is provided as well. In Section III, we mentioned that the path losses follow Gaussian distribution when only the shadowing is considered. The outage probability p_{out} is then equivalent to $1-\Phi(\frac{x-\mu_{PL}}{\sigma_{PL}})$, where $\Phi(\cdot)$ denotes the cumulative distribution function (CDF) of the standard normal distribution, $x = P_T + G_T - L_T + G_R - L_R - P_{R_{min}}$. The results of both theoretic and numerical analysis are shown in Figs. 4.

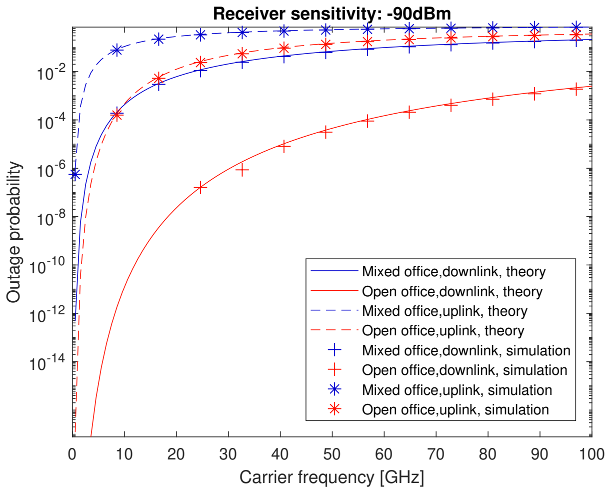


Fig. 4. Outage probability in −90 dBm sensitivity. In the simulation 100000 Monte Carlo runs are implemented.

one receiver sensitivity value applies in this simulation scenario, namely −90dBm (BLE case of Table IV). At a high receiver sensitivity (e.g., −146 dBm), we are able to reach very low or zero outage probabilities with both 3GPP InH channel models. At a lower receiver sensitivity (e.g., −90 dBm, the lowest receiver sensitivity in Table IV), the 10^{-2} outage probability target of Table III are achieved at sub-GHz carrier frequencies and frequencies below 3 GHz for both InH models and both in uplink and downlink, and they are achieved at carrier frequencies up to 100 GHz for the open-office InH model in downlink case.

Remark 1: We would like to mention that the difference of the results in the simulation and theory are mainly caused by the number of Monte Carlo runs. The results of simulation will eventually converge to the theoretic analysis, when the number of Monte Carlo runs tends to the infinity. However, the Monte Carlo method is very time-consuming, we could only push the result of simulation as close to the theoretic results as possible.

VII. Conclusions

This paper focused on the 3GPP indoor hotspot models (mixed office and open office) in the context of indoor industrial applications. We have compared the InH models between them and with the free space model and we have looked at the path losses, capacity, and outage probabilities achievable under these models. We have also compared the achievable figures with target values found in the literature and we have observed that the industrial targets can be reached under an open-office InH model at any carrier frequency, and under a mixed-office InH model at sub-GHz or few GHz carrier frequencies. For industrial applications in mm-waves bands (i.e., carrier frequencies above 30 GHz) more research studies are needed to improve the achievable capacity and outage probabilities.

Acknowledgement

The authors express their warm thanks to the Academy of Finland (project number 313039) for its financial support.

References

[1] S. A. Ashraf, I. Aktas, E. Eriksson, K. W. Helmersson, and J. Ansari, “Ultra-reliable and low-latency communication for wireless factory automation: From lte to 5g,” in *2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA)*, pp. 1–8, Sept 2016.

[2] I. Aktas, M. H. Jafari, J. Ansari, T. Dudda, S. A. Ashraf, and J. C. S. Arenas, “Lte evolution - latency reduction and reliability enhancements for wireless industrial automation,” in *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pp. 1–7, Oct 2017.

[3] T. X. Quach, H. Tran, E. Uhlemann, and M. T. Truc, “Secrecy performance of cognitive cooperative industrial radio networks,” in *2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, pp. 1–8, Sept 2017.

[4] G.-T. S. G. R. A. Network, “Study on 3d channel model for lte (release 12).” 3GPP TR 36.873 V12.7.0 (2017-12), 2017.

[5] G.-T. S. G. R. A. Network, “Study on channel model for frequencies from 0.5 to 100 ghz.” 3GPP TR 38.901 V14.3.0 (2017-12), 2017.

[6] Y. Li, Y. Liu, X. Zhang, and Q. Quan, “Dynamic channel model and performance analysis for lte-hi,” in *2017 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–5, March 2017.

[7] T. S. Rappaport, S. Sun, and M. Shafi, “Investigation and comparison of 3gpp and nyusim channel models for 5g wireless communications,” in *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)*, pp. 1–5, Sept 2017.

[8] B. Vejlgaard, M. Lauridsen, H. Nguyen, I. Z. Kovacs, P. Mogensen, and M. Sorensen, “Interference impact on coverage and capacity for low power wide area iot networks,” in *2017 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–6, March 2017.

[9] Y. Ai, M. Cheffena, and Q. Li, “Radio frequency measurements and capacity analysis for industrial indoor environments,” in *2015 9th European Conference on Antennas and Propagation (EuCAP)*, pp. 1–5, May 2015.

[10] L. R. Nair, B. T. Maharaj, and J. W. Wallace, “Capacity and robustness of single- and dual-polarized mimo systems in office and industrial indoor environments,” in *IEEE GLOBECOM 2007 - IEEE Global Telecommunications Conference*, pp. 4522–4526, Nov 2007.

[11] Y. Gao, T. Yang, and B. Hu, “Improving the transmission reliability in smart factory through spatial diversity with arq,” in *2016 IEEE/CIC International Conference on Communications in China (ICCC)*, pp. 1–5, July 2016.

PUBLICATION

4

Modeling and Mitigating 5G Wireless Downlink Interferences for Low-altitude Aerial vehicles

W. Wang, T. Fath, M. Valkama and E. S. Lohan

*2020 International Conference on Localization and GNSS (ICL-GNSS)*2020, 1–6

DOI: 10.1109/ICL-GNSS49876.2020.9115534

Modeling and Mitigating 5G Wireless Downlink Interferences for Low-altitude Aerial vehicles

Wenbo Wang*, Thilo Fath†, Mikko Valkama*, and Elena Simona Lohan*
* Electrical Engineering Unit, Tampere University, Finland, Emails: firstname.lastname@tuni.fi
† Airbus, Germany

***Abstract*—Future 5G networks will serve both terrestrial and aerial users, thanks to their network slicing and flexible numerology capabilities. The probability of Line-of-Sight (LoS) propagation will be intuitively higher for aerial users than for terrestrial users and this will provide a trade-off between increased capacity and increased interference. Our paper analyzes theoretically this trade-off and proposes solutions based on downlink multi-antenna beamforming and joint optimization of the signal-to-interference ratio of multiple aerial users. It is shown that Multiple-Input-Single-Output solutions offer the most convenient tradeoff between complexity and capacity /interference performance. Simulation results are provided for mmWave bands and low-altitude aerial vehicles.**

***Index Terms*—autonomous aerial vehicles, drones, interference, communication links, Signal-to-Interference Ratio (SIR), Multiple-Input-Single-Output (MISO)**

I. Introduction and motivation

5G cellular communications have already become a reality. The 5G network are meant to serve a multitude of users /robots /devices and will offer a multitude of services, thanks to the new paradigms introduced in 5G, such as network slicing [1, 2, 3, 4], network virtualization [1, 5, 6], and Software-Defined Network (SDN) [7, 8]. Future 5G wireless communications will serve not only terrestrial users, but also aerial users, such as Unmanned Aerial Aircraft (UAV), popularly known as drones, and other low-altitude aircraft (e.g., flying taxis, flying emergency aircraft, crops surveillance aircraft, etc.). The altitude's effect on wireless communication links is still not fully understood, especially when referring to altitudes of few km. The *low-altitude* terminology used in our title and in our work refers to aircraft altitudes up to 3 km, corresponding mostly to uncontrolled airspace, such as U-space aerial space [9] and G-class users [10] in aviation community.

Another differentiating factor between terrestrial and aerial users /devices is the fact that there is an increased likelihood of LoS connectivity between a terrestrial 5G Base Station (BS) and an aerial user compared to the situation when the user is on the ground. The increased LoS probability can increase reliability of the wireless connectivity, by ensuring a better Received Signal Strength (RSS) and a better Signal-to-Noise Ratio (SNR) than in Non Line-of-Sight (NLoS) scenarios. At the same time, it can also increase the amount of interference from non-desired transmitters (i.e., transmitters which are not transmitting useful information to the aerial user), and thus it may decrease the Signal-to-Interference Ratio (SIR).

The tradeoff between increased RSS and increased interference has been previously studied in the context of terrestrial users, for example, in [11] for cooperative beamforming with massive Multiple-Input Multiple-Output (mMIMO) solutions, in [12] for full-duplex solutions in Cloud Radio Access Networks (C-RAN), or in [13] for ultra dense terrestrial small cell deployments. The interference for downlink transmissions towards aerial users has been recently studied in [14] with focus on UAVs with maximum altitude of 300 m.

Our paper novelty is two-folds, namely: i) we provide a SIR model for aerial users with altitudes up to 3 km, extrapolating the 3GPP aerial channel modeling which are currently limited to 300m altitudes, and by including also cloud attenuation modeling, under eight different scenarios and ii) we propose an interference mitigation approach based on Multiple-Input Single-Output (MISO) and MIMO solutions.

II. Channel loss modeling

Wireless channel losses between an aerial receiver and a ground transmitter, including path losses and other atmospheric losses, have a large influence on determining the achievable SIR of the receivers. As we consider low-altitude vehicles with an altitude of up to 3000 m, we consider several hypotheses:

1. above 300 m altitude, we assume we have Free Space Loss (FSL) and LoS condition. This hypothesis is based on two observations:
    a. [15] reported that above 504 m, in near-urban and sub-urban areas, the measurements of path loss at L-band (i.e., 968 MHz) and C-band (i.e., 5060 MHz) fit the free space loss well;
    b. Rural Macrocell (RMa) and Urban Macrocell (UMa) models in [16] converge to the free space loss model at 300 m altitude.
2. below 300 m altitude, we use the model based on 3GPP rural macrocell (RMa) and urban macrocell (UMa) channel path-loss models [16]. In addition, according to 3GPP channel models, above 40 m and 100 m altitude in rural and urban, signals propagate purely in LoS condition, while below these altitude values, we have a combination of LoS and NLoS with probabilities defined in [16].
3. Signal attenuation due to propagation through clouds is also included in our modeling for aerial users; our model is based on ITU recommendations [17].

With these hypotheses in mind, the overall channel loss $\overline{PL}$ (large-scale loss, in dB scale) is given by,

$$\overline{PL} = \begin{cases} L^{3\text{GPP}} + L_{\text{cl}}(d_{\text{cl}}), & h_u \leq 300 \\ L^{3\text{GPP}}_{300} + 20\log_{10}(\frac{d}{d_{300}}) + +L_{\text{cl}}(d_{\text{cl}}), & h_u > 300 \end{cases} \tag{1}$$

where $L^{3\text{GPP}}$ is the 3GPP channel loss model in [16], $L_{\text{cl}}(\cdot)$ is the clouds attenuation model in [17], d_{cl} (in meter) is the propagation distance within clouds, $L^{3\text{GPP}}_{300}$ is a constant calculated by the above mentioned 3GPP channel loss model at 300 m altitude, d_{300} (in meter) is the transmitter-receiver (T-R) separation distance when the receiver is at 300 m altitude, d (in meter) is the actual T-R separation distance, h_u (in meter) is the altitude of users. The above parameters are also depicted in Fig. 1 for clarity purposes.

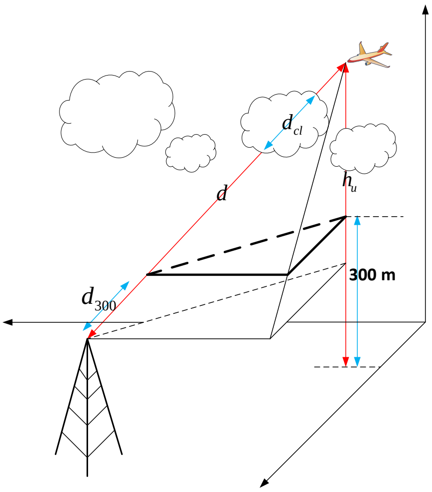


Fig. 1: Example of the channel loss model for aerial users.

III. Interference models

Cellular networks have been traditionally optimized to offer best performance to terrestrial users, e.g., by maximizing their SIR. SIR maximization can come with an increase in the TX power, and thus with an increase in the interference towards other users sharing the same frequency bands. In particular, such interference can be highly detrimental to aerial users, which are more likely to be in LoS connections than terrestrial ones. In order to model and analyze the interference, we will focus on two cases:

1) Multiple transmitters (TX) and single receiver (RX), i.e., the non-cooperative case. In this situation, each RX aims at maximizing its own SIR independently, no coordination of transmitters exists;
2) Multiple transmitters (TX) and multiple receivers (RX), i.e., the cooperative case. The difference to the previous case is that now, the designer is trying to maximize the overall performance for all users (terrestrial and aerial), by defining a properly chosen utility function which depends on the individual SIR.

In addition to the two cases described above, we will also consider the following four sub-cases:

i. Single-Input-Single-Output (SISO), i.e., omni-directional antennas both at TX and RX side;
ii. Single-Input-Multiple-Output (SIMO), i.e., omni-directional antenna at TX side and directional/multi-array antenna at RX side;
iii. MISO, i.e., directional/multi-array antenna at TX side and omni-directional antenna at RX side and
iv. MIMO, i.e., directional/multi-array antenna both at TX and RX sides.

The research questions we ask next are:

- to what extent are aerial users more affected by interference compared to terrestrial users, assuming that all other conditions are unchanged?
- which of the four above-mentioned antenna sub-cases is to be chosen by a designer who wants to achieve the best trade-off between interference and SIR and what metric is to be used for this?

A. Multiple TX and single RX

Let us consider first the non-cooperative scenario depicted in Fig. 2a that consists of N transmitters (TX) and one receiver (RX). The numbers of transmitters form a set denoted by $\mathcal{N}_{tx} = \{1, 2, 3, \cdots, N\}$. We make the assumption that the desired signal is from the k-th transmitter, while the other $N-1$ transmitters only cause interference. The numbers of transmitters whose signals reach the receiver simultaneously is a subset of the set $\mathcal{N}_{tx}$; this subset is denoted by $\mathcal{K}_t$ and we know that $\mathcal{K}_{tx} \subseteq \mathcal{N}_{tx}$. The SIR is defined as,

$$\text{SIR} = \frac{P_r}{P_{in}} \tag{2}$$

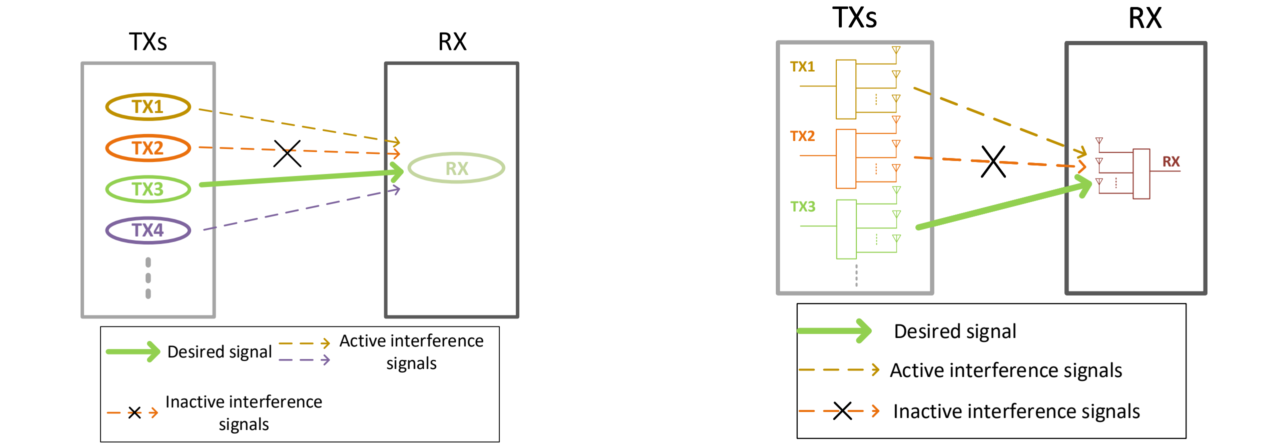
where SIR is in linear scale, P_r is the received signal power (in Watt) from the desired transmitter, P_{in} is the overall received interference signal power (in Watt) from all interfering base stations.

By slightly modifying the Friis formula, P_r yields to,

$$P_r = P_t^{(k)} G_t^{(k)} \xi_t^{(k)} G_r^{(k)} \xi_r L^{(k)} \tag{3}$$

where $P_t^{(k)}$ is the transmitted signal power (in Watt) from the k-th transmitter, $G_t^{(k)}$ is the k-th transmitter's gain (linear scale), $\xi_t^{(k)}$ is the loss (linear scale) in the k-th transmitter, $G_r^{(k)}$ is the receiver gain (linear scale) when receiving signals from the k-th transmitter, ξ_r is the loss (linear scale) in the receiver, e.g., due to feeders, $L^{(k)}$ is the path-loss (linear scale) of the channel between the k-th transmitter and the receiver. The channel loss $L^{(k)}$ is proportional to the T-R separation distance and the carrier signal frequency, according to the selected path-loss channel model.

Similarly, the overall received interference signal power P_{in} yields to,


TXs
RX
TX1
TX2
TX3
TX4
RX
Desired signal
Active interference signals
Inactive interference signals
TXs
RX
TX1
TX2
TX3
RX
Desired signal
Active interference signals
Inactive interference signals

(a) Illustration of a scenario with multiple TX and one RX.

(b) Illustration of interference channels in MIMO systems.

Fig. 2: Interference channels in multiple TX and one RX scenario.

$$P_{in} = \sum_{i\in\mathcal{K}_{tx}, i\neq k} P_t^{(i)} G_t^{(i)} \xi_t^{(i)} G_r^{(i)} \xi_r L^{(i)} \tag{4}$$

Under (3) and (4), (2) becomes,

$$\text{SIR} = \frac{P_t^{(k)} G_t^{(k)} \xi_t^{(k)} G_r^{(k)} L^{(k)}}{\sum\limits_{i\in\mathcal{K}_{tx}, i\neq k} P_t^{(i)} G_t^{(i)} \xi_t^{(i)} G_r^{(i)} L^{(i)}} \tag{5}$$

the loss ξ_r in the receiver is treated as temporally and spatially invariant hence can be cancelled, whereas the receiver gain $G_r^{(i)}$ varies in the multiple antennas system.

1) SISO: SISO refers to the case with an omni-directional antenna at both the transmitter and receiver side. The SISO system in multiple TX and single RX scenario is the benchmark for the other cases considered in this paper. In the SISO system, if we assume that the gain and loss in all the transmitters are identical, the SIR in (5) is now,

$$\text{SIR}_{\text{SISO}} = \frac{P_t^{(k)} L^{(k)}}{\sum\limits_{i\in\mathcal{K}_{tx}, i\neq k} P_t^{(i)} L^{(i)}} \tag{6}$$

Within a given dynamic range, the transmitted power P_t typically has constraints (e.g., physical limitation of amplifiers, domestic regulatory, economic considerations etc.), and thus the channel loss L dominates the SIR.

2) MISO/SIMO: MISO refers to the case with multiple antennas at the transmitter side and an omni-directional antenna at the receiver side. SIMO refers to the case with an omni-directional antenna at the transmitter side and multiple antennas at the receiver side.

In the MISO system, if we assume that losses for all transmitters are identical, the SIR in (5) transforms into,

$$\text{SIR}_{\text{MISO}} = \frac{P_t^{(k)} [\mathbf{L}^{(k)}]^{\mathsf{H}} \mathbf{G}_t^{(k)}}{\sum\limits_{i\in\mathcal{K}_{tx}, i\neq k} P_t^{(i)} [\mathbf{L}^{(i)}]^{\mathsf{H}} \mathbf{G}_t^{(i)}} \tag{7}$$

where $[\cdot]^{\mathsf{H}}$ is Hermitian transpose, $\mathbf{L}^{(k)}$ is $n_t \times 1$ channel loss vector (linear scale) from the kth transmitter, $\mathbf{G}_t^{(k)}$ is $n_t \times 1$ gain vector (linear scale) of the kth transmitter, n_t denotes the number of antennas in the transmitter.

In the SIMO system, if we assume the gain and loss in all transmitters are identical, the SIR in (5) becomes,

$$\text{SIR}_{\text{SIMO}} = \frac{P_t^{(k)} [\mathbf{G}_r]^{\mathsf{H}} \mathbf{L}^{(k)}}{\sum\limits_{i\in\mathcal{K}_{tx}, i\neq k} P_t^{(i)} [\mathbf{G}_r]^{\mathsf{H}} \mathbf{L}^{(i)}} \tag{8}$$

where $\mathbf{G}_r$ is the $n_r \times 1$ gain vector (linear scale) of the receiver, $\mathbf{L}^{(k)}$ is $n_r \times 1$ channel loss vector (linear scale) from the k-th transmitter with n_r denoting the number of antennas at the receiver.

3) MIMO: MIMO refers to the case with multiple antennas at both the transmitter and receiver side. In the MIMO system, if we assume the losses of all transmitters are identical, the SIR in (5) is then,

$$\text{SIR}_{\text{MIMO}} = \frac{P_t^{(k)} [\mathbf{G}_r]^{\mathsf{H}} \mathbf{L}^{(k)} \mathbf{G}_t^{(k)}}{\sum\limits_{i\in\mathcal{K}_{tx}, i\neq k} P_t^{(i)} [\mathbf{G}_r]^{\mathsf{H}} \mathbf{L}^{(i)} \mathbf{G}_t^{(i)}} \tag{9}$$

where $\mathbf{L}^{(k)}$ is the $n_r \times n_t$ channel loss vector (linear scale) from the k-th transmitter.

B. Multiple TX and multiple RX

Let us now consider the cooperative scenario shown in Fig. 3 that consists of N transmitters (TX) and M receivers (RX). In order to keep consistency of the notations used in this paper, we define the numbers of transmitters as a set $\mathcal{N}_{tx} = \{1, 2, 3, \cdots, N\}$ and the numbers of receivers as a set $\mathcal{M}_{rx} = \{1, 2, 3, \cdots, M\}$. The desired signal is transmitted from the k-th transmitter to the j-th receiver. The numbers of transmitters whose signals reach the j-th receiver simultaneously is a subset of the set $\mathcal{N}_{tx}$ denoted by $\mathcal{K}_{tx}^{(j)}$ with

$\mathcal{K}_{tx}^{(j)} \subseteq \mathcal{N}_{tx}$. The numbers of receivers receiving signals at the same time is a subset of the set $\mathcal{M}_{rx}$ denoted by $\mathcal{J}_{rx}$ with $\mathcal{J}_{rx} \subseteq \mathcal{M}_{rx}$.

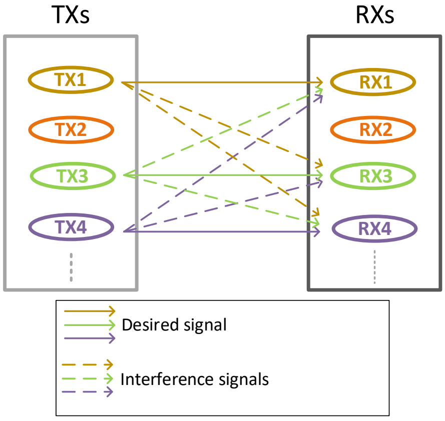


Fig. 3: Illustration of a scenario with multiple TX and multiple RX.

The SIR in (5) at j-th receiver is then,

$$\mathrm{SIR}^{(j)} = \frac{P_t^{(kj)} G_t^{(kj)} \xi_t^{(k)} G_r^{(kj)} L^{(kj)}}{\sum\limits_{i \in \mathcal{K}_{tx}^{(j)}, i \neq k} P_t^{(ij)} G_t^{(ij)} \xi_t^{(i)} G_r^{(ij)} L^{(ij)}} \tag{10}$$

where $P_t^{(kj)}$ is the transmitted power (in Watt) from the k-th transmitter to the j-th receiver, $G_t^{(kj)}$ is the antenna gain (linear scale) from the k-th transmitter to the j-th receiver, $G_r^{(kj)}$ is the antenna gain (linear scale) of the j-th receiver, $L^{(kj)}$ is the channel loss (linear scale) from the k-th transmitter to the j-th receiver.

At a time instant, the SIR of all active receivers could be represented by a set,

$$\mathcal{S} = \{\mathrm{SIR}^{(j)} : j \in \mathcal{J}_{rx}\} \tag{11}$$

In order to analyze the overall performance of multiple receivers scenarios, it is common to apply utility functions to the above SIR set [18]. In this work, it is of interest minimize the SIR for aerial users, i.e., to find first the minimum value in the set $\mathcal{S}$. Hence we define a utility function U as,

$$\begin{aligned} &U : \mathrm{SIR}^{(j)} \mapsto \mathrm{SIR}_{\mathrm{min}}, \\ &\mathrm{SIR}^{(j)}, \mathrm{SIR}_{\mathrm{min}} \in \mathcal{S}, \\ &U(\mathrm{SIR}^{(j)}) = \min_{j \in \mathcal{J}_r} \mathrm{SIR}^{(j)}. \end{aligned} \tag{12}$$

Besides, for terrestrial users, weighted sum-rate as a utility function is commonly used [18],

$$U^{WSR}(\mathrm{SIR}^{(j)}) = \frac{1}{|\mathcal{S}|} \sum_{j \in \mathcal{J}_r} \mathrm{SIR}^{(j)} \tag{13}$$

In this paper, since it is of our interest to investigate how the aerial users are affected by the interference, the lowest SIR of an aerial user needs to be above a certain threshold, we select (12) as our metric to evaluate the level of interference in multiple TX and multiple RX scenarios.

1) SISO: In the SISO system, if we assume that the gains and losses of all the transmitters are identical, the SIR in (10) becomes,

$$\mathrm{SIR}_{\mathrm{SISO}}^{(j)} = \frac{P_t^{(kj)} L^{(kj)}}{\sum\limits_{i \in \mathcal{K}_{tx}^{(j)}, i \neq k} P_t^{(ij)} L^{(ij)}} \tag{14}$$

2) MISO/SIMO: In the MISO system, if we assume that the losses of all transmitters are identical, the SIR in (10) is then,

$$\mathrm{SIR}_{\mathrm{MISO}}^{(j)} = \frac{P_t^{(kj)} [\mathbf{L}^{(kj)}]^{\mathsf{H}} \mathbf{G}_t^{(kj)}}{\sum\limits_{i \in \mathcal{K}_{tx}, i \neq k} P_t^{(ij)} [\mathbf{L}^{(ij)}]^{\mathsf{H}} \mathbf{G}_t^{(ij)}} \tag{15}$$

In the SIMO system, if we assume that the gains and losses of all transmitters are identical, the SIR in (10) becomes,

$$\mathrm{SIR}_{\mathrm{SIMO}}^{(j)} = \frac{P_t^{(kj)} [\mathbf{G}_r^{(kj)}]^{\mathsf{H}} \mathbf{L}^{(kj)}}{\sum\limits_{i \in \mathcal{K}_{tx}, i \neq k} P_t^{(ij)} [\mathbf{G}_r^{(ij)}]^{\mathsf{H}} \mathbf{L}^{(ij)}} \tag{16}$$

3) MIMO: In the MIMO system, if we assume that the losses of all transmitters are identical, the SIR in (10) transforms to,

$$\mathrm{SIR}_{\mathrm{MIMO}}^{(j)} = \frac{P_t^{(kj)} [\mathbf{G}_r^{(kj)}]^{\mathsf{H}} \mathbf{L}^{(kj)} \mathbf{G}_t^{(kj)}}{\sum\limits_{i \in \mathcal{K}_{tx}, i \neq k} P_t^{(ij)} [\mathbf{G}_r^{(ij)}]^{\mathsf{H}} \mathbf{L}^{(ij)} \mathbf{G}_t^{(ij)}} \tag{17}$$

IV. Interference for Aerial Users

A. Aerial users vs terrestrial users

As we discussed in the introduction, on the one hand, the desired signals received by aerial users undergo LoS propagation, which means lower signal attenuation compared to NLoS propagation for the same channel; on the other hand, the interfering signals experience also LoS conditions, and thus are subject to lower attenuation as well. In contrast, both desired and the interfering signals likely experience a mixture of LoS and NLoS loss for terrestrial users. Intuitively, it is difficult to give a simple judgment, whether aerial users are more vulnerable to the interference or not compared to terrestrial users.

Using (6) and assuming that the transmitted power of all transmitters is the same (i.e., no power control techniques are applied) and that the T-R separation distance for both aerial users and terrestrial users is the same, we numerically compare SIR for terrestrial and aerial users.

Fig. 4 demonstrates the comparison of SIR for an aerial and a terrestrial user. The considered carrier frequency is 30 GHz, the altitude of the aerial user is 150 m, the altitude of the terrestrial user is 2 m, the height of all transmitters is 35 m, the T-R separation distance between the desired transmitter and the respective user is 200 m, the T-R separation distance between the interfering transmitters and the user follows a uniform distribution $\mathcal{U}(250, 5000)$ (in meter). Due to the relatively low

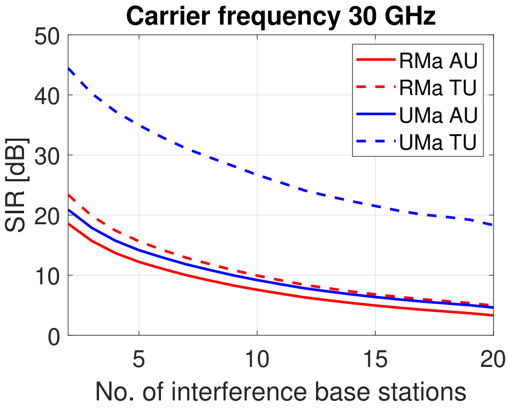


Fig. 4: Comparisons of SIR for an aerial user (AU) and a terrestrial user (TU).

altitude, the attenuation caused by clouds is not considered in this evaluation.

Using (14), in addition to the assumptions made in Fig. 4, we implement numerical analysis considering the attenuation caused by clouds. Fig. 5 shows the comparison of SIR for three aerial and three terrestrial users. The T-R separation distance between the desired transmitter and three aerial and three terrestrial users is 170, 200, 230 m respectively. The considered attenuation caused by clouds is, under consideration of $0.5\,\text{g/m}^3$ liquid water density, the ratio between the propagation distance within clouds and the T-R separation distance which follows a uniform distribution $\mathcal{U}(0, 0.5)$. The SIR shown in Fig. 5 is under the utility function (12) for three aerial /terrestrial users.

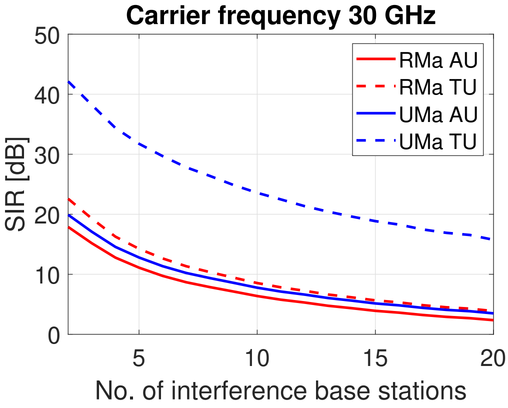


Fig. 5: Comparisons of SIR for 3 aerial users (AU) and 3 terrestrial users (TU).

Clearly, in both Fig. 4 and Fig. 5, the aerial users are more vulnerable to interference than terrestrial users. Especially in the urban area, the SIR of terrestrial users is at least 10 dB higher than the SIR of aerial users.

V. Multi-antenna-based interference mitigation

Ideally, by applying multiple antenna systems (i.e., MISO, SIMO, MIMO), the interference could be cancelled by appropriately using the null parts in the antenna radiation pattern. However, a perfect cancellation of interference has very high demands on the system, for example w.r.t. perfect beam alignment. In wireless communications for aerial drones, it is sensible to consider the aggregate interference to be small. For example, in (7) the interference can be considered to be

$$\sum_{i\in\mathcal{K}_{tx}, i\neq k} P_t^{(i)} [\mathbf{L}^{(i)}]^{\mathsf{H}} \mathbf{G}_t^{(i)} = \varepsilon \qquad (18)$$

where ε is a small positive number.

Utilization of multiple-antenna drone systems is considered in the 5G standard. It is thus of interest to see how the MISO/SIMO (i.e., considering the downlink as MISO scenario and the uplink as SIMO scenario) system could mitigate interference in wireless links for aerial drones.

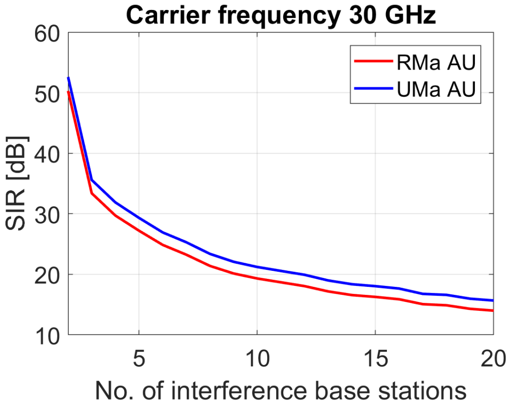


Fig. 6: SIR of an aerial user (AU) applying a MISO system.

In Fig. 6, besides of considering a 8×8 URA (Uniform Rectangular Array) in the transmitters, we used the same parameters as in Fig. 4, while the misalignment of beams is considered in Fig. 6. In comparison to Fig. 4, it can be seen that the MISO system significantly suppresses the interference in both RMa AU and UMa AU. For instance, for the case of 20 interference source transmitters, the MISO system improves the SIR by around 10 dB compared to the SISO system.

In the future, considering the upcoming mmWave bands, it is very promising to apply multiple-antenna systems on board of drones. We also simulate the MIMO scenario to have an idea how much the on-board multiple antenna system could help to mitigate interference.

Comparing Fig. 7 with Fig. 6, we can observe that due to 4×4 URA on board, the SIR is generally improved by 2–3 dB. However, the benefit of 2–3 dB in SIR performance is gained at the cost of higher complexity for all aerial users' on-board communication systems.

VI. Design recommendations

Based on the presented results, the design recommendations for using 5G to support communication data links for low-altitude aerial vehicles can be summarized as follows:

- The use of antenna arrays at the base station (i.e., MISO configuration) significantly reduces inference for the signals of aerial users.

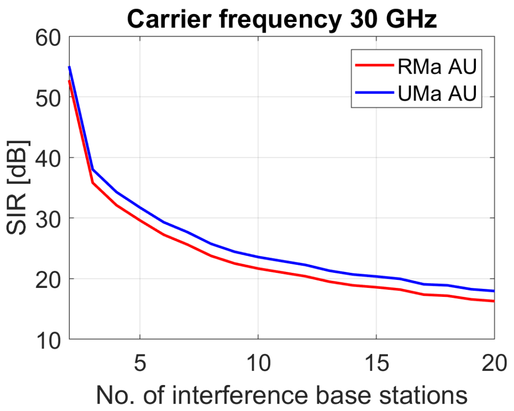


Fig. 7: SIR of an aerial user (AU) applying a MIMO system.

- The use of MIMO solutions will provide only a few dB extra gain for the receiver compared to the MISO case, at the cost of additional complexity due to the antenna arrays needed on-board of the aircraft. Therefore, MISO solutions are recommended as best tradeoff between complexity and performance. In addition, as future 5G base stations are to be equipped with multiple-antenna systems, MISO solutions are fully feasible in the near term future.

VII. Conclusion

Future 5G networks have large potential in serving aerial users. In contrast to terrestrial users, for which traditional communication networks are optimized for, aerial users are in LoS propagation conditions for most of the time (e.g., during cruising phase). Through numerical analysis, it has been shown that aerial users are more vulnerable to interference than terrestrial users. By applying a MISO/SIMO system (i.e., applying a multiple antenna system at the base station), a large improvement in the mitigation of interference can been achieved. The MIMO system does not bring too much extra improvement compared to the MISO/SIMO system but largely increases complexity of the on-board communication system.

Acknowledgements

The authors would like to thank the Academy of Finland (ULTRA project), for funding this research work.

References

[1] D. A. Chekired, M. A. Togou, L. Khoukhi, and A. Ksentini, "5g-slicing-enabled scalable sdn core network: Toward an ultra-low latency of autonomous driving service," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 8, pp. 1769–1782, Aug. 2019. DOI: 10.1109/JSAC.2019.2927065.

[2] X. Foukas, G. Patounas, A. Elmokashfi, and M. K. Marina, "Network slicing in 5g: Survey and challenges," *IEEE Communications Magazine*, vol. 55, no. 5, pp. 94–100, May 2017. DOI: 10.1109/MCOM.2017.1600951.

[3] I. Afolabi, T. Taleb, K. Samdanis, A. Ksentini, and H. Flinck, "Network slicing and softwarization: A survey on principles, enabling technologies, and solutions," *IEEE Communications Surveys Tutorials*, vol. 20, no. 3, pp. 2429–2453, 2018. DOI: 10.1109/COMST.2018.2815638.

[4] F. D'Ursol, C. Grasso, C. Santoro, F. F. Santoro, and G. Schembra, "The tactile internet for the flight control of uav flocks," in *2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft)*, Jun. 2018, pp. 470–475. DOI: 10.1109/NETSOFT.2018.8458493.

[5] X. Zhang and Q. Zhu, "Scalable virtualization and offloading-based software-defined architecture for heterogeneous statistical qos provisioning over 5g multimedia mobile wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 12, pp. 2787–2804, Dec. 2018. DOI: 10.1109/JSAC.2018.2871327.

[6] A. N. Al-Quzweeni, A. Q. Lawey, T. E. H. Elgorashi, and J. M. H. Elmirghani, "Optimized energy aware 5g network function virtualization," *IEEE Access*, vol. 7, pp. 44 939–44 958, 2019. DOI: 10.1109/ACCESS.2019.2907798.

[7] I. Bor-Yaliniz and H. Yanikomeroglu, "The new frontier in ran heterogeneity: Multi-tier drone-cells," *IEEE Communications Magazine*, vol. 54, no. 11, pp. 48–55, Nov. 2016. DOI: 10.1109/MCOM.2016.1600178CM.

[8] W. F. Elsadek, "Toward hyper interconnected iot world using sdn overlay network for ngn seamless mobility," in *2016 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*, Dec. 2016, pp. 460–463. DOI: 10.1109/CloudCom.2016.0078.

[9] L. Legros, R. Garrity, and A. Hately, *Initial view on principles for the u-space architecture*, https://www.sesarju.eu/node/3402 (accessed Aug 2019), 2019.

[10] *Airspace management operations manual - procedures for flexible use of airspace*, https://www.traficom.fi/sites/default/files/media/regulation/ASM-toimintaka%CC%88sikirja%20v1.8%20en.pdf (accessed Aug 2019), 2019.

[11] R. Dong, A. Li, W. Hardjawana, Y. Li, X. Ge, and B. Vucetic, "Joint beamforming and user association scheme for full-dimension massive mimo networks," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 8, pp. 7733–7746, Aug. 2019. DOI: 10.1109/TVT.2019.2923415.

[12] C. Fang, P. Li, and K. Feng, "Joint interference cancellation and resource allocation for full-duplex cloud radio access networks," *IEEE Transactions on Wireless Communications*, vol. 18, no. 6, pp. 3019–3033, Jun. 2019. DOI: 10.1109/TWC.2019.2908173.

[13] J. Xiao, C. Yang, A. Anpalagan, Q. Ni, and M. Guizani, "Joint interference management in ultra-dense small-cell networks: A multi-domain coordination perspective," *IEEE Transactions on Communications*, vol. 66, no. 11, pp. 5470–5481, Nov. 2018. DOI: 10.1109/TCOMM.2018.2851215.

[14] V. Yajnanarayana, Eric Wang, Y. -P, S. Gao, S. Muruganathan, and X. Lin Ericsson, "Interference mitigation methods for unmanned aerial vehicles served by cellular networks," in *2018 IEEE 5G World Forum (5GWF)*, Jul. 2018, pp. 118–122. DOI: 10.1109/5GWF.2018.8517087.

[15] D. W. Matolak and R. Sun, "Air–ground channel characterization for unmanned aircraft systems—Part III: The suburban and near-urban environments," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 8, pp. 6607–6618, 2017.

[16] *3GPP - 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Study on enhanced LTE support for aerial vehicles (release 15)*, 3GPP TR 36.777 V15.0.0, http://www.3gpp.org/DynaReport/36-series.htm, Jan. 2018.

[17] ITU, *Attenuation due to clouds and fog*, Recommendation ITU-R P.840-7, Dec. 2017.

[18] Y. Liu, Y. Dai, and Z. Luo, "Coordinated Beamforming for MISO Interference Channel: Complexity Analysis and Efficient Algorithms," *IEEE Transactions on Signal Processing*, vol. 59, no. 3, pp. 1142–1157, Mar. 2011. DOI: 10.1109/TSP.2010.2092772.

PUBLICATION 5

A Survey of Spoofer Detection Techniques via Radio Frequency Fingerprinting with Focus on the GNSS Pre-Correlation Sampled Data

W. Wang, I. Aguilar Sanchez, G. Caparra, A. McKeown, T. Whitworth and E. S. Lohan

Sensors 21.9 (2021)
DOI: 10.3390/s21093012

sensors

MDPI

Article

A Survey of Spoofer Detection Techniques via Radio Frequency Fingerprinting with Focus on the GNSS Pre-Correlation Sampled Data

Wenbo Wang [1,*], Ignacio Aguilar Sanchez [2], Gianluca Caparra [2], Andy McKeown [3], Tim Whitworth [3] and Elena Simona Lohan [1]

[1] Electrical Engineering Unit, Faculty of Information Technology and Communication Sciences, Tampere University, 33720 Tampere, Finland; elena-simona.lohan@tuni.fi

[2] European Space Agency, European Space Research and Technology Centre, 2201 AZ Noordwijk, The Netherlands; Ignacio.Aguilar.Sanchez@esa.int (I.A.S.); Gianluca.Caparra@esa.int (G.C.)

[3] GMV-NSL, Nottingham NG7 2TU, UK; andy.mckeown@gmvnsl.com (A.M.); tim.whitworth@gmvnsl.com (T.W.)

* Correspondence: wenbo.wang@tuni.fi

Abstract: Radio frequency fingerprinting (RFF) methods are becoming more and more popular in the context of identifying genuine transmitters and distinguishing them from malicious or non-authorized transmitters, such as spoofers and jammers. RFF approaches have been studied to a moderate-to-great extent in the context of non-GNSS transmitters, such as WiFi, IoT, or cellular transmitters, but they have not yet been addressed much in the context of GNSS transmitters. In addition, the few RFF-related works in GNSS context are based on post-correlation or navigation data and no author has yet addressed the RFF problem in GNSS with pre-correlation data. Moreover, RFF methods in any of the three domains (pre-correlation, post-correlation, or navigation) are still hard to be found in the context of GNSS. The goal of this paper was two-fold: first, to provide a comprehensive survey of the RFF methods applicable in the GNSS context; and secondly, to propose a novel RFF methodology for spoofing detection, with a focus on GNSS pre-correlation data, but also applicable in a wider context. In order to support our proposed methodology, we qualitatively investigated the capability of different methods to be used in the context of pre-correlation sampled GNSS data, and we present a simulation-based example, under ideal noise conditions, of how the feature down selection can be done. We are also pointing out which of the transmitter features are likely to play the biggest roles in the RFF in GNSS, and which features are likely to fail in helping RFF-based spoofing detection.

Keywords: global navigation satellite systems (GNSS); spoofing; radio frequency fingerprinting (RFF); I/Q (pre-correlation) data; support vector machines (SVM); classifiers; feature extractors

Citation: Wang, W.; Aguilar Sanchez, I.; Caparra, G.; McKeown, A.; Whitworth, T.; Lohan, E.S. A Survey of Spoofer Detection Techniques via Radio Frequency Fingerprinting with Focus on the GNSS Pre-Correlation Sampled Data. *Sensors* **2021**, *21*, 3012. https://doi.org/10.3390/s21093012

Academic Editor: Kamil Krasuski

Received: 26 February 2021
Accepted: 21 April 2021
Published: 25 April 2021

1. State-of-The-Art-Review and Paper Contributions

The radio frequency fingerprinting (RFF) concept refers to the process of identifying the hardware (HW) characteristic and HW-specific features or signatures embedded in the radio frequency (RF) waves transmitted over a wireless channel [1–4]. In a strict sense, RFF refers only to the transmitter-specific HW features. In a broader sense, the RFF process has also been studied in the context of channel characteristics or features, typically in the context of indoor positioning [5–8], as well as in the context of joint transmitter–receiver identification [9]. In this paper, we adopted the first definition of RFF, namely that the 'features' to be identified refer to HW specifics of a wireless transmitter. As a side note, this RFF concept is also encountered in the research literature under the names of *specific emitter identification (SEI)* or *physical layer identification*. The purpose of any RFF technique is to identify genuine transmitters (or transceivers) and distinguish them from malicious ones. For example, the authors in [10] performed a thorough analysis of GPS signals using a 30 m dish antenna, illustrating the evolution of the signal quality among the different GPS satellite generations. The paper indirectly showed that with a sufficiently high gain antenna, if the signal-to-noise ratio (SNR) is sufficiently improved, it is possible to identify the specific GNSS signal transmitter.

Especially in the context of global navigation satellite systems (GNSS), intentional interference such as jamming and spoofing has been on the rise in recent years and can have significant adverse effects on the navigation performance of GNSS receivers, as discussed for example in [11–15].

Future aviation applications, and in particular unmanned aerial vehicles (UAVs), will increasingly rely on GNSS-based navigation and positioning solutions [14,15]. Safety-critical applications, such as those from the aviation domain, require a high capability of anti-spoofing and anti-jamming detection, or, in other words, a high identification accuracy of genuine and malicious transmitters.

There are many authentication and anti-spoofing methods in GNSS which are not based on RFF and such methods that have been widely studied in post-correlation, and especially at navigation levels [11,16–19]. Recently, with the advent of RFF concepts in many non-GNSS wireless communications and with increased capabilities of machine learning (ML) approaches, the RFF solutions have also started to be considered in the GNSS field; in particular, the research problem of whether RFF could work with raw GNSS data, in the pre-correlation domain, before acquisition and tracking, remains an unsolved problem. It is the purpose of this paper to shed more light on whether RFF on pre-correlation GNSS data can work and which are the challenges and limitations in this field. In order to address this research gap of how to apply the well-known radio frequency fingerprinting and ML methods (to date widely used in other research fields) in the context of GNSS receivers, we present here a comprehensive survey of RFF and ML methods, discuss their applicability in the GNSS context, and we introduce a novel methodology to deal with RFF in GNSS, by presenting equivalent block diagrams of the genuine and non-genuine GNSS transmitters. We also give an initial glimpse of what kind of transmitter features are the most important in the context of GNSS transmitters, based on an in-house-made simulator, with Matlab and Python modules. We further summarize the remaining challenges when dealing with realistic environments and point out a few possible paths for future research in this challenging field.

A schematic block diagram of the three domains (pre-correlation, post-correlation, and navigation) of a typical GNSS receiver is shown in Figure 1. The pre-correlation domain refers to the data at the output of the Automatic Gain Converter (AGC) and Analog-to-Digital Converter (ADC) shown in Figure 1, in other words, to the raw I/Q samples before the acquisition stage of the GNSS receiver. These samples are typically received at a very low signal-to-noise-ratio, but they can carry important information about the ’features’ of the transmitter, as they are not yet smoothed or filtered with the correlation filters.

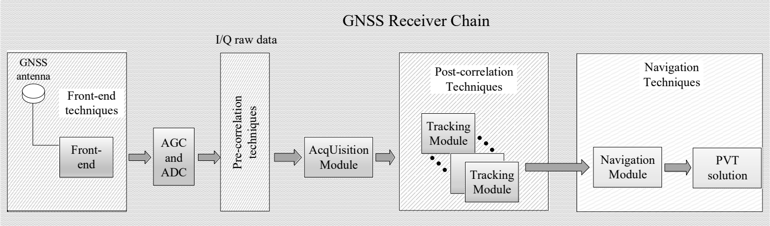


Figure 1. The three domains of a typical GNSS receiver: pre-correlation; post-correlation; and navigation domains.

A good survey of anti-spoofing methods based on the post-correlation and navigation data in GNSS can be found for example in [19]. However, no pre-correlation methods and no RFF methods were addressed in there. Others surveys of anti-spoofing methods can be found for example in our previous work in [11,20], where again only the post-correlation and navigation anti-spoofing solutions were addressed. Feature-selection methods for RFF based on the navigation domain of a GNSS signal have also been addressed in [21]. Surveys on the RFF methods are more difficult to find in the current literature, and they are typically focused on non-GNSS signals, such as cellular, Internet of Things (IoT), or WiFi signals [22–26].

As seen in the discussions above, there is still a lack of surveys of RFF methods for GNSS transmitter authentication in the current literature, particularly on surveys of GNSS authentication relying on pre-correlation signals. In this paper, we are addressing this lack, via a comprehensive study of the literature in the past two decades, as well as via theoretical insights and the preliminary analysis of algorithms. Our contributions are as follows:

1. Offering a thorough survey of RFF methods applied with GNSS and non-GNSS wireless data in the literature, and discussing which of these RFF methods have potential in GNSS, and in particular in GNSS with pre-correlation data. Finding good anti-spoofing methods based on pre-correlation GNSS data could have tremendous benefits for the future GNSS receivers, by being able to detect and remove non-genuine signals even before processing them further in the acquisition and tracking loops. Our survey is unique in the current literature, as the RFF methods for GNSS have to date not been widely investigated and there is a current lack of unified surveys on this;
2. Proposing a step-by-step problem definition of RFF in the context of GNSS signals, by delving in depth in the sources of possible transmitter hardware impairments, and also discussing the possible channel and receiver–hardware impairments; this problem decomposition into feature-by-feature investigation is also lacking from the current GNSS literature, to the best of our knowledge;
3. Proposing a four-step generic RFF approach, consisting of: feature identification, feature extraction, data pre-processing, and data classification. Classical ML and transforms methods are used in this four-step methodology, but the four-step block diagram is rather novel;
4. Presenting the mathematical models of different GNSS transmitter features, with a particular emphasis of five main identified features, namely: the power amplifier non-linearities, the digital-to-analog converters' non-linearities, the phase noises of the local oscillators, the I/Q imbalances, and the band-pass filtering at the edge of the transmitter front-end; unified mathematical methods of the transmitter HW impairments are not found in the current literature to the best of the authors' knowledge;
5. Providing the equivalent transmitter block diagrams for GNSS and spoofers by incorporating the aforementioned five hardware effects into the models;
6. Presenting an illustrative simulation-based analysis based under ideal conditions in order to emphasize the impact of each HW feature on the RFF performance. Three feature extractors to identify the transmitter HW impairments were used, namely the kurtosis, the Teager–Kaiser energy operator (TKEO), and the spectrogram. The classification accuracies given as examples are based on support vector machines (SVM). Such a simplified analysis allows us to identify the strongest features among the five considered ones and to point out the remaining challenges to overcome to achieve the feasibility of RFF methods under more realistic GNSS scenarios;
7. Bringing in a qualitative discussion on the existing algorithms and providing a roadmap towards further research on RFF in GNSS for interference detection and classification.

The rest of this paper is organized as follows: Section 2 presents the use case of a spoofing attack on an on-board GNSS receiver and describes the various spoofing types and anti-spoofing approaches existing in the literature. It also clarifies the fact that the focus of our paper is on pre-correlation approaches using the I/Q sample-level data as inputs, but the proposed methodology and the identified feature extractors and classifiers can also be applied in a broader sense, with post-correlation and navigation GNSS data, as well as with non-GNSS data. Section 3 gives an overview of the main identified transmitter HW impairments (i.e, 'features'), which can separate between genuine and spoofing transmitters in RFF-based approaches. Section 4 presents the equivalent transmitter block diagrams for GNSS and spoofer signals, by emphasizing the places in the transmission payload where the various RF impairments can appear. This also shows the equivalent block diagram of the whole transmitter–channel–receiver chain and discusses the additional impairments that can be introduced by the channels and the receiver parts. Section 5 focuses on feature-extractor transforms and presents various transforms which can be employed to determine the underlying features in the received signal. Section 6 focuses on classification approaches which can be used to identify the features, after the feature-extractor transform is applied. Section 8 summarizes the main RFF solutions from the existing literature, applied on pre-correlation signals, for both GNSS and non-GNSS signals. Section 9 discusses the methods applicable to GNSS among those listed in Section 8 and offers a qualitative and comparative view of such approaches. Finally, Section 10 summarizes the open challenges in this field as well the further methodological steps to be under-taken for a designer implementing RFF algorithms based on pre-correlation GNSS data.

2. Problem Definition and Use-Case Example

Most of the GNSS signals use the code-division multiple access (CDMA) technique, with a received signal power around −160 dBW. This means that the received signals are usually below the noise floor. For this reason, the direct observation of the signal is in general not feasible, if not using extremely high gain antennas. Therefore, when applying RF fingerprinting it is essential to evaluate the capability of the technique to operate at low SNR.

A spoofing scenario is illustrated in Figure 2. In this example scenario, both the drone-based spoofer and the GNSS target receiver (e.g., a civil aircraft such as a flying taxi or a rescue helicopter) receive the broadcasting GNSS signals from satellites. During the spoofing attack, the GNSS target receiver receives the spoofing signals from the spoofer as well as together with the genuine GNSS signals from sky satellites and its task is to identify and mitigate the spoofing interference for attaining optimal positioning performance. Based on the GNSS signal received from the genuine satellites on sky, the spoofer is able to create fake GNSS-like signals which it will broadcast in the air. There are many ways in which a spoofer can generate a GNSS signal, as described below, whether these involve simplistic, intermediate, and sophisticated attacks.

Figure 2 illustrates only one of the many possible scenarios one could imagine when a GNSS receiver is spoofed by one or several malicious transmitters. More details about spoofing classes and possible mitigation solutions are addressed below.

Spoofing attacks are typically split into three classes, described in detail in [11]:

- *Simplistic spoofing attacks*, such as those generated by a software defined radio (SDR) GNSS generator connected to an antenna. In this type of attack, the GNSS transmitter is not synchronized to the genuine GNSS satellites, which means that there are typically jumps in the carrier-to-noise ratios (CNR) and Doppler shifts measured at the receiver and such spoofing attacks can be identified in the pseudorange domain via various consistency checks algorithms, such as those described in [27–29];
- *Intermediate spoofing attacks* [30,31]: these are more complex than the simplistic attacks as they combine a GNSS generator with a GNSS receiver and are able to align the code-phase and synchronize the frequency with the signal transmitted from a genuine GNSS satellite in the sky. A replay attack or a meaconing attack with a single receiver (when the signal from a genuine GNSS satellite is captured and re-sent with a delay) is an example of such an intermediate spoofing attack;

- *Sophisticated spoofing attacks* [32]: these are the most complex spoofing attacks to mitigate, as they are an extension of the intermediate spoofing attack, where the signals received from multiple GNSS antennas (sometimes placed at different locations) are modified (e.g., through random delays and Doppler shifts) and re-transmitted in a combined manner, in such a way that the receiver is duped to believe the signals are obtained from various genuine satellites.

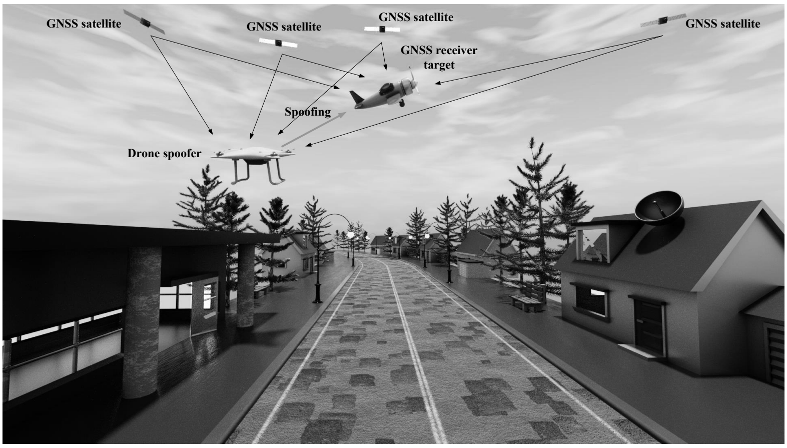


Figure 2. The illustration of a spoofer attacking scenario.

Spoofing attacks adversely affect the quality of positioning, navigation and timing (PNT) services of GNSS receivers, by introducing errors in the estimated PVT. For example, as shown in [31], an intermediate spoofer with a spoofer-to-signal ratio of 0 dB (i.e., equal spoofer and GNSS signal power) introducing a code delay of 0.5 chips can deteriorate the detection probability of the GNSS signal by 20% and with a code delay of only 0.25 chips, the detection probability decreases with 75% (i.e., from 100% to 25%). The spoofing impact on the good functionality of a GNSS receiver can be thus significant and it is of utmost importance to devise counter-spoofing methods, especially in life-critical applications such as aviation applications.

Current counter-spoofing methods can be classified into three main categories [11,33], according to the three GNSS-receiver domains depicted in Figure 1:

- *Pre-correlation link-level methods* relying on signal samples before the acquisition stage, i.e., on I/Q data. This is the case addressed in this paper. Such pre-correlation anti-spoofing methods are still very rare in the literature;
- *Post-correlation link-level methods* relying on the despread signal, at the output of the tracking stage for a single satellite. Examples can be found in [33,34] and they are out of the scope of this paper;
- *Navigation or system-level methods* relying on the pseudorange signals coming from all visible satellites. These are by far the most encountered anti-spoofing methods in the current literature and a few examples can be found in [27–29] (they are also outside the scope of this paper).

Our paper focuses on the pre-correlation spoofing identification approaches, taking as the input the I/Q raw data (at sample level) and aiming to identify, based on RF fingerprinting approaches, whether the received signal comes from a genuine GNSS transmitter or from a spoofing transmitter.

We are proposing a **four-step methodology** for the RFF-based pre-correlation spoofing detection and transmitter identification, as listed below. Each of these four steps is further detailed in Sections 3–6.

1. **Identification of relevant features**—this step refers to first identifying the different RF 'features' created by the inherent hardware impairments in any transmitter. Several such features will be subsequently described in Section 3;
2. **Feature-extraction transform**—this steps refers to choosing a suitable feature-extraction transform to emphasize the selected features from the previous step. Several feature-extraction transforms are addressed in Section 5;
3. **Data pre-processing stage**—this step refers to choosing the most suitable format of saving the data at the output of the feature-extraction transform, namely as time-stamped vector data, in matrix form, as an image of certain size and number of pixels, etc. The data format selection will be influenced by the algorithms selected in the feature-classification step, as subsequently described in Section 6, as well as by the data type at the output of the feature-extraction step. For example, spectrogram-type data are also easily stored in image form, while transforms such as kurtosis or Teager–Kaiser are more suitable to be stored in a vector format;
4. **Feature classification**—this step refers to applying a selected classification methods, such as based on analytically-derived thresholds or on machine learning algorithms when training data are available, and classifying the received signal into 'genuine' versus 'non-genuine/spoofer' classes. Several feature classification approaches are discussed in Section 6. A qualitative discussion is then provided in Section 9.

The workflow of an RFF algorithm based on the aforementioned four steps is illustrated in Figure 3.

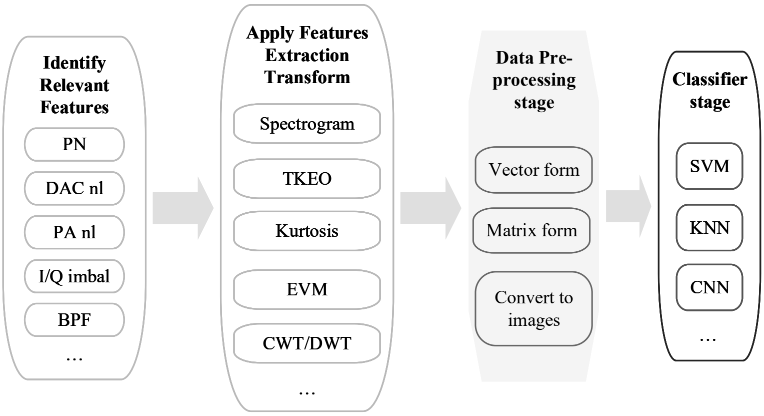


Figure 3. The proposed methodology for an RFF algorithm applied to GNSS pre-correlation sampled data.

3. Transmitter Hardware Impairments or 'RF Features' Overview

A first step in building the equivalent block diagrams for a GNSS transmitter (genuine or spoofer) was to identify the possible sources of hardware (HW) impairments at the transmitter side for wideband-signal transmitters, based on works in [35–43] and analytical thinking. Five sources of HW impairments were identified in GNSS transmitters, as follows:

1. **Phase noise (PN)**: PN is unavoidable in any wireless transmitter, as it is introduced by the transmitter clock instabilities; atomic clocks on-board genuine GNSS transmitters are intuitively expected to have lower phase noise than the clock of spoofers and other malicious transmitters [36–38]. PN models are discussed in Section 3.1;
2. **Power amplifier (PA) non-linearities**: non-linearities close to the saturation region for PAs (and especially for high-power amplification needs as it is the case of GNSS transmitters) can represent an important HW feature to distinguish between different

transmitters. In addition to non-linearities, possible memory effects of the PA can also create differentiating features at the transmitter. PA models are discussed in Section 3.2;

3. **I/Q imbalance**: the I/Q imbalance in a transmitter is introduced in the translation of the baseband signals to passband signals due to the facts that the phase shift is not perfectly at 90° in the analogue domain and that the analogue gain is not perfectly matched for I and Q components. I/Q imbalance models are discussed in Section 3.3;
4. **Digital-to-analog converter (DAC) non-linearity**: signal distortions are also possibly produced by the non-linear DAC operation at each transmitter. DAC models are discussed in Section 3.4;
5. **Band-pass filter (BPF)** passband and out-of-band ripples: the transmitter BPF filter also puts its 'fingerprint' on the transmitted signal and can act as a smoother of the other HW features. BPF models are discussed in Section 3.5.

Each of these identified HW impairments is further detailed in the subsequent subsections.

3.1. PN Models

Typically, the phase noises are random noises, modelled via random time waveforms $\phi(t)$ and characterized by their power spectral density (PSD), denoted here via $S_\phi(f)$. A non-ideal local oscillator generating a waveform of amplitude $A(t)$ at the oscillator frequency f_o outputs a signal $x(t)$ of the form [35]:

$$x(t, f_o) = A(t)cos\big(2\pi f_o t + \phi(t)\big) \tag{1}$$

The PSD of the PN is typically modelled via a power law noise [44,45]:

$$S_\phi(f) = \sum_{n_\phi=0}^{4} \frac{k_{n_\phi}}{4\pi^2 f^{n_\phi}} \tag{2}$$

where f is the frequency, k_ϕ is a constant parameter of the model and $n_\phi = 0, \ldots, 4$ are the summation parameters, defining the PN type, e.g., $n_\phi \in \{0, 2\}$ corresponds to a white-noise model (with 0 for additive white noise sources external to the oscillator and 2 for additive white noise sources internal to the oscillator), $n_\phi = \in \{1, 3\}$ corresponds to a flicker PN (i.e., 1 for flicker phase noise and 3 for flicker frequency noise), and $n_\phi = 4$ corresponds to a random-walk PN.

The usually adopted model for GNSS signals is to ignore everything except the white-noise PN model at $n_\phi = 2$ in eq. (2). In this case, the PN PSD is simplified to $S_\phi(f) = \frac{\sigma_\phi^2}{4\pi^2 f^2}$ with σ_ϕ^2 being the variance of the white noise [35]. Without a loss of generality, this white-noise PN is also the model adopted in what follows. Nevertheless, extensions to other PN PSDs are straightforward and can be easily incorporated in our model. An example of another PN PSD model can be found for example in [46] where a combination of terms at $n_\phi = 0$ and $n_\phi = 2$ was considered.

The on-board GNSS local oscillators are atomic clocks based on rubidium/cesium clocks [37]. Typical spoofer local oscillators have lower stability than classical atomic clocks and they rely on technologies such as oven-controlled crystal oscillator (OCXO) or temperature-controlled crystal oscillator (TCXO). This can be modelled with a lower PN variance σ_ϕ^2 for genuine GNSS transmitters than for spoofers.

A typical measure of the PN PSD is through the so-called Allan variance $\sigma_A^2(\tau)$ given by [47]

$$\sigma_A^2(\tau) = \frac{8}{(2\pi f_o \tau)^2} \int_0^\infty S_\phi(f) sin^2(\pi f \tau) df \tag{3}$$

Usually, it is very difficult to extract $S_\phi(f)$ from Equation (3), and as discussed for example in [47], there might be several $S_\phi(f)$ functions matching the measured $sigma_A^2(\tau)$.

Nevertheless, for the purpose of RFF, we are not interested in measuring the exact $S_\phi(f)$, but we only consider it as one of the HW features at the transmitter, with the assumption that the spoofer and the genuine GNSS transmitters have different PSDs $S_\phi(f)$.

3.2. PA Non-Linearity Models

The power amplifier is an important element in the wireless communications system, and its non-linearity behaviour varies from device to device. It is expected that PA non-linearities can also be used as differentiating features between GNSS satellite transmitters and spoofers or jammers, due to the fact the GNSS PAs are high-cost high power amplifiers (HPA), such as solid state power amplifiers (SSPA) or a travel-wave tube amplifier (TWTA) [39], while non-genuine GNSS transmitters typically have low-power amplifiers (LPA) [40]. The highest PA power efficiency is achieved at the saturation point, where heavy non-linearity occurs in all PA models [48].

There are typically two classes of models for PA non-linearities [49]: the memoryless non-linear models and the non-linear models with linear memory. The memoryless non-linear model of a system with input $x(t)$ and output $y(t)$ (assuming a continuous-time model) is given by the L_{th} order polynomial:

$$y(t) = \sum_{l=1}^{L} \alpha_l x^l(t) \tag{4}$$

where $\alpha_l, l = 1, \ldots, L$ is the l_{th} coefficient of a PA non-linearity of order L. When the wideband signals pass through the power amplifier, the bandwidth of signals is not negligible compared with the inherent bandwidth of the amplifier, and therefore a frequency-dependent behaviour occurs. This behaviour is called a memory effect. Regarding the non-linear model with linear memory, the two most encountered models are the Wiener model and the Hammerstein model, as described in [49]. We illustrated these two models in Figure 4. The corresponding mathematical expressions (this time in the discrete-time domain) are, respectively:

Wiener model:

$$y_{Wiener}(s) = \sum_{n=0}^{N} c_n \left[\sum_{q=0}^{Q-1} h(q) x(s-q) \right]^n \tag{5a}$$

Hammerstein model:

$$y_{Hammerstein}(s) = \sum_{q=0}^{Q-1} h(q) \left[\sum_{n=0}^{N} c_n x^n(s-q) \right] \tag{5b}$$

where s is the sample index (assuming the $x(t)$ signal was sampled at a sampling rate $1/T_s$, namely at $t = s/T_s$ time instants), $h(q)$ denotes the q-th coefficient of a finite impulse response (FIR) filter, and c_n denotes the n_{th} order coefficient in the polynomial memory model.

Due to the difficulties of estimating the coefficients for FIR filters in both the Wiener and Hammerstein model, the memory polynomial [50] has become a popular model for the behaviour of power amplifiers. The expression of MP is given by [50],

$$y_{MP}(n) = \sum_{k=0}^{K-1} \sum_{m=0}^{M} a_{km} x(n-m) |x(n-m)|^k \tag{6}$$

where a_{km} are the model parameters. In our work, we used the memory polynomial to model PA in navigation payload with user-defined model parameters a_{km} which were considered different for each transmitter (i.e., satellite and spoofer transmitters).

In order to maximize the power efficiency and the lifespan of the satellite payload, the GNSS signals are usually designed to exhibit a (quasi) constant complex envelope. For instance, this is achieved by including an inter-modulation product among the signal components. For this reason, it is reasonable to expect that the PA non-linearities will not significantly distort the genuine GNSS signals. This might not hold for many spoofing signals, which may simplify the signal generation by only emulating some of the signal components and/or omit the inter-modulation product. However, it shall be noted that a spoofer usually needs to generate low-power levels, hence it is easier to ensure linearity with LPA. The fact that the spoofer needs to transmit at a lower power than the GNSS transmitters is due to the fact that spoofers are usually within the range of a few tens of meters to a few km away from the GNSS receivers, while GNSS satellites are at more than 20,000 km away from the receivers.

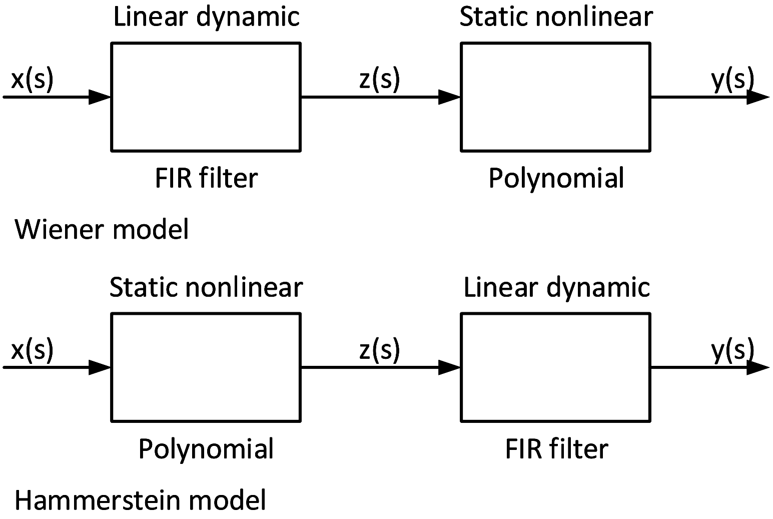


Figure 4. The block diagram for the Wiener model and Hammerstein model.

3.3. I/Q Imbalance Models

During the baseband-to-passband conversion, the I and Q components ($x_I(t)$ and $x_Q(t)$) at the transmitter can be modelled via [41,42]:

$$\begin{aligned} x_I(t) &= A(t)cos(2*pi*f_c) \\ x_Q(t) &= g_{IQ}A(t)sin(2*pi*f_c+\phi_{IQ}) \end{aligned} \tag{7}$$

where $A(t)$ is the baseband amplitude, f_c is the passband carrier frequency, g_{IQ} is the I/Q amplitude imbalance factor, also known as the gain imbalance factor [42] and measured typically in dB, and ϕ_{IQ} is the I/Q phase imbalance factor, also known as quadrature skew factor [42]. Above, the PN effect was ignored for clarity purposes. The imbalance factors g_{IQ} and ϕ_{IQ} are transmitter-dependent constants and it is expected that a genuine GNSS transmitter would have lower absolute values $|g_{IQ}|$ and $|\phi_{IQ}|$ than a spoofer. For a perfect transmitter, without any I/Q imbalance, one would have $g_{IQ}[dB] = 0$ and $\phi_{IQ} = 0$. Imperfect transmitters have been studied for example in [42], based on multipurpose universal software radio peripheral (USRP) as those that may be used by a Software Defined radio (SDR) spoofer and values below 1 dB and below 8 degrees have been estimated for $|g_{IQ}|$ and $|\phi_{IQ}|$ values, respectively.

3.4. DAC Models

Based on [43], the DAC model is given by

$$y(t) = x(t) + x^{HQ}(t) + x^{CM}(t) + x^{VQ}(t) \tag{8}$$

where $y(t)$ is the output continuous-time signal, $x(t)$ is the input continuous-time signal and the corresponding discrete-time form is $x[n]$, $x^{HQ}(t)$ is the horizontal quantization additive effect, $x^{CM}(t)$ is the clock additive effect, and $x^{VQ}(t)$ is the vertical quantization additive effect. The horizontal quantization additive effect $x^{HQ}(t)$ is given by

$$x^{HQ}(t) = \sum_{n=-\infty}^{\infty} x[n] g\left(\frac{t - nT_g}{T_g}\right) - x(t) \tag{9}$$

where T_g is a constant generation period, $g(t)$ is a unitary pulse function:

$$g(t) = \begin{cases} 1, & 0 \leq t \leq 1 \\ 0, & \text{elsewhere} \end{cases} \tag{10}$$

The clock additive effect $x^{CM}(t)$ is:

$$x^{CM}(t) = \sum_{n=-\infty}^{\infty} x[n] h_n(t - nT_g) \tag{11}$$

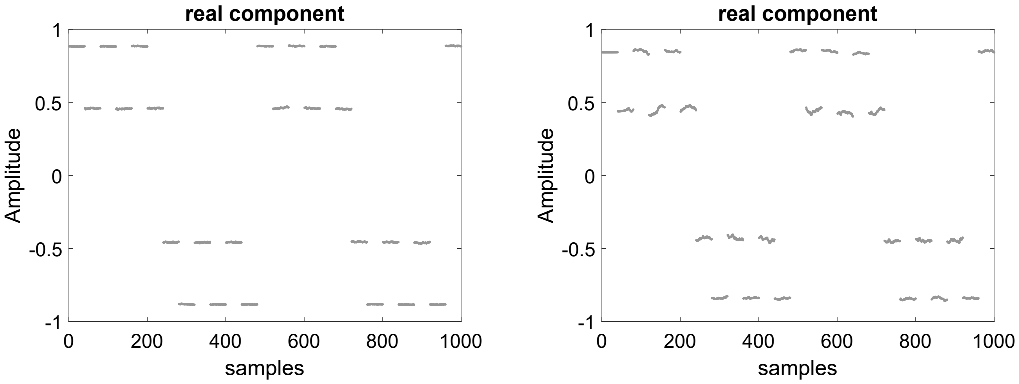
where $h_n(t)$ yields to:

$$h_n(t) = -\text{sign}(\Delta_n) g\left(\frac{t - nT_g}{\Delta_n}\right) + \text{sign}(\Delta_{n+1}) g\left(\frac{t - (n+1)T_g}{\Delta_{n+1}}\right) \tag{12}$$

where Δ_n is a time amount. For example, based on (10), $g\left(\frac{t}{\Delta_n}\right)$ has a rising edge at time instant zero and a falling edge at time instant Δ_n. By assuming the nearest voltage level that DAC could provide for $x[n]$ is $\hat{x}[n]$, the vertical quantisation additive effect is:

$$x^{VQ}(t) = \sum_{n=-\infty}^{\infty} \{\hat{x}[n] - x[n]\} \cdot \left[g\left(\frac{t - nT_g}{T_g}\right) + h_n(t - nT_g) \right] \tag{13}$$

Here, we demonstrate two examples in Figure 5a,b to illustrate the effect of DAC in different transmitters. These two examples are given for the in-phase components of the signal. Clearly, the distortions existing in spoofer DAC are heavier than that in a genuine GNSS transmitter.



(**a**) Signal after DAC in a genuine GNSS transmitter. (**b**) Signal after DAC in spoofer transmitter.

Figure 5. Examples of DAC characteristics at the transmitter, for a genuine (**a**) and a spoofer (**b**) transmitter.

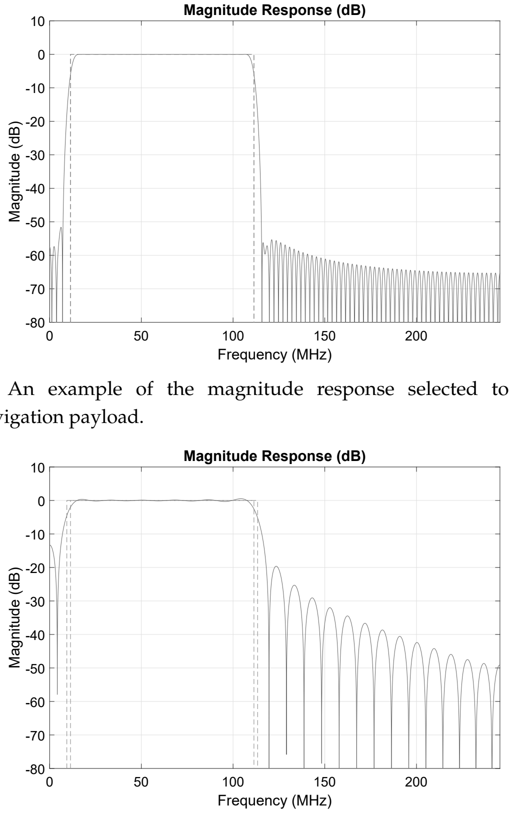
3.5. BPF Models

The band-pass filter (BPF) is equipped at transmitters to filter out undesired non-central frequencies signals. In this work, we model BPF using a finite impulse response (FIR) filter. A general form of an FIR filter output $y[n]$ can be given by

$$y[n] = \beta_0 x[n] + \beta_1 x[n-1] + \cdots + \beta_k x[n-k] + \cdots + \beta_K x[n-K] \tag{14}$$

where β_k is the k_{th} impulse response, K is the order of the filter.

We use the window design method for the genuine GNSS transmitter BPF and the least squares method for spoofer transmitter BPF. An example of BPFs used for a genuine GNSS transmitter versus a spoofer transmitter is shown in Figures 6a,b, respectively. The exact parameters of the filters used in the genuine GNSS transmitters are not known, however, without loss of generality, the assumption here is that the passband and stop-band ripples of a BPF for a genuine transmitter are smaller than those for the BPF of a spoofer. This is expected to be more evident for spoofers based on SDR, which generally include configurable BPFs.



(**a**) An example of the magnitude response selected to model the BPF for the Galileo navigation payload.

(**b**) An example of the magnitude response of a band-pass filter for a spoofer transmitter.

Figure 6. Examples of characteristics of the band-pass filter at the transmitter for a genuine (**a**) and spoofer (**b**) transmitter.

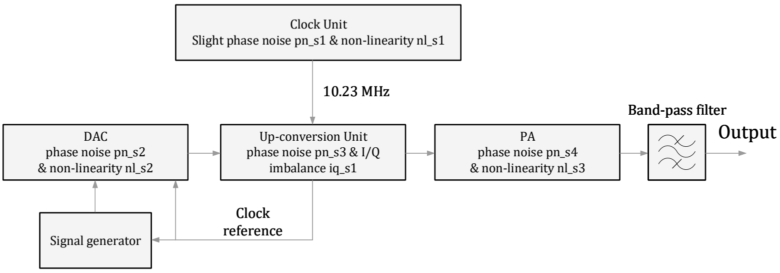
4. Equivalent Block Diagrams for GNSS and Spoofing Signals

Section 3 identified the main sources of the transmitter feature. This section will present, to the best of our knowledge for the first time in the literature, two equivalent simplified models of a genuine GNSS transmitter and a spoofer GNSS transmitter, by taking into account all five HW impairments identified and discussed in the previous section. These equivalent models will serve as the bases for addressing RFF in the context of GNSS, as they clearly identify the places of various HW features and point out situations where the same type of feature (e.g., phase noise) can affect multiple blocks. In order to build these equivalent transmitter block diagrams, we gathered information from the Galileo standards and manufacturer brochures, e.g., as in [51] and from software-defined radio GNSS transmitter sheets such as those in [52].

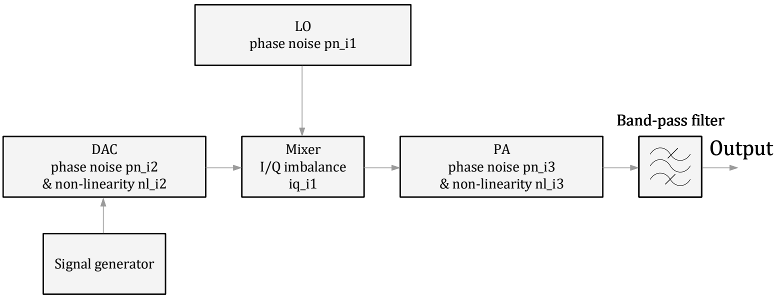
4.1. Equivalent Transmitter Block Diagrams

The equivalent block diagrams of a GNSS (e,g., Galileo) satellite transmitter and of a spoofer GNSS transmitter are depicted in Figure 7a,b, respectively. These summarizing block diagrams help in identifying at a glance the places where the different HW impairments discussed in Section 3 appear. For example, phase noises can appear in each of the transmitter blocks, such as the clock unit, Digital-to-Analog Converter (DAC), up-conversion unit/mixer units and power amplifier. I/Q imbalances are typically only present in the up-conversion unit/mixer units. Non-linearities can appear in the DAC and PA units. Different blocks have different noise levels: for example, the phase noise pn_s1 (s stands for satellite here) from the clock unit is not the same phase noise as in the up-conversion unit (phase noise pn_s2), etc. Moreover, the phase noise pn_s1 from the GNSS transmitter is different from the phase noise pn_i1 from spoofer (i stands for interferer, here), and the same is valid for all the different transmitter ((s1, s2, s3, ...) and spoofer (i1, i2, ...) features depicted in Figure 7a,b. The non-linearity nl_s1 effect in the Galileo clock unit (Figure 7a) appeared due to the additional DAC units employed in the Galileo clock unit [51]. Such additional DACs are, however, unlikely to be used in a spoofer, and thus the local oscillator (LO) of a spoofer (Figure 7b) does not exhibit additional non-linearity effects.

The GNSS power amplifier is typically an HPA, while the spoofer power amplifier is typically an LPA, as discussed in Section 3. The levels of various transmitter impairments are not known for GNSS transmitters and need to be learnt via the RFF feature extractors and classifiers discussed next, and based on training data. High-quality training data would need GNSS samples at various sampling rates (i.e., corresponding to both low-end and high-end receivers), for the duration of several milliseconds for each training sequence, and typically thousands of training sequences for robust RFF results. This may represent one of the main challenges or bottlenecks of RFF approaches at the pre-correlation level: for example, 2 ms of data sampled at a moderate sampling rate of 24 Mbps has 24,000 complex-valued samples per each sequence in the training data. Assuming 1000 sequences in the training database and data saved on 8-bit per real sample, this would require 0.48 GB of data in each training sequence. The 2 ms of data pieces per training sequence was shown as an example. We expect that several milliseconds of observations of I/Q raw data will be needed. As a rule of thumb, GNSS signal acquisition is usually performed using at least 10 ms. The needed size for the training databases increases with the increased processing time, with the increased sampling rate, and with the increased amount of sequences in the training database. Through some of the feature-extraction methods discussed in Section 5, one can reduce the dimensionality of the data, for example using images instead of matrices, or applying principal component analysis (PCA) methods to reduce the data dimensionality. More about PCA will be discussed in Section 6.



(**a**) The equivalent cascade model of GNSS transmitter and distortions, based on [51].



(**b**) The equivalent cascade model of spoofer transmitter and distortions, based on [52].

Figure 7. The diagrams of an equivalent model for GNSS and spoofer transmitter. In GNSS transmitters, all distortions are indexed with s*; in a spoofer transmitter, all distortions are indexed with i*.

4.2. Equivalent Block Diagram of the Full Transmitter-Channel-Receiver Chain

Figure 8 shows the equivalent full transmission chain of a generic system with N genuine GNSS transmitters and M spoofers, $N \geq 1, M \geq 1$. Assuming that spoofers (if more than one) are placed at different locations, the wireless channel experimented by each of the genuine and non-genuine transmitters will exhibit different multipath and fading profiles, as well as different noise levels. In this generic example, there will be $N + M$ different wireless channels, which can typically be assumed to be non-correlated. A typical channel impulse response $h_i(t), i = 1, \ldots N + M$ can be modelled via a tapped-delay line with L_i multipaths via

$$h_i(t) = \sum_{l=1}^{L_i} \alpha_{i,l}\delta(t - l\tau_{i,l}) \tag{15}$$

where $\alpha_{i,l}$ are the complex channel coefficients of the l-th path of the i-th channel, and $\tau_{i,l}$ are the multipath delays of the l-th path of the i-th channel. Above, $\delta(t)$ is the Dirac pulse. Clearly, such a channel acts as a finite impulse response (FIR) filter which is likely to smooth out some of the transmitter HW features.

A signal $s_i(t), i = 1, \ldots N + M$ originated from a genuine GNSS transmitter ($i = 1, \ldots N$) or from a spoofer ($i = N + 1, \ldots N + M$) will reach the receiver antenna in the combined form $r(t)$:

$$r(t) = \sum_{i=1}^{N+M} \sum_{l=1}^{L_i} \alpha_{i,l} s_i(t - l\tau_{i,l}) + \eta_i(t) \tag{16}$$

where $\eta_i(t)$ is the additive noise corresponding to the i-th channel. Typically, $\eta_i(t)$ is modelled as the Gaussian noise of a zero mean and σ_i^2 variance, and the overall channel variance $\sum_{i=1}^{N+M} \sigma_i^2$, as well as the transmitted signal power, which will determine the carrier-to-noise ratio (CNR) at the receiver. The impact of the channel effects on the RFF have been reported as either insignificant or as negative in the literature so far, meaning that the transmitter features were either found to be invariant to the type of channel (static versus fading, multipath versus single path, etc.) [53,54] or to adversely affect the transmitter features, by smoothing them out [55]. However, very few studies, to the best of our knowledge, addressed the impact of channel impairments on the RFF, and to date, all have been performed in a non-GNSS context. For example, the studies on [53] were done for WiFi signals, the studies in [54] were for Zigbee signals, and the studies in [55] were for 3G cellular signals. Therefore, more simulation-based and measurement-based experiments are needed in order to fully understand the channel effects on RFF in GNSS and this remains one interesting research challenge.

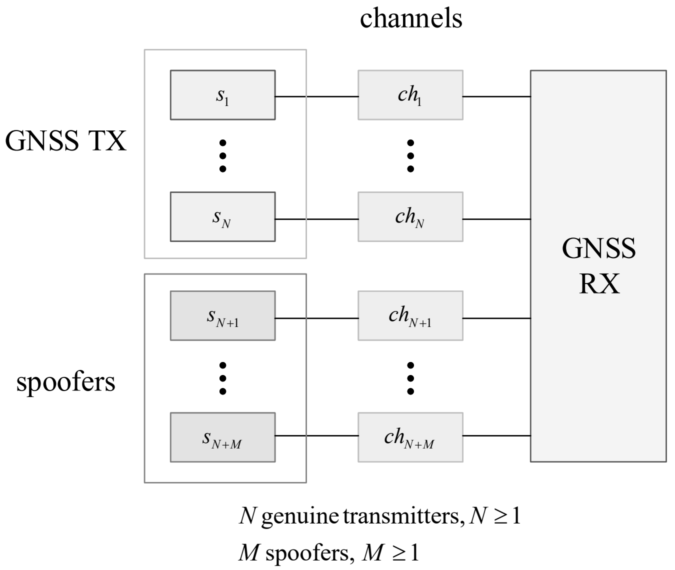


Figure 8. The illustration of the EVM principle. The blue arrow denotes the transmitted symbol, the yellow arrow denotes the received symbol, the blue arrow denotes the estimate, and the crimson arrow denotes the estimation error.

Furthermore, the receiver from Figure 8 also has its own HW elements such as front-end filtering, analog-to-digital (ADC) conversion, local oscillators, and power amplification, and each of these elements will act as additional distortions to the individual transmitter features, as they will be common to all signals $s_i(t)$ found in the received signal $r(t)$ (see Equation (16)). As shown in [3], the same GNSS data from GNSS satellites collected with two different antennas give different fingerprints. This means that, in order to be able to fully identify a GNSS transmitter, one should be able to remove the receiver front-end features from the analysis. For example, one could try to model the behaviour of a certain type of receiver (e.g., USRP, commercial GNSS receiver) and a certain antenna type (e.g., Talysman, Zenith, etc.) and try to compensate the fingerprint it produces via some equalization-like functions. No such models exist in the current literature, according to the best of our searches, and this also remains a topic of open investigation. Moreover, the impact of the receiver sampling rate on RFF accuracy remains to be addressed in the GNSS context. Some studies of the effect of quantization and sampling rates on RFF in the context of non-GNSS signals can be found in [56] (for WiFi signals) and [57] (for BLE signals) and the current understanding is that, typically, higher sampling rates give better RFF accuracy. Such findings are still to be confirmed in the GNSS context.

5. RF Feature Extractors

Section 3 gave an overview of the main RF features that a wireless transmitter can have. The question addressed in this section is how to identify such features, or, more precisely, what feature-extraction transforms $\mathcal{T}(\cdot)$ are available from the literature.

5.1. Error Vector Magnitude (EVM)

The error vector magnitude is a time-domain transform that measures how far the estimated symbols at the receiver side may deviate from the true symbols. I/Q imbalance, thermal noise, in- and out-of-band leakage, and phase noise are all causes that can degrade the EVM metric, thus EVM has the potential to be a good feature-extractor transform to capture hardware impairments from the received signals.

In general, EVM is applied in the context of demodulated signals, as follows: let us assume that a symbol $\mathbf{x}$ is transmitted, and that at the receiver, a symbol $\mathbf{y}$ is received. The receiver estimates (e.g., via decoding process) the symbol $\hat{\mathbf{x}}$. Therefore, the estimation error $\boldsymbol{\epsilon}$ is: $\boldsymbol{\epsilon} = \mathbf{x} - \hat{\mathbf{x}}$, as depicted in Figure 9. The EVM of the symbol $\mathbf{x}$ is defined as

$$\mathrm{EVM}_{\mathbf{x}} \triangleq \frac{\|\boldsymbol{\epsilon}\|_2}{\|\mathbf{x}\|_2} \tag{17}$$

where $\|\cdot\|_2$ is the Euclidian norm.

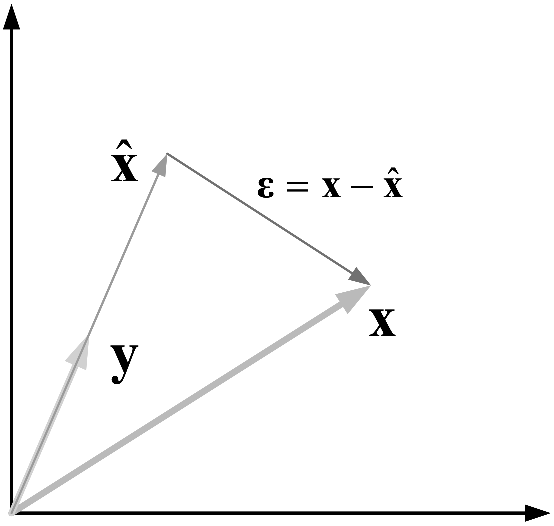
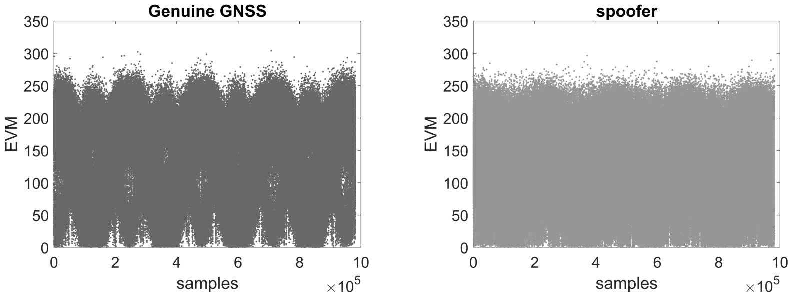


Figure 9. The illustration of EVM principle. The blue arrow denotes the transmitted symbol, the yellow arrow denotes the received symbol, the blue arrow denotes the estimate, and the crimson arrow denotes the estimation error.

When the input to the EVM transform is the I/Q sampled data, one can apply the EVM as follows: $\mathbf{x}$ is a complex-valued sequence of an ideal GNSS signal (i.e., without any distortions); it can be generated, for example, via a GNSS signal generator; $\hat{\mathbf{x}}$ is the received signal (genuine or spoofer) at the I/Q level. Then, the EVM based on pre-correlation data measures the discrepancy between an ideal GNSS signal and the received signal. Under the hypothesis that the spoofer transmitter non-idealities will be further away from the ideal case **x** than the GNSS transmitter non-idealities, then the EVM of a genuine GNSS signal is expected to be smaller than the EVM of a spoofer.

Figure 10a,b show two illustrative examples of EVM outputs for genuine GNSS transmitter and spoofer, respectively (both using Galileo E1 signal specifications and based on a software simulator built by us). The EVM results for the genuine Galileo E1 transmitter and spoofer have visible differences, with EVM values for the spoofer being, on average, slightly higher than those for the Galileo signal, as predicted by the theory. The examples in Figure 10a,b are based on a very high CNR of 100 dB–Hz, for illustrative purposes. At lower CNRs, such differences are no longer visible to the naked eye, but they still have some potential to be captured by a machine learning algorithm, for example.



(**a**) EVM of genuine Galileo E1 transmitter.

(**b**) EVM of spoofer transmitter.

Figure 10. Illustrative example of EVM applied on pre-correlation data, in the absence of channel and receiver effects.

5.2. Kurtosis

Kurtosis is a measure of the Gaussian behaviour of a random variable and it is defined as

$$\mathcal{T}_{kurtosis}(r(n)) = \mathbf{E}\left(\left(\frac{r(n) - \mathbf{E}(r(n))}{std(r(n))}\right)^4\right) \tag{18}$$

where $r(n)$ is the complex sampled signal (sampled at sampling times nT_s, with $T_s = 1/f_s$ being the sampling interval, and f_s the sampling frequency); $\mathbf{E}(\cdot)$ is the expectation operator, and $std()$ is the standard deviation operator. For Gaussian-distributed sequences $r(n)$, $\mathcal{T}_{kurtosis}(r(n))$ is close to level 3. For non-Gaussian distributed sequences, this value is higher or larger than 3. Kurtosis was one of the feature extractors selected in our simulations.

An example of a histogram for the kurtosis results of genuine GNSS transmitter and spoofer is shown in Figure 11. The magenta line represents the threshold to differentiate the spoofer from a genuine GNSS transmitter. It is typically expected that the received GNSS signals in the pre-correlation domain are Gaussian (see blue histogram from Figure 11), due to the fact that the pre-correlation data are dominated by the thermal noise. In the presence of a strong spoofer, this Gaussian property may be lost, due to the fact that spoofer power might become the dominant one.

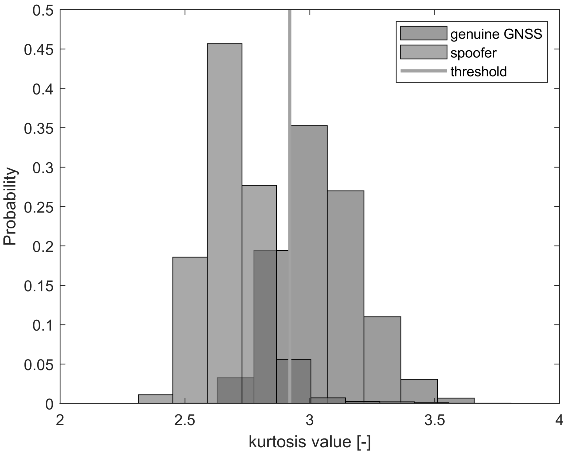


Figure 11. Example of the Galileo E1 and spoofer histograms when kurtosis is applied as a feature extractor.

5.3. Teager–Kaiser Energy Operator (TKEO)

The Teager–Kaiser energy operator (TKEO) is a transform which can estimate the instantaneous energy of a signal, and thus may uncover features that are distinguishable in power or energy. The TKEO transform $\mathcal{T}_{TKEO}$ of a complex signal $r(n)$ is defined as [58]

$$\mathcal{T}_{TKEO}(n) = |r(n)|^2 - \frac{1}{2}\Big(r^*(n+1)r(n-1) + r(n+1)r^*(n-1)\Big) \tag{19}$$

where $r(n)$ is the complex sampled signal and $r^*(n)$ is the conjugate of $r(n)$.

TKEO has been previously used in the context of RFF in GNSS in [3] with promising results. It is also one of the feature extractors selected in our study.

5.4. I/Q Data Spectrograms and Other Short-Time-Short-Frequency (STSF) Transforms

The short-time Fourier transform (STFT) $\mathcal{T}_{STFT}$ is simply a Fourier transform within a window (i.e., short time); and the discrete STFT over a window of N_w samples of the received signal $r(\cdot)$ is given by

$$\mathcal{T}_{STFT}(f,m) = \sum_{n=1}^{N_w} r(n)w(n-m)e^{-j2\pi fn} \tag{20}$$

where m is the time sample index, the $r(n)$ is the complex sampled signal, containing the I and Q components ($r(n) = I(n) + jQ(n)$), f is the frequency, and $w(\cdot)$ is a time window (e.g., Hamming, Hannig, etc.). The spectrogram $\mathcal{T}_{Spectrogram}$ is squared absolute value of the STFT transform, namely:

$$\mathcal{T}_{Spectrogram}(f,m) = |\mathcal{T}_{STFT}(f,m)|^2 \tag{21}$$

Clearly, $\mathcal{T}_{Spectrogram}(f,m)$ and $\mathcal{T}_{STFT}$ are two-dimensional frequency-time transforms and can be stored both as a matrix and in image form. We investigated both approaches and found that by storing the spectrogram into an image form, we obtained more accurate results than by operating with the matricial form.

Figure 12 shows the comparisons of spectrogram-based results between a genuine Galileo E1 transmitter and a spoofer also based on Galileo E1 signal characteristics. The results are based on our in-house Matlab-based simulator, based on the block diagrams in Figure 7a,b and at a very high carrier-to-noise (CNR) ratio of 100 dB–Hz, in order to be able to also identify (for illustration purposes) the different HW features by the naked eye. The results are shown in the absence of channel and receiver effects. It can be seen in Figures 7a,b that there exist visible differences between these two images, e.g., the spectrogram of spoofer I/Q data has one extra line on the upper half of the image compared to the spectrogram of the genuine Galileo I/Q data. The underlying models of the HW features used in our simulator for the genuine and spoofer transmitters were based on the assumptions that phase noises and I/Q imbalances were weaker for a genuine signal than from the spoofer signal. The PA non-linearity models were based on [59], by picking two different PA non-linearity models from there to characterize the spoofer and the genuine GNSS transmitter.

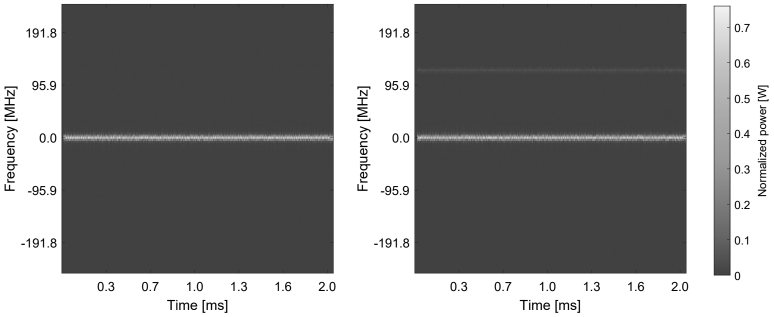


Figure 12. An example of spectrogram-based feature extraction. The left-hand figure is a spectrogram of genuine GNSS (Galileo E1) transmitter, the right-hand figure is a spectrogram of spoofer (Galileo E1) transmitter.

5.5. Wavelet Transforms

A wavelet transform decomposes an incoming signal into some 'coarse' and 'fine' coefficients, based on shifted and scaled versions of a so-called 'mother wavelet' function. Unlike the Fourier transform that cannot offer compact support in both the time and frequency domains, a wavelet transform can offer a compact/bounded support in both tome- and wavelet-domains. Wavelet transforms have been extensively used in watermarking and image-processing applications, and have been reported to be able to identify 'hidden' features; thus, they look like relevant feature extractors for RF fingerprints. Wavelet transforms, in the context of RF fingerprinting, have been previously used, for example in [25,60,61]. The work in [25,60] was only focusing on narrowband signals, in contrast to GNSS. The work in [61] used GNSS simulation-based signals, but only focused on a few simplified transmitter HW impairments. While the work in [61] showed some limited promising results with the discrete wavelet transforms in the context of RFF, our further investigations with more realistic transmitter models as described in Sections 3 and 4 did not show any improvement by using a wavelet transform instead of a spectrogram. Wavelet transforms have an increased complexity compared to other feature-extraction transforms because they output two pairs of complex coefficients (the coarse and fine-approximation coefficients); by distinction, for example, the spectrogram only has one complex output sequence.

6. RF Feature Classifiers

Feature classification methods can be typically split into two main classes: (i) methods based on thresholding or the direct sorting of the outputs of the feature extraction stage; and (ii) methods based on machine learning (ML) classifiers. The second category was by far the category most encountered in RF fingerprinting, as shown previously in Table 1.

Table 1. Overview of state-of-the-art: RFF-related studies based on pre-correlation data, for wireless communications, and navigation applications.

Ref., Year	Studied Signal Types	Studied Algorithms	Detection Performance Metrics Given?	Using I/Q (or Pre-Correlation Data)?	Domain
[62], 2003	Bluetooth and WiFi	Bayesian step detector of transients	No	Yes	IoT
[63], 2006	Ethernet devices	Matched filtering	No	No	Cable networks
[60], 2007	Chipcon sensors at 433 MHz carrier	DWT	No	Yes	IoT
[64], 2008	WiFi	Support vector machines (SVM) and CNN	No	Yes	IoT
[65], 2009	QPSK and DQPSK modulated narrowband signals	Maximum likelihood classification	No	Yes	IoT
[22], 2010	WiFi and 4G/LTE	Analysis of variance (ANOVA) classification	No	Yes	Cellular
[66], 2012	TDMA satellites with QPSK modulation	SDA	No	Yes	Satcomm
[48], 2014	16-APSK modulated narrowband signal	Analytical study	No	No	IoT
[67], 2015	UWB noise radar	MDA	Yes	No	Radar
[68], 2003	**GNSS**	Allan deviation and time interval error	Yes	No	GNSS
[24], 2017	nRF24LU1+ IoT devices at 2.4 GHz	Permutation entropy (PE) and dispersion entropy (DE) with SVM	Yes	Yes	IoT
[69], 2017	GMSK-modulated narrowband signals	Normalized PE	No	Yes	IoT
[21], 2017	**GNSS**	Allan deviation and time interval error	Yes	No	GNSS
[56], 2017	WiFi	Probabilistic neural network (PNN) classifier	No	Yes	IoT
[70], 2018	**GNSS**	Polarization vector with dual antennas	No	No	GNSS
[71,72], 2019	Cellular signals	Kurtosis	No	Yes	Cellular
[25], 2019	GSM	Continuous wavelet transform (CWT) and CNN	Yes	Yes	Cellular
[73], 2019	IoT amplifiers	Linear discriminant analysis (LDA)	Yes	Yes	IoT

Table 1. *Cont.*

Ref., Year	Studied Signal Types	Studied Algorithms	Detection Performance Metrics Given?	Using I/Q (or Pre-Correlation Data)?	Domain
[74], 2019	AM-modulated signal	CNN	Yes	Yes	IoT
[75], 2019	QPSK-modulated narrowband signals	Hilbert–Huang Transform (HHT) and CNN	Yes	Yes	IoT
[76,77], 2020	ADS-B signals	CNN	Yes	Yes	Aviation (surveillance)
[78], 2020	UAV controller	SVM, random forest, neural networks	Yes	Yes	Aviation (UAVs)
[79], 2020	ADS-B signals	CNN, message structure aided attentional convolution network (MSACN)	Yes	Yes	Aviation (surveillance)
[80], 2020	Wimax transmitters	SVM	Yes	Yes	IoT
[81], 2020	UAV transmitters	Neural networks	Yes	Yes	Aviation (UAVs)
[82], 2021	ZigBee signals	Gaussian probabilistic LDA	Yes	Yes	IoT

6.1. Threshold-Based Classification

The threshold-based classification is also known as a traditional hypothesis testing and can be implemented through well-known algorithms such as likelihood ratio testing (LRT) or Gaussian likelihood ratio testing (GLRT) [83,84]. The traditional hypothesis testing problem is a problem of distinguishing between two hypotheses, namely $\mathcal{H}_0$ and $\mathcal{H}_1$:

$$\begin{cases} \mathcal{H}_0 & \text{spoofer is absent} \\ \mathcal{H}_1 & \text{spoofer is present} \end{cases} \tag{22}$$

If the feature-extraction transform outputs scalar or vector values (instead of N-dimensional matrices with $N \geq 2$), a classification can be envisaged via a simple threshold, for example, by comparing the scalar value or the vector statistics (mean, minimum, maximum, median, etc.) to a certain pre-defined threshold. If the data are in N-dimensional form, then LRT/GLRT methods with Gaussian multivariate modelling can be employed.

The challenging part in this approach is choosing a suitable threshold, when no a priori knowledge about the genuine and spoofing signals is available. Such a threshold can be determined based on theoretical assumptions (e.g., kurtosis transform is known to be close to 3 for Gaussian-distributed variables) or by using an initial training base with genuine and spoofing signals and derive a threshold based on the training database. Another challenge in this threshold-based approach is that most of the transmitter features are 'hidden' and not distinguishable through classical hypothesis testing, as the probability distribution functions of $\mathcal{H}_0$ and $\mathcal{H}_1$ hypotheses from Equation (22) would overlap.

In our work, we used the optimal false alarm rate from ML-based classification to calculate the detection rate. By comparing this detection rate with the optimal one from ML-based classification, we evaluate the performance of the threshold-based method.

6.2. ML-Based Classification

Machine learning (ML) methods have been widely used in the literature as methods of classification in RF fingerprinting approaches or for transmitter identification and authentication (see the references from Table 1). Typically, three main classes of ML approaches are encountered, namely: unsupervised learning (k-means, fuzzy k-means, etc), supervised learning (e.g., kNN, SVM, random forest, gradient boosting, etc.), and reinforcement learning (e.g., Markov decision processes, etc.). In addition, deep learning methods, such as CNN, can be applied typically both in a supervised or unsupervised manner. The fact that the data are not annotated or labelled in unsupervised approaches makes the unsupervised approaches less useful than the supervised ones in the context of RFF, where one would like to have the exact labels of the genuine transmitters. Moreover, reinforcement learning methods are typically rather complex and rely on harnessing additional data from the environment. They have not been studied yet in the context of RFF for GNSS to the best of the authors' knowledge and are highly unlikely to work with GNSS pre-correlation data as their complexity combined with the huge amount of pre-correlation data to be processed will be prohibitive. A recent, not yet peer-reviewed work on reinforcement learning (i.e., a policy gradient method) with RFF for an ADALM-PLUTO software defined radio (SDR) can be found in [85], but the focus in there was to apply reinforcement learning to enhance the spoofer capabilities in the context of a quadrature phase shift keying (QPSK) communication systems, not to identify the spoofer. For these reasons, only the supervised and deep learning approaches have been investigated to date in the context of RFF and these are also the ones we will briefly describe in the next sub-sections.

6.2.1. kNN Classifier

The kNN classifier is the most used classifier from the class of unsupervised ML approaches. The principals behind it are simple: for every sample, it will look at the k nearest neighbours, and the class of this sample will be determined by the class of the majority in the nearest neighbours. Figure 13 presents an example when the nearest neighbours are three: the three nearest neighbours of a testing yellow dot are two red dots and one blue dot, and as a result, the yellow dot is determined as a red class.

Figure 14a,b demonstrate the impact of a different number of nearest neighbours on the boundary of two classes (a spoofer and a Galileo E1 signal). A large number of nearest neighbours may lead to an over-fitting problem while an insufficient number of nearest neighbours degrades the classification performance.

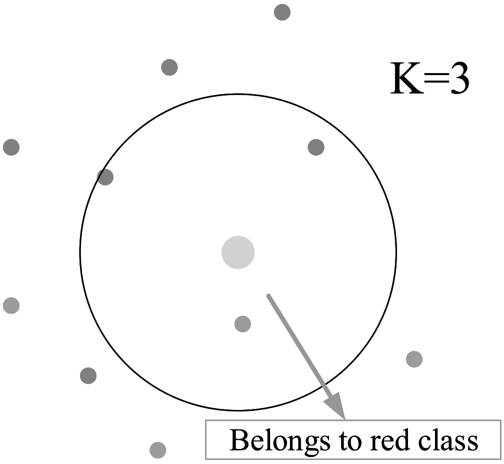
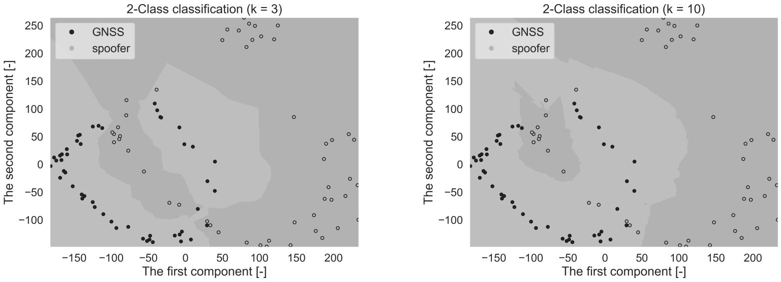


Figure 13. An example of KNN for three nearest neighbours.



(**a**) When nearest neighbours are three. (**b**) When nearest neighbours are 10.

Figure 14. An example based on Galileo E1 and spoofer simulated data: the first two principal components of PCA of spectrogram images are classified by KNN under a different number of nearest neighbours: 3 (**left**) and 10 (**right**).

6.2.2. SVM Classifier

As the problem we address here is a classification problem with two classes: spoofer absent (or $\mathcal{H}_0$ hypothesis) versus spoofer present (or $\mathcal{H}_1$ hypothesis), the most encountered ML classifier for a two-class problem is the support vector machine (SVM), as SVM is designed to maximize the margin between classes in such a two-class case. The SVM classifier could be versatile by using a kernel trick. Considering 2D points $(\mathbf{x}, \mathbf{y})$, here, we list several popular kernels $k(\mathbf{x}, \mathbf{y})$:

- Linear kernel: $k(\mathbf{x}, \mathbf{y}) = \mathbf{x} \cdot \mathbf{y}$;
- Polynomial kernel: $k(\mathbf{x}, \mathbf{y}) = (\mathbf{x} \cdot \mathbf{y})^d$, d is the exponent;

- Sigmoid kernel: $k(\mathbf{x}, \mathbf{y}) = \tanh a\mathbf{x} \cdot \mathbf{y} + b$, $a > 0$ and $b < 0$;
- Gaussian kernel (also known as an rbf kernel): $k(\mathbf{x}, \mathbf{y}) = e^{\left(-\frac{\|\mathbf{x}-\mathbf{y}\|^2}{2\sigma^2}\right)}$.

Typically, a Gaussian kernel takes best into account the irregular boundary in the I/Q GNSS datasets. As the dimensions of raw I/Q data are typically huge, some forms of dimensionality reduction can be typically employed. One such form is known under the name of **Principal components analysis (PCA)**.

PCA is a common method to pre-process data for the purpose of reducing the dimension of the target dataset before the classifications. The first few principal components implies the most dominant features existing in the dataset, whilst using PCA is an effective way to improve the classification performance.

For example, Figure 15 demonstrates the first 20th components in the spectrogram images of a Galileo E1 and a spoofer (also based on Galileo E1 signal specifications), respectively. The plots are shown for a very high CNR level (100 dB–Hz) for illustration purposes. The PCA levels are clearly distinct in the two plots of Figure 15, pointing out the fact that the various transmitter HW features can indeed differentiate between the transmitter types to some extent by further processing via SVM for example.

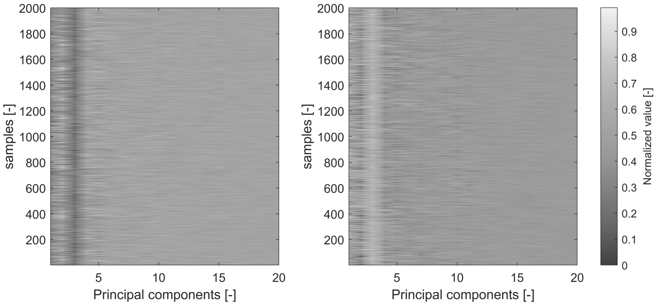


Figure 15. Comparisons between the PCA results in spectrogram images of GNSS (**left**) and spoofer (**right**). The values in the colour bar represent the amplitude levels of the PCA coefficients.

6.2.3. CNN Classifier

Convolutional neural networks (CNN), the most frequently encountered category of deep learning classifiers, have been widely applied in image identification and pattern recognition. Recently, CNN classifier has also started to be considered as a promising method for the radio identification and RFF [86,87]. A general CNN consists of a combination of convolutional layers, pooling layers, and fully connected layers. This works as the following:

1. The convolutional layer applies a convolution operation between the input signal matrix and a filter (or kernel) (the input signals here are the signals that come to the convolutional layer; the input does not necessarily mean the input data to the beginning of neural networks). For example, Figure 16 considers a 5 × 5 'input' and a 3 × 3 filter, the red rectangle selects the same size of data as the filter, then the selected data have a convolution operation with the filter. The red rectangle moves after each convolution operation until all the 'input' data experience the convolution operation with the filter.
2. The pooling layer will reduce the number of parameters; it is essentially a sampling method. The common pooling methods are max pooling, average pooling, and sum pooling. Here, we provide an example of max pooling in Figure 17. Max pooling: it chooses the largest number in the selected data.
3. The fully connected layer is the actual neural network, by using the activation function, such as the sigmoid (or logistic function), we are able to label the outputs. A common fully connected layer is made of three parts, the input layer, the hidden layer(s)

(also refers to neurons), and the output layer. Figure 18 gives an example of a fully connected neural network. The fully connected neural network can be composed of multiple layers of fully connected neurons. Each layer can be followed by an activation function, such as a relu, sigmoid, or logistic function. The output layer, the last layer of the neural network, commonly uses a sigmoid activation function to assign the probability to each possible class. Figure 18 gives an example of a fully connected neural network.

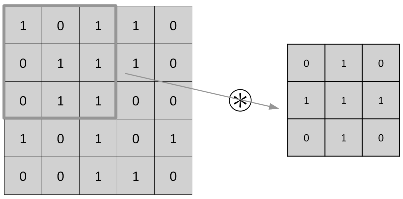


Figure 16. An example of convolutional layer.

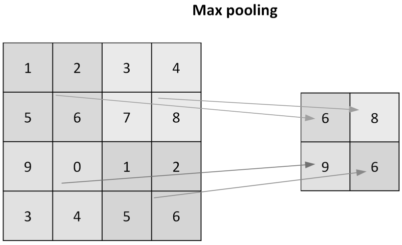


Figure 17. An example of max pooling.

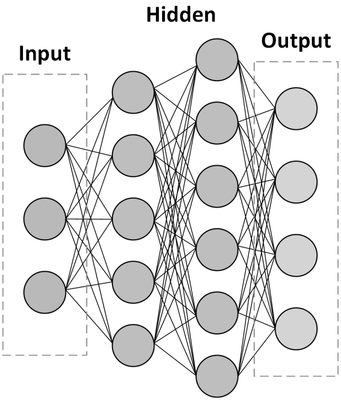


Figure 18. An illustration of a fully connected neural network.

6.2.4. Other Approaches

Other approaches of ML-based classification less encountered in the context of RFF are: linear discriminant analysis (LDA) [73,82], logistic regression (LR) [88], and random forest [89].

LDA is usually used to separate two or more classes or to achieve dimensionality reduction. The basic idea behind LDA is to find a projection of the input data such that the separation of classes could be maximized. This method is limited, however, by the condition that both input classes follow normal distributions. LR usually works with classes characterized by linear features and it is not well suited to non-linear features as those created by power amplifiers and digital-to-analog converters. The studies in [88], applied in the non-GNSS context, also showed that the SVM outperforms LR. The random forest algorithm is one kind of decision tree used in the classifications, which implements the 'if-then-else' logic in order to classify samples. The random forest algorithms are more complex than simple decision-tree algorithms and their complexity is prohibitive complexity for GNSS pre-correlation samples.

7. Simulation-Based Example and Feature Down Selection

An in-house-based simulator was built based on Matlab 2020b version and Python 3.7.5. The Matlab modules were used to generate I/Q samples based on a GNSS and a spoofer model, each having five types of transmitter features: PA non-linearities, DAC non-linearities, I/Q imbalance, phase noises, and BPF. The parameters of genuine GNSS transmitters are typically not available in open access, as they are protected via IPR. In the absence of such GNSS exact parameters for these HW features, we adopted various models from the literature. For example, the PA non-linearities were modelled according to [59], and the phase noise existing in the clock unit and up-conversion unit was modelled according to [90]. Details on the parameters used in our simulator are given in Table 2. In order to mimic the characteristics of a sophisticated spoofer, the phase noise of the local oscillator in the spoofer was modelled according to [52], a high-end software-defined radio designed for GNSS signal transmitting and receiving. A simplified model was used for classifying one genuine GNSS transmitter versus one spoofer transmitting GNSS-like signals. As the main goal was to study the feasibility of RFF in the context of GNSS, an ideal, almost noise-free case was considered with a carrier-to-noise ratio (CNR) $C/N_0 = 100$ dBHz. While the noise-free approach is not realistic in real-life scenarios, the purpose here was to show if there is any potential of RFF with pre-correlation GNSS data and to identify which HW features are likely to best differentiate between different transmitters.

A two-millisecond observation window of Galileo E1 band signals was used in the examples shown in this section. In order to deal better with smaller C/N_0 levels that the ideal case considered here, one could consider the increase in the observation window. However, the simulation times and the complexity of RFF processing would also increase. Under a different randomness seed, we generated 2000 matrices (or images) of genuine GNSS signals and spoofer signals, respectively (thus a total of 4000 inputs to the ML algorithm). Furthermore, the 4000 data inputs were randomly split into 80% of training data and 20% of test data. Such matrices (or images) were the outputs of three considered feature-extraction transforms, namely applied kurtosis, TKEO and spectrogram, applied on the 2 ms observation interval of the raw signal sampled at a very high sampling rate of 491 MHz. Such a high sampling rate was needed in our model because we adopted a quasi-RF model, in order to model the clocks' non-idealities. The feature-extraction transforms were selected based on the discussions in Section 5, in order to enhance the capability of differentiating genuine GNSS signals from spoofer signals. An SVM classifier, from the scikit-learn library, together with a radial-basis-function kernel was implemented in Python to perform the classification. The grid search method was used to provide the optimized classification results and 100-fold cross-validation on the training dataset were employed to guarantee the convergence of the results.

The results of the classification are presented via the confusion-matrix metric. Figure 19 illustrates the definition of the confusion matrix used in our work.

In our simulator, each feature can be active or inactive, making the simulator flexible to be able to down select or identify the 'strongest' features, as well as their overall impact when they act jointly (as in a realistic transmission scenario). Figure 20 shows the confusion-matrix results, first when all features are combined, and then feature-by-feature, in order to be able to identify which features have a strong impact on RFF and which a have weak or no impact. One very interesting result based on Figure 20 is that, even at a 100 dB–Hz carrier-to-noise ratio, both the phase-noise and DAC-non-linearity features fail to provide differences between the two classes (spoofer present versus genuine Galileo signal present).

Moreover, as seen in Figure 20, the band-pass filter effects can only provide moderate differentiation between the spoofer and GNSS. These results, at a large degree, imply that the phase noise and DAC non-linearity are 'weak' features in the GNSS RFF context, while PA and I/Q imbalance, as well as BPF to some extent, are 'strong' features. This is also qualitatively illustrated in the next section.

Table 2. Parameters in simulation.

Parameters	**Value**	
Observation interval (ms)	2	
Galileo band	E1	
Intermediate frequency (MHz)	61.38	
Maximum Doppler shift (kHz)	5	
TX filter bandwidth (MHz)	100	
Parameters Used in Genuine GNSS Simulator		
DAC phase noise	Frequency offset (Hz)	Level (dBc/Hz)
	1	−90
DAC non-linearity	$y = x - 0.0038x\|x\|^2$	
Clock unit phase noise	Frequency offset (Hz)	Level (dBc/Hz)
	1	−95
	10	−125
	100	−135
Clock unit non-linearity	Ignored	
Up-conversion unit phase noise	Frequency offset (Hz)	Level (dBc/Hz)
	1	−50
	10	−70
	100	−95
Up-conversion unit I/Q imbalance	Amplitude (dB)	Degree
	1	3
Band-pass filter	See Figure 6a	
Parameters Used in Spoofer Simulator		
DAC phase noise	Frequency offset (Hz)	Level (dBc/Hz)
	10	−50
	100	−70
	500	−85
DAC non-linearity	$y = x - 0.05x\|x\|^2$	
LO phase noise	Frequency offset (Hz)	Level (dBc/Hz)
	1	−80
	10	−110
	100	−135
Mixer I/Q imbalance	Amplitude (dB)	Degree
	3	5
Band-pass filter	See Figure 6b	

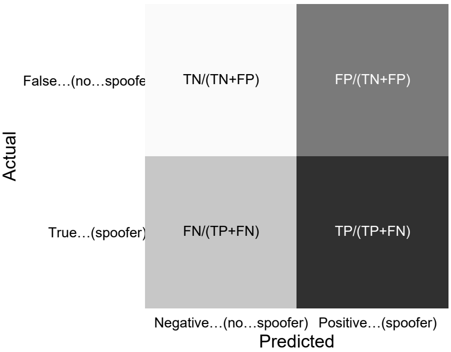
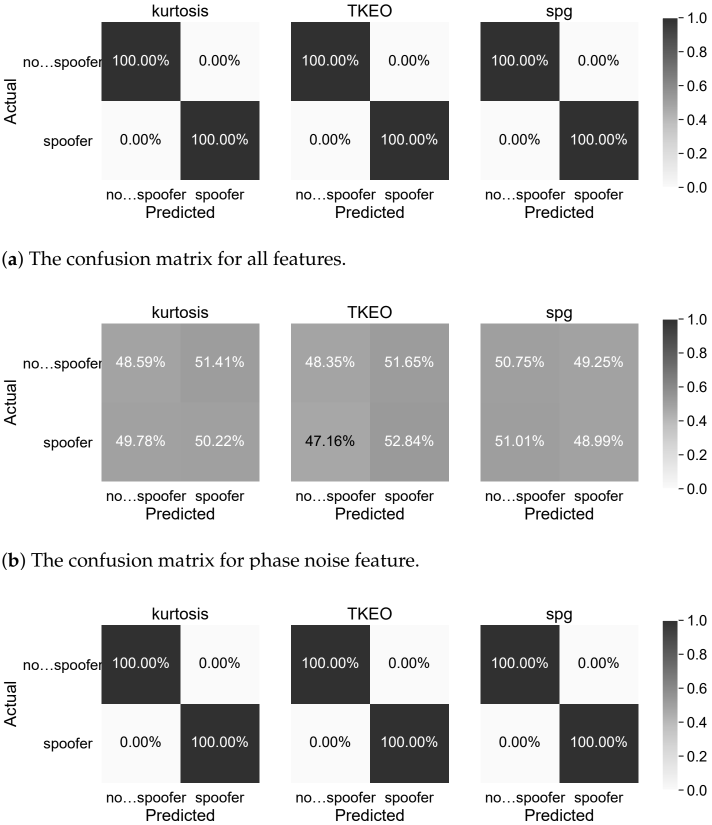


Figure 19. The illustration for normalized confusion matrix. FN is short for false negative rate, FP is short for false positive rate, TN is short for a true negative rate, TP is short for a true positive rate.

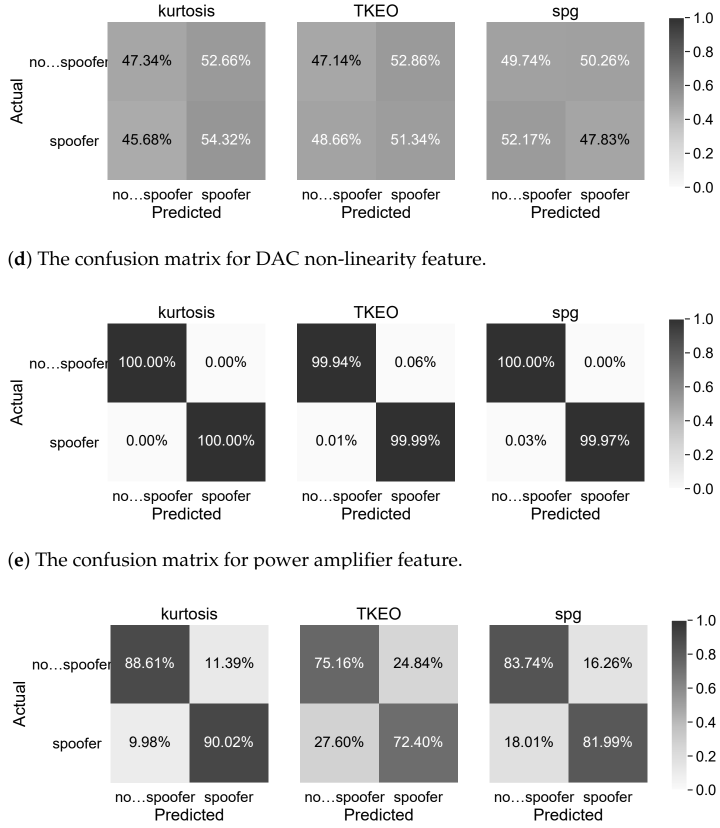


(**a**) The confusion matrix for all features.

(**b**) The confusion matrix for phase noise feature.

(**c**) The confusion matrix for I/Q imbalance feature.

Figure 20. *Count*.



(**d**) The confusion matrix for DAC non-linearity feature.

(**e**) The confusion matrix for power amplifier feature.

(**f**) The confusion matrix for band-pass filter feature.

Figure 20. The confusion matrix of a 1 versus 1 scenario under 100 dB-Hz CNR.

8. Comparative Summary of Pre-Correlation RFF Methods in Existing Literature

Table 1 gives a concise survey of main RFF-related studies in the recent literature, by specifying the wireless system under investigation, as well as the main algorithms used for feature detection and classification in those RFF approaches. As seen in Table 1 most of the research work dedicated to RFF has to date been for non-GNSS signals. Moreover, as clearly seen from the last column in Table 1, RFF in the aviation context has been receiving more and more attention in the last two years, e.g., focusing on automatic dependent surveillance-broadcast (ADS-B) surveillance signals and on UAV transmitters and controllers. Table 1 shows that a wide variety of classifiers have to date been investigated in the literature in the context of RFF: from a discrete wavelet transform (DWT) and continuous wavelet transform (CWT) to various neural networks, such as convolutional neural networks (CNN), probabilistic neural networks (PNN) and other machine learning algorithms, such as support vector machines (SVM), subclass discriminant analysis (SDA), multiple discriminant analysis (MDA), or permutation-entropy (PE)-based approaches.

Unlike the typical narrowband terrestrial signals typically studied to date with RFF techniques (see Table 1), the GNSS signals are wideband and continuously transmitted, and hence do not exhibit strong transients to be used as differentiating factors. This means that, for GNSS signals, one should go deeper into the transmitter hardware characteristics and detect the possibly differentiating features between spoofers and genuine GNSS transmitters.

9. Qualitative Discussion and Open Challenges

Based on our literature research and the preliminary theoretical analysis, Table 3 shows a suitability analysis of various combinations of feature-extraction transforms and classifiers for four selected classifiers and five selected feature-extraction transforms. The suitability analysis took into account both the expected performance and the complexity of the algorithm.

Table 3. Preliminary analysis on the suitability of various feature-extraction transforms for various classification methods (+ = low , ++ = medium, +++ = high) in the context of pre-correlation GNSS data.

Classifier Type	Feature Extraction Transform					
	EVM	Kurtosis	TKEO	Spectrogram	CWT	DWT
Classification via kNN	+	+	+	+	+	+
Classification via SVM	+	++	+	+++	+	++
Classification via CNN	+	+	+	+++	+	+
Classification via Thresholding	+	+++	+	+	+	+

The most promising combinations, based on our preliminary analysis, are the kurtosis and thresholding combination, and the spectrogram and SVM combination. Potential good results may also be expected, based on a current literature search and theoretical analysis, from kurtosis and SVM combination, as shown in Table 3. Further simulation-based and measurement-based analysis is necessary to validate these findings and this remains a topic of future research. The methodology presented in this paper can serve as a basis for also studying other possible combinations of feature-extraction transforms and classifiers.

Table 4 also discusses the expected impact of various features of the transmitter HW on the accuracy of the results. The analysis is based on the theoretical insights from the mathematical models presented in Section 3. It is expected that the PA non-linearity, the phase noises and the I/Q imbalances are the strongest differentiating features of the transmitter HW impairments, while the DAC non-linearities are expected to have little or no impact upon the classification performance (as differences between the GNSS and spoofer DAC non-linearities are not expected to be high). The band-pass filter (BPF) at the end of the transmission chain is, however, expected to have a negative impact upon the ability to differentiate among various features, because it is acting as a smoother (or high-frequency removing unit). In practice, an RFF algorithm would, most likely, not be able to distinguish between each individual transmitter feature and would treat all effects jointly. Based on sufficiently large databases, it is expected that the positive-impact effects from Table 4 will be predominant compared to the zero- and negative-impact effects.

Table 4. Preliminary analysis on the impact of various hardware features upon the capacity to distinguish between transmitters, based on Section 7: 0 = no impact, + = positive impact (i.e., can increase the RFF accuracy).

	Transmitter Features				
	Phase Noise	I/Q Imbalance	DAC Non-Linearity	PA Non-Linearity	BPF
Impact	0	+	0	+	+

10. Conclusions and Roadmap Ahead

This paper presented a survey of RFF methods for spoofing mitigation in GNSS receivers. While the survey of methods and the methodology presented in here can be generally applied also in a non-GNSS context, the focus in our paper has been on GNSS pre-correlation data, as the pre-correlation anti-spoofing methods are still rare in the current literature.

A four-step methodological approach has been proposed in Section 2, by breaking down the RFF problem into several parts: the effects (or features) occurring at the transmitter side, the channel effects, and the receiver effects. We identified the main sources of possible hardware imperfections (i.e., features) at the transmitter side and we introduced in Section 3 detailed mathematical models for the identified HW impairments for GNSS transmitters. It has also been shown that such HW features are best identified with the help of various feature-extraction time-domain or frequency-domain transforms. Some of the most encountered feature-extraction transforms in the current literature were discussed in Section 5. We also surveyed the literature to identify classification algorithms useful in the context of RFF. Several classification methods, both via thresholding and via machine learning algorithms, were addressed in Section 6. Section 8 provided a qualitative comparison of approaches suitable for GNSS pre-correlation data, based on our literature survey, theoretical modelling, and preliminary simulation-based observations. It is to be emphasized that such RFF algorithms need to be further tested via measurement-based data for understanding their full capacity in a realistic environment, but one of the main take-away points of our research has been that the transmitter HW imperfections do have the possibility to act as differentiating features between spoofers and genuine transmitters if proper combinations of feature-extraction transform and classifiers are found. Our focus has been on the transmitter HW features, but we also discussed the possible effects of the wireless channels and the hardware blocks at the receiver side. To sum up, several challenges remain for the roadmap ahead:

- Addressing the impact of the signal mixtures from signals from various satellites and various frequency bands: typically, the received signal is a mixture of all satellites visible in the sky at the considered moment, and possibly, of one or several spoofing signals. One approach to look at a single signal at a time would be to first despread each signal from each identified pseudo-random code, and then apply successive or parallel interference cancellation methods to identify each signal, one by one. The errors in the estimation of the signals from various satellites would, of course, affect the quality of the re-constructed signal, and possibly, the accuracy of the RFF-based classification. Another approach would be to create huge training databases with all possible mixtures of satellites in the sky and to use those databases in the classification process;
- Evaluating and mitigating the impact of channel multipath and fading effects: each wireless channel (from satellite or spoofer) has its own random signature, determined by the multipath delays, Doppler spreads, and fading effects. As these effects are random in nature, they will, most likely, not provide additional 'features', but will have a negative impact on the strength of the transmitter features. The effect of the wireless channels upon the RFF algorithms can be further investigated via simulation- or measurement-based approaches and it remains a topic of future investigation;
- Understanding the impact of the receiver HW features upon the RFF methods: while the same receiver is capturing either genuine GNSS signals or a mixture of genuine signals and spoofer(s), and thus the same receiver effects are present in both situations (spoofer present or spoofer absent), the receiver also has local oscillators, ADC and filter blocks, etc., and each of them can introduce additional phase noises, non-linearities and I/Q imbalances. Intuitively, such effects will have a negative impact upon the classification accuracy compared to an ideal receiver (without any HW imperfections), but such effects need to be further analysed based on measurements or simulated data.

- Dealing with the negative impact of high noise levels on RFF performance, especially when dealing with low-power signals such as those in the pre-correlation domain: GNSS signals in urban scenarios, such as GNSS receivers on-board of drones flying through tall buildings, can be received at relatively low CNRs, and these low CNRs are likely to act as smoothers of the transmitter features, to the point of fading them out. It remains an open research question what the CNR threshold is above which the RFF methods with pre-correlation GNSS samples are likely to work;
- Validating through real-field measurements the promising RFF performance for authenticating GNSS signals.

One of the main contributions of our paper was presenting a step-by-step methodological approach proposed to be adopted for a designer wishing to build an RFF algorithm in a GNSS receiver. The identified transmitter HW features are likely to be reflected not only in the pre-correlation data (illustrated in our examples through the paper), but also in the post-correlation and navigation domains, thus our four-step methodology also paves the road towards more advanced RFF GNSS processing in all three domains (pre-correlation, post-correlation, and navigation), with a future aim to offer robust and hybrid anti-spoofing solutions. An additional contribution of this paper has been to present an ample survey of existing RFF methods in the literature used with both GNSS and non-GNSS signals and already showing promising results. As described in this last section, several challenges are still to be overcome towards the success of RFF methods, especially when relying on the low-power GNSS I/Q raw data. It is our belief that this survey bridges the missing gap between the RFF studies in the non-GNSS context and the anti-spoofing methods studied to date only at the post-correlation and navigation levels in the GNSS context. It is our intent that this paper sheds new light on how to approach an RF fingerprinting process to identify hidden transmitter features, by first decomposing the problem into the relevant transmitter features and then by selecting the most suitable pair of feature-extraction transform and classifier algorithm in order to classify the transmitters according to their features or HW impairments. While many challenges still remain in the RFF GNSS research field, it is also the authors' belief, based on our understanding of the research problem, that by combining various authentication methods, at different levels (pre-correlation, post-correlation, and navigation levels), one is more likely to obtain good results than by using a single authentication method. The simulation-based results presented here are only for some selected illustrative parameters and are useful in the context of down selecting the most important HW features of a GNSS transmitter. We saw that, even under ideal conditions such as 100 dBHz carrier-to-noise ratio, the phase noise and the DAC nonlinearities are not differentiating features, while P non-linearities, I/Q imbalances, and band-pass filters carry the potential of being good RF 'fingerprints'. For the sake of a reduced complexity of simulations, the observation window used in our simulations was of 2 ms. Further investigative studies at a lower C/N_0 than 100 dBHz should also increase the observation windows, in order to deal better with the high noise level typical in the pre-correlation domains. The equivalent block diagrams and the methodological approach presented here, as well as the initial pre-selection of relevant features and feature extractors can also serve the basis towards further studies in the post-correlation domain, where the noise levels are significantly lower than in the pre-correlation domain, especially for the long post-detection integration times.

Author Contributions: Conceptualization, W.W., I.A.S., G.C., E.S.L.; methodology, W.W., I.A.S., G.C., E.S.L.; software, W.W. and E.S.L.; validation, W.W.; formal analysis, W.W., I.A.S., G.C., A.M., T.W., E.S.L.; investigation, W.W., I.A.S., G.C., A.M., T.W., E.S.L.; resources, W.W., I.A.S., G.C., A.M., T.W., E.S.L.; writing—original draft preparation, W.W. and E.S.L.; writing—review and editing, I.A.S., G.C., A.M., T.W.; visualization, W.W.; supervision, E.S.L.; project administration, I.A.S., T.W., and E.S.L.; funding acquisition, E.S.L. and A.M., T.W. All authors have read and agreed to the published version of the manuscript.

Funding: This research was partly funded by the European Space Agency (ESA) in the project FINESSE ("Fingerprinting GNSS for authentication"). The opinions expressed herein reflect the authors' view only. Under no circumstances shall the ESA be responsible for any use that may be made of the information contained herein. This work was also partly supported by the Academy of Finland, under the project ULTRA (328226, 328214).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

ADC	Analog-to-Digital Converter
AGC	Automatic Gain Control
ANOVA	Analysis of Variance
APSK	Amplitude and Phase Shift Keying (modulation)
BLE	Bluetooth Low Energy
BPF	Band-Pass filter
BPSK	Binary Phase Shift Keying (modulation)
CDMA	Code Division Multiple Access
CNR	Carrier-to-Noise Ratio
CNN	Convolutional Neural Networks
CWT	Continuous Wavelet Transform
DAC	Digital-to-Analog Converter
DE	Dispersion Entropy
DQPSK	Differential Quadrature Phase Shift Keying (modulation)
DWT	Discrete Wavelet Transform
ESA	European Space Agency
ESTEC	European Space Research and Technology Centre
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GLRT	Gaussian Likelihood Ratio Test
FE	Front-End
FIR	Finite Impulse Response
GNSS	Global Navigation Satellite System
GSM	Global System for Mobile Communications
HHT	Hilbert–Huang Transform
HW	Hardware
IoT	Internet of Things
I/Q	In-Phase /Quadrature
LDA	Linear Discriminat Analysis
LPA	Low Power Amplifier
LO	Local Oscilator
LRT	Likelihood Ratio Test
LTE	Long-Term Evoloution
MDA	Multiple Discriminant Analysis
MSACN	Message Structure Aided Attentional Convolution Network
OXCO	Oven Controlled Crystal Oscillator
PA	Power Amplifier
PCA	Principal Component Analysis
PE	Permutation Entropy
PN	Phase Noise

PNN	Probabilistic Neural Networks
PSD	Power Spectral Density
QPSK	Quadrature Phase Shift Keying (modulation)
RF	Radio Frequency
RFF	Radio Frequency Fingerprinting
SDR	Software Defined Radio
SNR	Signal-to-Noise Ratio
SVM	Support Vector Machines
SW	Software
TCXO	Temperature Controlled Crystal Oscillator
TDMA	Time Division Multiple Access
TKEO	Teager–Kaiser Energy Operator
UAV	Unmanned Aerial Vehicles
USRP	Universal Software Radio Peripheral
UWB	Ultra Wide-Band

References

1. Rehman, S.; Sowerby, K.; Alam, S.; Ardekani, I. Radio frequency fingerprinting and its challenges. In Proceedings of the 2014 IEEE Conference on Communications and Network Security, San Francisco, CA, USA, 29–31 October 2014; pp. 496–497.
2. Deng, S.; Huang, Z.; Wang, X.; Huang, G. Radio Frequency Fingerprint Extraction Based on Multidimension Permutation Entropy. *Int. J. Antennas Propag.* **2017**, *2017*, 1538728. [CrossRef]
3. Morales-Ferre, R.; Wang, W.; Sanz-Abia, A.; Lohan, E.S. Identifying GNSS Signals Based on Their Radio Frequency (RF) Features—A Dataset with GNSS Raw Signals Based on Roof Antennas and Spectracom Generator. *Data* **2020**, *5*, 18. [CrossRef]
4. Bassey, J.; Li, X.; Qian, L. Device Authentication Codes based on RF Fingerprinting using Deep Learning. *arXiv* **2020**, arXiv:2004.08742.
5. Wozmca, P.; Kulas, L. Influence of a radio frequency on RF fingerprinting accuracy based on ray tracing simulation. *Eurocon* **2013**, *2013*, 202–206. [CrossRef]
6. Greenberg, E.; Levy, P. Propagation aspects for RF fingerprinting at open areas over irregular terrain. In Proceedings of the 2017 11th European Conference on Antennas and Propagation (EUCAP), Paris, France, 19–24 March 2017; pp. 3529–3533. [CrossRef]
7. Kalayci, A.O.; Akdemİr, E. RF fingerprinting based indoor localization for uncooperative emitters. In Proceedings of the 2018 26th Signal Processing and Communications Applications Conference (SIU), Izmir, Turkey, 2–5 May 2018; pp. 1–4. [CrossRef]
8. Khandker, S.; Torres-Sospedra, J.; Ristaniemi, T. Improving RF Fingerprinting Methods by Means of D2D Communication Protocol. *Electronics* **2019**, *8*, 97. [CrossRef]
9. Rehman, S.U.; Sowerby, K.W.; Coghill, C. Analysis of impersonation attacks on systems using RF fingerprinting and low-end receivers. *J. Comput. Syst. Sci.* **2014**, *80*, 591–601.
10. Thoelert, S.; Steigenberger, P.; Montenbruck, O.; Meurer, M. GPS III Arrived–An Initial Analysis of Signal Payload and Achieved User Performance. In Proceedings of the 32nd International Technical Meeting of the Satellite Division of The Institute of Navigation, Miami, FL, USA, 16–19 September 2019; pp. 1059–1075. [CrossRef]
11. Morales-Ferre, R.; Richter, P.; Falletti, E.; de la Fuente, A.; Lohan, E.S. A Survey on Coping With Intentional Interference in Satellite Navigation for Manned and Unmanned Aircraft. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 249–291. [CrossRef]
12. Rustamov, A.; Gogoi, N.; Minetto, A.; Dovis, F. Assessment of the Vulnerability to Spoofing Attacks of GNSS Receivers Integrated in Consumer Devices. In Proceedings of the 2020 International Conference on Localization and GNSS (ICL-GNSS), Tampere, Finland, 2–4 June 2020; pp. 1–6. [CrossRef]
13. Honkala, S.; Thombre, S.; Kirkko-Jaakkola, M.; Zelle, H.; Veerman, H.; Wallin, A.E.; Dierikx, E.F.; Kaasalainen, S.; Söderholm, S.; Kuusniemi, H. Performance of EGNSS-Based Timing in Various Threat Conditions. *IEEE Trans. Instrum. Meas.* **2020**, *69*, 2287–2299. [CrossRef]
14. Issam, S.M.; Adnane, A.; Madiabdessalam, A. Anti-Jamming techniques for aviation GNSS-based navigation systems: Survey. In Proceedings of the 2020 IEEE 2nd International Conference on Electronics, Control, Optimization and Computer Science (ICECOCS), Kenitra, Morocco, 2–3 December 2020; pp. 1–4. [CrossRef]
15. Nicola, M.; Falco, G.; Ferre, R.M.; Lohan, E.S.; de la Fuente, A.; Falletti, E. Collaborative Solutions for Interference Management in GNSS-Based Aircraft Navigation. *Sensors* **2020**, *20*, 4085. [CrossRef]
16. Caparra, G. Authentication and Integrity Protection at Data and Physical Layer for Critical Infrastructures. 2017. Available online: paduaresearch.cab.unipd.it/9797/1/tesi_Gianluca_Caparra.pdf (accessed on 24 April 2021).
17. Caparra, G.; Ceccato, S.; Laurenti, N.; Cramer, J. Feasibility and Limitations of Self-Spoofing Attacks on GNSS Signals with Message Authentication. In Proceedings of the 30th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+), Portland, OR, USA, 25–29 September 2017; pp. 3968–3984.
18. Wu, Z.; Zhang, Y.; Yang, Y.; Liang, C.; Liu, R. Spoofing and Anti-Spoofing Technologies of Global Navigation Satellite System: A Survey. *IEEE Access* **2020**, *8*, 165444–165496. [CrossRef]

19. Psiaki, M.L.; Humphreys, T.E. GNSS Spoofing and Detection. *Proc. IEEE* **2016**, *104*, 1258–1270. [CrossRef]
20. Schmidt, D.; Radke, K.; Camtepe, S.; Foo, E.; Ren, M. A Survey and Analysis of the GNSS Spoofing Threat and Countermeasures. *ACM Comput. Surv.* **2016**, *48*, 1–31. [CrossRef]
21. Borio, D.; Gioia, C.; Canopons, E.; Baldini, G. Feature selection for GNSS receiver fingerprinting. *InsideGNSS* **2017**, *17*, 2120.
22. Kuciapinski, K.S.; Temple, M.A.; Klein, R.W. ANOVA-based RF DNA analysis: Identifying significant parameters for device classification. In Proceedings of the 2010 International Conference on Wireless Information Networks and Systems (WINSYS), Athens, Greece, 26–28 July 2010; pp. 1–6.
23. Danev, B.; Zanetti, D.; Capkun, S. On Physical-Layer Identification of Wireless Devices. *ACM Comput. Surv.* **2012**, *45*, 1–29. [CrossRef]
24. Baldini, G.; Giuliani, R.; Steri, G.; Neisse, R. Physical layer authentication of Internet of Things wireless devices through permutation and dispersion entropy. In Proceedings of the 2017 Global Internet of Things Summit (GIoTS), Geneva, Switzerland, 6–9 June 2017; pp. 1–6. [CrossRef]
25. Baldini, G.; Gentile, C.; Giuliani, R.; Steri, G. Comparison of techniques for radiometric identification based on deep convolutional neural networks. *Electron. Lett.* **2019**, *55*, 90–92. [CrossRef]
26. Fadul, M.K.M.; Reising, D.R.; Sartipi, M. Identification of OFDM-Based Radios Under Rayleigh Fading Using RF-DNA and Deep Learning. *IEEE Access* **2021**, *9*, 17100–17113. [CrossRef]
27. Broumandan, A.; Lachapelle, G. Spoofing Detection Using GNSS/INS/Odometer Coupling for Vehicular Navigation. *Sensors* **2018**, *18*, 1305. [CrossRef]
28. Lo, S.; Chen, Y.H.; Jain, H.; Enge, P. Robust GNSS Spoof Detection using Direction of Arrival: Methods and Practice. In Proceedings of the 31st International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2018), Miami, FL, USA, 24–28 September 2018; pp. 2891–2906. [CrossRef]
29. Nguyen, V.H.; Falco, G.; Falletti, E.; Nicola, M. A Dual Antenna GNSS Spoofing Detector Based on the Dispersion of Double Difference Measurements. In Proceedings of the 2018 9th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC), Noordwijk, The Netherlands, 5–7 December 2018.
30. Gao, Y.; Li, H.; Lu, M.; Feng, Z. Intermediate spoofing strategies and countermeasures. *Tsinghua Sci. Technol.* **2013**, *18*, 599–605. [CrossRef]
31. Li, J.; Zhang, J.; Chang, S.; Zhou, M. Performance Evaluation of Multimodal Detection Method for GNSS Intermediate Spoofing. *IEEE Access* **2016**, *4*, 9459–9468. [CrossRef]
32. Humphreys, T.E.; Ledvina, B.M.; Psiaki, M.L.; O'Hanlon, B.W.; Kintner, P.M. Assessing the spoofing threat. *GPS World* **2018**, *20*, 28–38.
33. Schmidt, E.; Gatsis, N.; Akopian, D. A GPS Spoofing Detection and Classification Correlator-Based Technique Using the LASSO. *IEEE Trans. Aerosp. Electron. Syst.* **2020**, *56*, 4224–4237. [CrossRef]
34. Falletti, E.; Motella, B.; Gamba, M.T. Post-correlation signal analysis to detect spoofing attacks in GNSS receivers. In Proceedings of the 2016 24th European Signal Processing Conference (EUSIPCO), Budapest, Hungary, 29 August–2 September 2016; pp. 1048–1052. [CrossRef]
35. Thombre, S.; Raasakka, J.; Hurskainen, H.; Nurmi, J.; Valkama, M.; Lohan, S. Local oscillator phase noise effects on phase angle component of GNSS code correlation. In Proceedings of the 2011 International Conference on Localization and GNSS (ICL-GNSS), Tampere, Finland, 29–30 June 2011; pp. 110–115. [CrossRef]
36. Psiaki, M.L.; Powell, S.P.; O'hanlon, B.W. GNSS Spoofing Detection using High-Frequency Antenna Motion and Carrier-Phase Data. Proceedings of the 26th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2013, Nashville, TN, USA, 16–20 September 2013; p. 29492991.
37. Calero, D.; Fernandez, E. Characterization of Chip-Scale Atomic Clock for GNSS navigation solutions. In Proceedings of the 2015 International Association of Institutes of Navigation World Congress (IAIN), Prague, Czech Republic, 20–23 October 2015; pp. 1–8. [CrossRef]
38. Fernandez, E.; Calero, D.; Pares, M.E. CSAC Characterization and Its Impact on GNSS Clock Augmentation Performance. *Sensors* **2017**, *17*, 370. [CrossRef] [PubMed]
39. Giofre, R.; Colantonio, P.; González, L.; De Arriba, F.; Cabría, L.; Molina, D.L.; Garrido, E.C.; Vitobello, F. Design Realization and Tests of a Space-Borne GaN Solid State Power Amplifier for Second Generation Galileo Navigation System. *IEEE Trans. Aerosp. Electron. Syst.* **2018**, *54*, 2383–2396. [CrossRef]
40. Broumandan, A.; Jafarnia-Jahromi, A.; Lachapelle, G. Spoofing detection, classification and cancelation (SDCC) receiver architecture for a moving GNSS receiver. *GPS Solut.* **2015**, *19*, 475–487. [CrossRef]
41. Valkama, M.; Renfors, M.; Koivunen, V. Advanced methods for I/Q imbalance compensation in communication receivers. *IEEE Trans. Signal Process.* **2001**, *49*, 2335–2344. [CrossRef]
42. Handel, P.; Zetterberg, P. Receiver I/Q Imbalance: Tone Test, Sensitivity Analysis, and the Universal Software Radio Peripheral. *IEEE Trans. Instrum. Meas.* **2010**, *59*, 704–714. [CrossRef]
43. D'Apuzzo, M.; D'Arco, M.; Liccardo, A.; Vadursi, M. Modeling DAC Output Waveforms. *IEEE Trans. Instrum. Meas.* **2010**, *59*, 2854–2862. [CrossRef]
44. Lei, Y.; Tan, J.; Guo, W.; Cui, J.; Liu, J. Time-Domain Evaluation Method for Clock Frequency Stability Based on Precise Point Positioning. *IEEE Access* **2019**, *7*, 132413–132422. [CrossRef]

45. Chen, X.; Peng, C.; Huan, H.; Nian, F.; Yang, B. Measuring the Power Law Phase Noise of an RF Oscillator with a Novel Indirect Quantitative Scheme. *Electronics* **2019**, *8*, 767. [CrossRef]
46. Gomez-Casco, D.; Lopez-Salcedo, J.A.; Seco-Granados, G. Generalized integration techniques for high-sensitivity GNSS receivers affected by oscillator phase noise. In Proceedings of the 2016 IEEE Statistical Signal Processing Workshop (SSP), Palma de Mallorca, Spain, 26–29 June 2016; pp. 1–5. [CrossRef]
47. Zhang, S.; Wang, X.; Wang, H.; Yang, J. From Allan variance to phase noise: A new conversion approach. In Proceedings of the EFTF-2010 24th European Frequency and Time Forum, Noordwijk, The Netherlands, 13–16 April 2010; pp. 1–8. [CrossRef]
48. Majidi, M.; Mohammadi, A.; Abdipour, A. Analysis of the Power Amplifier Nonlinearity on the Power Allocation in Cognitive Radio Networks. *IEEE Trans. Commun.* **2014**, *62*, 467–477. [CrossRef]
49. Schreurs, D.; O'Droma, M.; Goacher, A.A.; Gadringer, M. *RF Power Amplifier Behavioral Modeling*; Cambridge University Press: New York, NY, USA, 2008.
50. Kim, J.; Konstantinou, K. Digital predistortion of wideband signals based on power amplifier model with memory. *Electron. Lett.* **2001**, *37*, 1417–1418. [CrossRef]
51. OHB System AG- Galileo -European Satellite Navigation System (space segment). OHB Brochure. 2021. Available online: https://www.ohb-system.de/files/images/mediathek/downloads/190603_OHB-System_Galileo_FOC-Satellites_2019-05.pdf (accessed on 20 February 2021).
52. National Instruments Corp. Global Synchronization and Clock Disciplining with NI USRP-293x Software Defined Radio. 2020. Available online: https://www.ni.com/fi-fi/innovations/white-papers/20/global-synchronization-and-clock-disciplining-with-ni-usrp-293x-.html (accessed on 24 April 2021).
53. Rehman, S.U.; Sowerby, K.W.; Alam, S.; Ardekani, I.T.; Komosny, D. Effect of channel impairments on radiometric fingerprinting. In Proceedings of the 2015 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT), Abu Dhabi, United Arab, 7–10 December 2015; pp. 415–420. [CrossRef]
54. Kennedy, I.O.; Kuzminskiy, A.M. RF Fingerprint detection in a wireless multipath channel. In Proceedings of the 2010 7th International Symposium on Wireless Communication Systems, York, UK, 19–22 September 2010; pp. 820–823. [CrossRef]
55. Zheng, T.; Sun, Z.; Ren, K. FID: Function Modeling-based Data-Independent and Channel-Robust Physical-Layer Identification. In Proceedings of the IEEE INFOCOM 2019-IEEE Conference on Computer Communications, Paris, France, 29 April–2 May 2019; pp. 199–207. [CrossRef]
56. Tascioglu, S.; Kose, M.; Telatar, Z. Effect of sampling rate on transient based RF fingerprinting. In Proceedings of the 2017 10th International Conference on Electrical and Electronics Engineering (ELECO), Bursa, Turkey, 30 November–2 December 2017; pp. 1156–1160.
57. Ur Rehman, S.; Sowerby, K.; Coghill, C. RF fingerprint extraction from the energy envelope of an instantaneous transient signal. In Proceedings of the 2012 Australian Communications Theory Workshop (AusCTW), Wellington, New Zealand, 30 January–2 February 2012; pp. 90–95. [CrossRef]
58. Hamila, R.; Lohan, E.S.; Renfors, M. Subchip multipath delay estimation for downlink WCDMA system based on Teager-Kaiser operator. *IEEE Commun. Lett.* **2003**, *7*, 1–3. [CrossRef]
59. Brihuega, A.; Anttila, L.; Abdelaziz, M.; Eriksson, T.; Tufvesson, F.; Valkama, M. Digital predistortion for multiuser hybrid MIMO at mmWaves. *IEEE Trans. Signal Process.* **2020**, *68*, 3603–3618. [CrossRef]
60. Rasmussen, K.B.; Capkun, S. Implications of Radio Fingerprinting on the Security of Sensor Networks. In Proceedings of the 2007 Third International Conference on Security and Privacy in Communications Networks and the Workshops—SecureComm 2007, Nice, France, 17–21 September 2007.
61. Gahlawat, S. Investigation of RF Fingerprinting Approaches in GNSS. Ph.D. Thesis, Tampere University, Tampere, Finland, 2020, [CrossRef]
62. Hall, J.; Barbeau, M.; Kranakis, E. Detection Of Transient In Radio Frequency Fingerprinting Using Signal Phase. In Proceedings of IASTED International Conference on Wireless and Optical Communications, Banff, AL, Canada, 14–16 July 2003.
63. Gerdes, R.M.; Daniels, T.E.; Mina, M.; Russell, S.F. Device identification via analog signal fingerprinting: A matched filter approach. In Proceedings of the 144 Proceedings of the Network and Distributed System Security Symposium NDSS, San Diego, CA, USA, 23–26 February 2006; p. 78.
64. Brik, V.; Banerjee, S.; Gruteser, M. Wireless device identification with radiometric signatures. In Proceedings of the 14th ACM international conference on mobile computing and networking, ser. MobiCom '08, San Francisco, CA, USA, 8–12 September 2008; pp. 116–127.
65. Candore, A.; Kocabas, O.; Koushanfar, F. Robust stable radiometric fingerprinting for wireless devices. In Proceedings of the 2009 IEEE International Workshop on Hardware-Oriented Security and Trust, San Francisco, CA, USA, 27 July 2009; pp. 43–49. [CrossRef]
66. Yuanling Huang.; Hui Zheng. Radio frequency fingerprinting based on the constellation errors. In Proceedings of the 2012 18th Asia-Pacific Conference on Communications (APCC), Jeju, Korea, 15–17 October 2012; pp. 900–905. [CrossRef]
67. Lukacs, M.; Collins, P.; Temple, M. Classification performance using 'RF-DNA' fingerprinting of ultra-wideband noise waveforms. *Electron. Lett.* **2015**, *51*, 787–789. [CrossRef]

68. Borio, D.; Gioia, C.; Baldini, G.; Fortuny, J. GNSS Receiver Fingerprinting for Security-Enhanced Applications. In Proceedings of the 29th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+), Portland, OR, USA, 12–16 September 2016; pp. 2960–2970.
69. Jia, Y.; Zhu, S.; Gan, L. Specific Emitter Identification Based on the Natural Measure. *Entropy* **2017**, *19*, 117. [CrossRef]
70. at al., W.D.W. Authentication by Polarization: A Powerful Anti-Spoofing Method. In Proceedings of the 31st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+), Miami, FL, USA, 24–28 September 2018; pp. 3643–3658. [CrossRef]
71. Ali, A.; Fischer, G. Symbol Based Statistical RF Fingerprinting for Fake Base Station Identification. In Proceedings of the 2019 29th International Conference Radioelektronika (RADIOELEKTRONIKA), Pardubice, Czech Republic, 16–18 April 2019; pp. 1–5. [CrossRef]
72. Ali, A.; Fischer, G. The Phase Noise and Clock Synchronous Carrier Frequency Offset based RF Fingerprinting for the Fake Base Station Detection. In Proceedings of the 2019 IEEE 20th Wireless and Microwave Technology Conference (WAMICON), Cocoa Beach, FL, USA, 8–9 April 2019; pp. 1–6. [CrossRef]
73. Chen, X.; Hao, X. Feature Reduction Method for Cognition and Classification of IoT Devices Based on Artificial Intelligence. *IEEE Access* **2019**, *7*, 103291–103298. [CrossRef]
74. Hanna, S.S.; Cabric, D. Deep Learning Based Transmitter Identification using Power Amplifier Nonlinearity. In Proceedings of the 2019 International Conference on Computing, Networking and Communications (ICNC), Honolulu, HI, USA, 18–21 Febuary 2019; pp. 674–680. [CrossRef]
75. Pan, Y.; Yang, S.; Peng, H.; Li, T.; Wang, W. Specific Emitter Identification Based on Deep Residual Networks. *IEEE Access* **2019**, *7*, 54425–54434. [CrossRef]
76. Zha, H.; Tian, Q.; Lin, Y. Real-World ADS-B signal recognition based on Radio Frequency Fingerprinting. In Proceedings of the 2020 IEEE 28th International Conference on Network Protocols (ICNP), Madrid, Spain, 13–16 October 2020; pp. 1–6. [CrossRef]
77. Nicolussi, A.; Tanner, S.; Wattenhofer, R. Aircraft Fingerprinting Using Deep Learning. In Proceedings of the 2020 28th European Signal Processing Conference (EUSIPCO), Amsterdam, The Netherlands, 18–21 January 2021; pp. 740–744. [CrossRef]
78. Ezuma, M.; Erden, F.; Kumar Anjinappa, C.; Ozdemir, O.; Guvenc, I. Detection and Classification of UAVs Using RF Fingerprints in the Presence of Wi-Fi and Bluetooth Interference. *IEEE Open J. Commun. Soc.* **2020**, *1*, 60–76. [CrossRef]
79. Weng, L.; Peng, J.; Li, J.; Zhu, Y. Message Structure Aided Attentional Convolution Network for RF Device Fingerprinting. In Proceedings of the 2020 IEEE/CIC International Conference on Communications in China (ICCC), Chongqing, China, 9–11 August 2020; pp. 495–500. [CrossRef]
80. Reising, D.; Cancelleri, J.; Loveless, T.D.; Kandah, F.; Skjellum, A. Radio Identity Verification-based IoT Security Using RF-DNA Fingerprints and SVM. *IEEE Internet Things J.* **2020**, 1. [CrossRef]
81. Soltani, N.; Reus-Muns, G.; Salehihikouei, B.; Dy, J.; Ioannidis, S.; Chowdhury, K. RF Fingerprinting Unmanned Aerial Vehicles with Non-standard Transmitter Waveforms. *IEEE Trans. Veh. Technol.* **2020**, *69*. [CrossRef]
82. Zhou, X.; Hu, A.; Li, G.; Peng, L.; Xing, Y.; Yu, J. A Robust Radio Frequency Fingerprint Extraction Scheme for Practical Device Recognition. *IEEE Internet Things J.* **2021**, 1. [CrossRef]
83. Frisch, M.; Messer, H. Transient signal detection using prior information in the likelihood ratio test. *IEEE Trans. Signal Process.* **1993**, *41*, 2177–2192. [CrossRef]
84. Kelly, E.J. An Adaptive Detection Algorithm. *IEEE Trans. Aerosp. Electron. Syst.* **1986**, *AES-22*, 115–127. [CrossRef]
85. Karunaratne, S.; Krijestorac, E.; Cabric, D. Penetrating RF Fingerprinting-Based Authentication with a Generative Adversarial Attack. *arXiv* **2020**, arXiv:2011.01538,
86. Riyaz, S.; Sankhe, K.; Ioannidis, S.; Chowdhury, K. Deep learning convolutional neural networks for radio identification. *IEEE Commun. Mag.* **2018**, *56*, 146–152. [CrossRef]
87. Morin, C.; Cardoso, L.; Hoydis, J.; Gorce, J.M. Deep Learning-Based Transmitter Identification on the Physical Layer. INRIA Report. 2021. Available online: https://hal.inria.fr/hal-03117090 (accessed on 24 April 2021).
88. Ibrahim, Y.; Mu'Azu, M.B.; Adedokun, A.E.; Sha'Aban, Y.A. A performance analysis of logistic regression and support vector machine classifiers for spoof fingerprint detection. In Proceedings of the 2017 IEEE 3rd International Conference on Electro-Technology for National Development (NIGERCON), Owerri, Nigeria, 7–10 November 2017; pp. 1–5. [CrossRef]
89. Patel, H. Introduction of Random Forest Classifier to ZigBee Device Network Authentication Using RF-DNA Fingerprinting. *J. Inf. Warf.* **2014**, *13*, 33–45.
90. Rebeyrol, E.; Macabiau, C.; Ries, L.; Issler, J.L.; Bousquet, M.; Boucheret, M.L. Phase noise in GNSS transmission/reception system. In Proceedings of the 2006 National Technical Meeting of the Institute of Navigation, Monterey, CA, USA, 18–20 January 2006; pp. 698–708.

PUBLICATION

6

Pre-correlation and post-correlation RF fingerprinting methods for GNSS spoofer identification with real-field measurement data

W. Wang, E. S. Lohan, I. Aguilar Sanchez and G. Caparra

*in Proceedings of NAVITEC*2022

Pre-correlation and post-correlation RF fingerprinting methods for GNSS spoofer identification with real-field measurement data

Wenbo Wang
Tampere University
ORCID: 0000-0002-4319-4103

Elena Simona Lohan
Tampere University
0000-0003-1718-6924

Ignacio Aguilar Sanchez
European Space Agency
0000-0003-3619-6175

Gianluca Caparra
European Space Agency
0000-0003-3331-6899

Abstract—**Radio Frequency fingerprinting (RFF) methods are gaining popularity as physical-layer identification or authentication methods in various navigation and communication applications. Traditionally, RFF has been used in terrestrial communications to identify the genuine transmitters from spoofers and jammers. In recent literature, RFF has gained attention also in the context of satellite navigation and Low Earth Orbit (LEO) satellite communications, though this research area is still in an incipient phase. RFF studies in the context of satellite transmitters (or transceivers) are typically hindered by the challenges in acquiring high-quality raw measurement data. In this paper, we analyze via RFF methods, in both pre-correlation and post-correlation domain, the raw GNSS data collected at three locations: Tampere (Finland), Nottingham (UK), and Nuremberg (Germany). The datasets for the first two scenarios have been collected by the authors, while the third dataset is available in open access. We show that we are able to reach average classification probabilities of spoofer versus GNSS up to 99.99% (i.e., Nuremberg measurements) with pre-correlation data and up to 87.72% (i.e., Nottingham measurements) with post-correlation data. We also discuss the challenges and limitations of RFF in the context of GNSS.**

Index Terms—**Radio Frequency Fingerprinting (RFF), Global Navigation Satellite Systems (GNSS), Machine Learning (ML), Support Vector Machines (SVM).**

I. Introduction and motivation

In a broad sense, the Radio Frequency Fingerprinting (RFF) methods refer to a set of methods based on machine learning (ML) techniques and using the patterns or hidden features of the received signals in order to identify, classify, or estimate various parameters [1]–[4]. Such parameters can refer to the transmitter characteristics (e.g., RFF here may refer to the problem of identifying genuine transmitters from spoofers or other interferer, based on transmitter hardware features), to the channel characteristics (e.g., RFF here may refer to the task of identifying a certain time-space location based on wireless channel features), or to the receiver characteristics (e.g., RFF here may refer to the problem of identifying a receiver type, based on the receiver hardware features). Typically, the transmitter, channel, and receiver effects cannot be separated and they are analyzed jointly based on the received signal, for one or several of the above-mentioned purposes, i.e., transmitter identification/classification, space-time localization, or receiver identification/classification.

The research problem addressed in this paper falls within the area of using RFF for transmitter identification/classification, or, more specifically, we address the problem of detecting a spoofer from a genuine Global Navigation Satellite System (GNSS) transmitter, through the processing of received signal samples in pre-correlation and post-correlation domains, respectively.

Our previous work in [3] has addressed the similar problem of spoofer detection in GNSS based only on pre-correlation In-Phase/Quadrature (I/Q) GNSS raw data and relying fully on simulation-based results. In [3] we modeled five transmitter impairments in a Galileo GNSS and a spoofing GNSS transmitter, namely: phase noises, power amplifier non-linearities, I/Q imbalance, Digital-to-Analog Converter (DAC) non-linearities, and transmitter Band-Pass Filter (BPF) features. Under the assumptions of very low channel noise over an Additive White Gaussian Noise (AWGN) channel with carrier-to-noise ratios (C/N_0) of $100\,$dB-Hz, we showed in [3] a simulation-based classification accuracy with Support Vector Machines (SVMs) of up to 100% when all the five transmitter features are taken into account in a joint manner. We also showed in [3] that not all individual transmitter features carried an equal role in the RFF performance. In particular, the transmitter features with the strongest impact proved to be the power-amplifier non-linearities, the I/Q imbalance, and the transmitter BPF. One of the main limitations in the work in [3] has been the fact that it relied fully on simulated models, with high C/N_0 profiles. Therefore, this paper extends the work in [3] by focusing on real-life measurements of Global Positioning System (GPS) data with realistic channels, having a C/N_0 around $35-45\,$dB-Hz. We are also looking in this paper at both pre-correlation and post-correlation approaches. In a measurement-based approach, the individual weights of each transmitter feature cannot be distinguished from each other and only the global effect can be investigated. We have selected three different scenarios, based on two GPS-and-spoofer datasets collected by the Authors in Nottingham, UK and Tampere, FIN, respectively, as well as on an open-access GPS-and-spoofer dataset collected in Fraunhofer, DE [5].

With respect to related work to this research, RFF approach in the GNSS context has been poorly addressed in the literature so far. The authors in [6] investigated the spoofer detection with simulated GPS data and an SVM classifier and obtained a classification accuracy about 84% (computed as the complement of their reported false rejection rate values). No validation based on measurement data was provided in [6]. The work in [7] is a combined a simulation-based and Universal Software Radio Platform (USRP)-based RFF work with GPS C/A signals. The authors generated a GPS signal in a lab, by using a USRP with customized RF module, and applied a k-means clustering for signal classification. However, no statistical results were provided in [7], only a feasibility study was done, showing visually that RFF has some potential in GNSS context.

While the studies in [6] and [7] focused on the GPS pre-correlation data, the authors in [8] relied on the post-correlation and navigation data and made the analyses on measurement datasets from Texas Spoofing Test Battery (TEXTBAT) data. An SVM classifier with Principal Component Analysis (PCA) was applied on datasets containing C/N_0 measurements and early-late phase measurements in post-correlation domain. Moderate-to-high classification accuracies up to 92.3% were obtained. No pre-correlation studies were included in [8] and their overall accuracy figures were much better than the results based on the confusion matrix figures that showed maximum class accuracies below 60%. Our results are to be expressed in Section IV terms of confusion matrix accuracy and we will show that one can achieve better classification results than in [8] based on pre-correlation data, and moderately lower classification results based on post-correlation data. In our paper, the pre-correlation data is used in conjunction with a spectrogram-based feature-extraction method, followed by SVM with PCA as the dimension-reduction tool. Such pre-correlation data can only identify the sate whether a spoofer is present or not, but it cannot identify the spoofer itself, since all the pre-correlation data is merged from all visible satellites at I/Q level. The classification accuracy with post-correlation data decreases, because in post-correlation domain, the receiver has already despread the pseudo-random codes from each signal present (genuine GNSS satellite or spoofer), and thus there is more burden in the classifier to be able to identify correctly each signal in the mixture. In addition, the despreading process needed to access the post-correlation data acts as a smoother of RF features, and thus some RFF information may be lost. We will also propose an algorithmic flowchart of combining pre-correlation and post-correlation findings.

The rest of the paper is organized as follows: Section II looks back the RF fingerprinting techniques in GNSS, and brings up our understanding of a generic transmitter for GNSS signals broadcasting purpose, as well as the development of methodology dealing with the RF fingerprinting in GNSS. Section III describes thoroughly the measurement campaigns in Nottingham, Nuremberg, and Tampere, and an example of the hardware setup is provided. Section IV starts with a flow chart of RF fingerprinting based anti-spoofing Position, Velocity, and Time (PVT) solution, and, then, it presents the pre- and post-correlation classification accuracies based on the three measurement datasets. Section V concludes the current work, emphasizes the open challenges and limitations in RFF for GNSS, and discusses the way forward.

II. RF Fingerprinting in GNSS

Following the literature searches, e.g., [3], [9], [10], and general understanding of the GNSS transmitter functionalities, a generic diagram of a GNSS transmitter is depicted in Fig. 1. This block diagram allows us to have a close look at the differences in terms of possible hardware impairments (or 'RF features') between a GNSS satellite and a GNSS spoofer.

To begin with, the clock unit shown in Fig. 1 is typically a combination of multiple atomic clocks on-board of a GNSS satellite; for example, rubidium atomic frequency standards and passive hydrogen masers are typically used. At the same time, the typical GNSS spoofers do not have the budget for expensive atomic clocks; for example, an over €10000 USRP RIO 2954R uses an Oven Controlled Crystal Oscillator (OCXO).

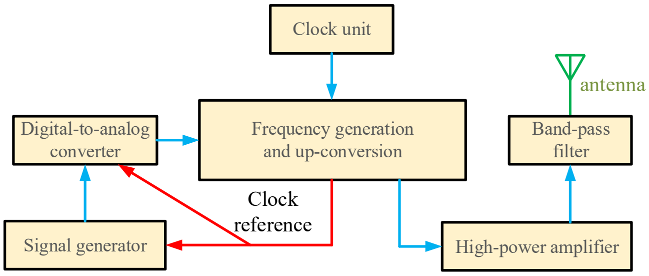


Fig. 1: A generic diagram of a transmitter for GNSS signals, valid for both satellites and spoofers. The differences stay in the hardware characteristics of each of the illustrated blocks. The red arrows indicate the signals do not carry extra features from the previous unit; the blue arrows imply that the signals carry extra features from the previous unit.

Also, as illustrated in Fig. 1, the digital-to-analog converter (DAC) unit is present in both the genuine and spoofer GNSS signal transmitters. However, the DAC in GNSS satellites very likely shows different hardware characteristics of non-linearity and phase noises than a common spoofer. In the up-conversion process, GNSS satellites could attain a lower level of phase noises and I/Q imbalances than a spoofer. The high power amplifier (HPA) in GNSS satellites usually promises better linearity and less frequency-dependent variations than a common power amplifier used in a spoofer. As for the band-pass filter (see Fig. 1), a flat response of desired band signals and steep cut-off are achievable in GNSS satellites, but less steep cut-off ranges are achievable in a spoofer. These aspects of hardware differences existing in satellites and spoofer set the ground of RF fingerprinting in GNSS as they create unique transmitter hardware features for each transmitter.

In this paper, we develop a methodology to tackle the RF fingerprinting in GNSS as illustrated in Fig. 2. The possible factors leading to RF fingerprints (or RF features) are listed

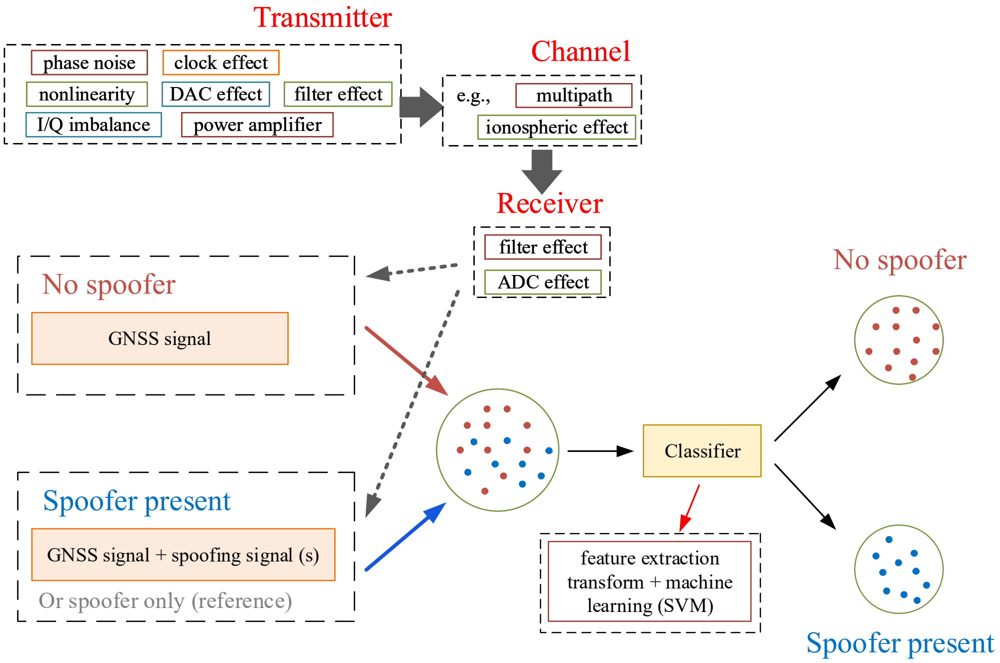


Fig. 2: The methodology of this work.

in the diagram in Fig. 2. Such 'features' are basically present over the whole transmitter-channel-receiver chain, but the differentiating features between a GNSS and a spoofer are mainly coming from the transmitter side. In the channel part, we emphasize that multipath effects may occur for both GNSS signals and spoofer signals, whereas the atmospheric effects, e.g., ionospheric effect, only exist in the GNSS signals, unless we may have a high-altitude spoofer, e.g., a spoofer installed on a Low Earth Orbit (LEO) satellite, which is extremely rare to the best of the Authors' knowledge. The receiver 'features' are common to both spoofer and GNSS received signals, as the receiver captures a mixture of both signal types (genuine and, possibly spoofer signals). Therefore, the receiver features (such as filtering and analog-to-digital converter) are likely to act as 'smoothers' of the relevant RF fingerprints.

Our models assume that two categories can be present, namely 'no-spoofer' and 'spoofer-present' categories. As a benchmark case, we also consider the 'spoofer-only' case, as a sub-category 'spoofer-present' class. This 'spoofer-only' case is a theoretical possibility, not realistic in practice, but which can be verified in laboratory settings and can be used for training the ML-based classification algorithms as well as for providing benchmark results. In the 'spoofer-present' class, both the genuine GNSS signals and spoofer signals are present, while in the 'spoofer-only' class, we assume that only the spoofer signals are present (e.g., as generated by a GNSS signal generator in lab conditions).

A conceptual 'classifier' block, consisting of a feature-extraction transform and a machine learning method, as shown in Fig. 2, is employed to distinguish between the above-mentioned two categories ('no-spoofer' versus 'spoofer-present'). The purpose of a feature-extraction transform, detailed also in our previous work in [3], is to enhance the possible differentiating features between spoofers and genuine GNSS signals, before feeding the data into the classifier. Various feature-extraction transforms have been studied in the literature in various contexts, such as in the context of Bluetooth [11], Internet of Things (IoT) communications [12], Radio Frequency Identification (RFID) [13], Automatic Dependent Surveillance-Broadcast (ADS-B) [14], Unmanned Aerial Vehicle (UAV) data [15], or WiFi [14], [16]. In [3], we have investigated several feature-extraction transforms and have selected the most relevant ones in GNSS context, as described below. As GNSS signals are not packet-based signals, the feature-extraction transforms which rely on transients in the signal, such as transient windowing [12], or preamble based [15] are not suitable. However, various time-frequency transforms have shown to be suitable with GNSS signals.

One can apply the feature-extraction transforms at different parts of the receiver chain. We focus on two domains in here, namely **the pre-correlation domain** (using directly the I/Q samples at the Analog-to-Digital converter (ADC) output) and **the post-correlation domain** (using the correlation-output samples, after the time-frequency-domain correlation is performed with the reference pseudorandom code). The types of the possible feature-extraction transforms are domain dependent.

For example, in the pre-correlation stage, I/Q raw samples are available, and transforms such as short-time-short-frequency (STSF), discrete wavelet transform (DWT), kurtosis, spectrogram, or Teager-Kaiser energy operator (TKEO) can be applied as feature-extraction methods. The mathematical forms of these transforms can be found in our previous work [3]. In here we have selected only the spectrogram, kurtosis, TKEO, and DWT, as the most promising ones among those previously investigated. In the post-correlation stage, the outputs of time-frequency correlation are available for each satellite (as correlation is performed with all reference codes of the satellites on sky). Therefore, the post-correlation methods could, in theory, identify not only if a spoofer is present, but also which of the identified satellite signals is coming from a spoofer. Such as distinction cannot be made with pre-correlation data; based on pre-correlation data, the classifier can only state if the spoofer is present or not in the received I/Q samples. In the post-correlation domain, the correlator itself plays the role of a feature-extraction transform, thus no additional feature-extraction transforms are applied.

For both GNSS (here a GPS C/A signal coming from satellites on the sky at the moment of the measurements, details in section III) and spoofer signals, examples of pre- and post-correlation feature-extraction outputs are shown in Fig. 3. In the pre-correlation domain, we present the outputs of spectrogram as an example, while in the post-correlation domain we present the output of the time-frequency correlator block, centered along the maximum peak. These examples are from the measurements in Tampere. Fig. 3 shows that the hardware features specific to GPS and spoofing signals are hard to be distinguished with naked eye; yet, as we will show in Section IV, there are intrinsic features which can be classified with a ML classifier such as SVM.

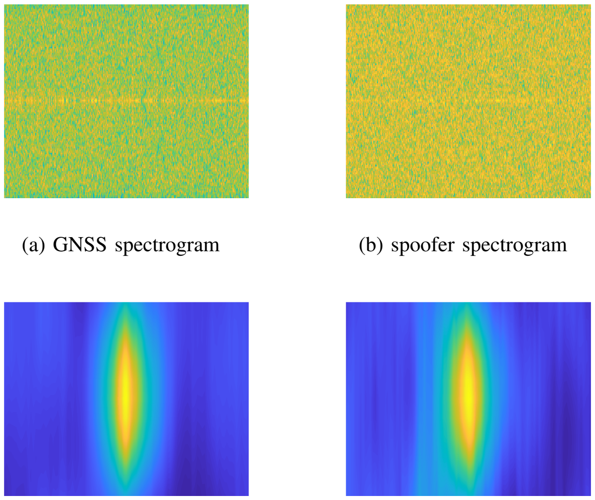
III. Measurement campaigns and measurement-data description

Two measurement campaigns were conducted by the Authors in Nottingham, UK and Tampere, Finland, respectively. In addition, we also used a measurement dataset available in open access [5] and collected from Nuremberg, Germany. All measurements were recorded in L1 band for GPS C/A signals.

In the measurements performed in Nottingham and Tampere, three scenarios were recorded, namely the clear-sky GNSS signals, Spirent/spectracom-based spoofer signals, and GNSS-and-spoofer mixture signals. In the Nuremberg measurements, we only have two scenarios available, namely the clear-sky GNSS signals and Spirent-based spoofer signals.

In the measurements we conducted in Tampere, a Spectracom GSG-64 GNSS signal generator was used to act as the spoofer, Tallysman TW3972 was our roof antenna to receive GPS signals, and an USRP RIO 2954R was used as the receiver, for the collection of I/Q samples. In the Nottingham and Nuremberg measurements, the Spirent signal generator was used as the spoofer.

We used a carrier-to-noise ratio estimator in Fig. 4 to estimate each C/N_0 of signals contained per measurement. The C/N_0 estimator is adapted from [17], where I_P, Q_p and Q_N are in-phase components, quadrature components, and noise samples, respectively. To be more specific, Q_N samples correspond to the outputs of the complex correlators outside the peak values. All signals are integrated and dumped through a low-pass filter (LPF).


(a) GNSS spectrogram

(b) spoofer spectrogram

(c) GNSS post-correlation

(d) spoofer post-correlation

Fig. 3: Feature extraction examples in pre- and post-correlation of GNSS and spoofer signals based on Tampere measurements. a) GPS pre-correlation data, spectrogram; b) Spoofer pre-correlation data, spectrogram; c) Time-frequency post-correlation data (centered around the correlation peak), GPS signal; c) Time-frequency post-correlation data (centered around the correlation peak), spoofer signal;

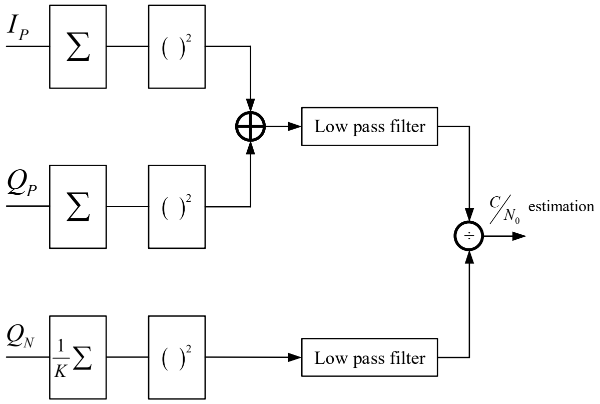


Fig. 4: A basic carrier-to-noise ratio estimator used in our data processing.

The detailed parameters in the measurements are listed in Table I. The pseudorandom (PRN) satellite index in the measurements is given together with the estimated C/N_0 per satellite. In Nottingham and Tampere measurements, 25 MHz sampling frequency and 16 bits quantization were used; the Nuremberg measurements are with 20 MHz sampling frequency and 8 bits quantization. For the pre-correlation clas-

TABLE I: Parameters in measurements

		PRN index (corresponding C/N_0 [dB-Hz])	**Sampling frequency [MHz]**	**Quantization [bit/sample]**	**Pre-correlation window [ms]**	**Post-correlation window**
Nottingham	GNSS	2 (45.26), 4 (36.33), 25 (50.14), 26 (40.34), 29 (50.45), 31 (48.05)	25	16	1	1 ms coherent integration, 8 blocks of non-coherent integration, total 8 ms integration interval.
	spoofer	2 (49.73), 4 (49.62), 12 (49.95), 25 (51.72), 26 (49.94), 29 (51.50), 31 (51.07)				
	GNSS+spoofer	2 (42.81), 4 (36.34), 18 (40.33), 25 (49.12), 26 (44.54), 27 (49.04), 29 (50.30), 31 (49.87)				
Nuremberg	GNSS	1 (47.04), 4 (49.48), 6 (43.55), 9 (43.40), 11 (41.80), 13 (44.00), 17 (46.81), 20 (49.53), 23 (49.29), 31 (45.60), 32 (46.54)	20	8	1	1 ms coherent integration, 8 blocks of non-coherent integration, total 8 ms integration interval.
	spoofer	7 (46.69), 8 (46.89), 10 (47.94), 15 (46.87), 19 (45.85), 21 (46.03), 24 (45.42), 26 (47.51), 27 (48.15), 28 (46.90)				
	GNSS+spoofer	not available				
Tampere	GNSS	1 (35.06), 3 (37.82), 17 (35.20), 19 (35.49), 21 (33.02), 22 (36.88), 31 (35.81), 32 (32.80)	25	16	1	10 ms coherent integration, 5 blocks of non-coherent integration, total 50 ms integration interval.
	spoofer	1 (34.57), 3 (35.52), 4 (34.23), 17 (35.50), 19 (34.85), 21 (34.74), 22 (34.58), 31 (36.66)				
	GNSS+spoofer	1 (34.60), 3 (36.60), 12 (35.72), 17 (33.76), 19 (34.18), 22 (35.54), 31 (33.92)				

* we marked the first four/six strong receiving signals with purple highlight;

** we marked the spoofer signal within the mixture using blue colour.

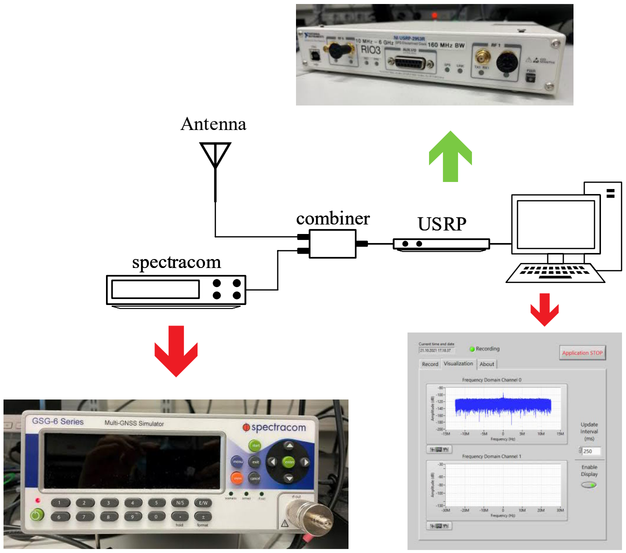


Fig. 5: A demonstration of devices setup. The example setup means to receive the combination of GNSS and spoofer signals at L1 band.

sification, we split signals into 1 ms per sample for a total 1 minute signal duration; for the post-correlation classification, due to the low C/N_0 values in Tampere measurements, we applied 10 ms coherent integration and 5 blocks of non-coherent integration. A picture of the hardware setup for 'GNSS+spoofer' mixture collected in Tampere is shown in Fig. 5. The Spectracom generator is used as a spoofer transmitter; the spoofer and GPS sky-antenna signals are combined via a combiner block and, afterwards, an USRP records the data stream and stores the data in the computer.

We also emphasize that, in both Nottingham and Tampere measurements, the noise level in spoofer signals has been adjusted to match the C/N_0 level in GPS signals. This was done in order to minimize the influence of noise in the identification of spoofer. In the Nuremberg measurements, it is unknown whether a similar process was applied or not. However, it could be seen from Table I that the C/N_0 levels between GNSS and spoofer signals show insignificant differences.

IV. Spoofer Identification Results

We propose the flow chart in Fig. 6 to implement an RF-fingerprinting-based online anti-spoofing PVT solution. To start, a batch of I/Q samples are buffered, and go through the pre-correlation and post-correlation classification stages.

After these processes and after removing spoofer signals when identified, the PVT solution will be formed either with current received satellite signals (if enough available) or by the aid of complementary methods. In both pre-correlation and post-correlation methods we apply a supervised learning method, namely SVM, for the classification part.

Regarding to the available scenarios in the measurements, we define three classes as:

1. GNSS signals at L1 band;
2. ‘spoofer’ generated GPS L1 band signals;
3. the mixture of GNSS signals and ‘spoofer’ generated GPS signals at L1 band.

We note that the third class is not available in Nuremberg measurements, as mixture signals were not collected in that particular dataset.

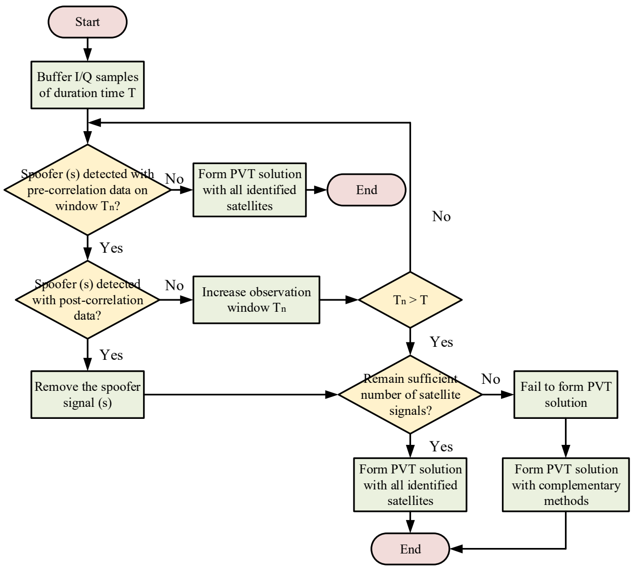

Start
Buffer I/Q samples of duration time T
Spoofer (s) detected with pre-correlation data on window Tn?
No
Form PVT solution with all identified satellites
End
No
Yes
Spoofer (s) detected with post-correlation data?
No
Increase observation window Tn
Tn > T
Yes
Yes
Remove the spoofer signal (s)
Remain sufficient number of satellite signals?
No
Fail to form PVT solution
Yes
Form PVT solution with all identified satellites
Form PVT solution with complementary methods
End

Fig. 6: The flow chart of RF fingerprinting based anti-spoofing PVT solution.

A. Classification with pre-correlation data

The pre-correlation methods focus on the classification among the defined three classes. In this work, all I/Q samples are firstly processed by DWT, kurtosis, spectrogram, and TKEO respectively, followed by a PCA process to reduce dimension in data. Eventually, by utilizing grid search method, we tune the parameters in SVM to achieve the optimal prediction of classes.

The outputs of DWT, kurtosis, and TKEO are in vector format, while the spectrogram has the image format as inputs. Reading an image data typically consumes a larger memory than reading a vector. Consequently, after the whole data pool is split into training and testing parts, with 50 Monte-Carlo runs for the each of the 3 transforms (DWT, kurtosis, and TKEO) we randomly draw 5000 samples for training and 1000 samples for testing; for the spectrogram we randomly draw 2000 samples for training and 400 samples for testing (to keep a similar complexity level as in the vector-format inputs).

In the machine learning stage, we set 20 components for PCA process and a radial basis function (RBF) kernel for SVM; the grid search is utilised for the fine tuning of the SVM parameters. The prediction results are expressed using confusion matrix with mean values over 50 Monte Carlo runs; a definition of confusion matrix could be found, for example, in [3] and it is basically showing on its diagonal values the probabilities to classify correctly each class; thus the average over the diagonal values give an estimate of the average classification accuracy which can be attained. The non-diagonal values are basically showing the probabilities of mis-classifying a certain class into another class.

The classfication results of Nottingham, Nuremberg, and Tampere are shown in Fig. 7, Fig. 8, and Fig. 9, respectively. As above-mentioned, the mean value over diagonal in each confusion matrix indicate the overall prediction accuracy: in the Nottingham measurements, the spectrogram reaches 80.06% average classification accuracy, followed by the DWT with 73.08%; in the Nuremberg measurements, the spectrogram reaches 99.99%, average classification accuracy, also followed by the DWT with 97.96%; in the Tampere measurements, the spectrogram reaches 97.03% average classification accuracy, followed by the kurtosis transform with 95.94%. In all three classifications, the combination of the spectrogram transform and SVM is able to distinguish classes with very good accuracy and spectrogram transform proved to be the best among the four considered feature-extraction transforms in all scenarios.

As we have adjusted the noise level in spoofer signals of Nottingham and Tampere measurements, the good classification results for spoofer signals cannot be attributed solely to the noise features. However, the noise might play a part in the classification, as the spoofer and GPS noises are slightly different. Nevertheless, most of the good classification accuracy is likely due to the intrinsic hardware features, as the noise variances (or CNR) are of the same order in the spoofer and GPS signals.

As seen in the results so far, the combination of the spectrogram transform and SVM classifier provides the best prediction results in all three measurements. The spectrogram used in this work is based on short-time Fourier transform (STFT), with a 128-length periodic Hann window with 75% window length overlap, and 128 fast Fourier transform (FFT) length while the FFT results are centered.

The kurtosis transform in the Tampere measurements gives surprisingly very good prediction accuracy, whereas this transform in other two measurement scenarios (Nuremberg and Nottingham) basically fails to distinguish between the classes. To uncover this phenomenon, Fig. 10 illustrates the histogram of I/Q samples’ amplitude distribution; clearly the distribution of amplitude values among three classes in the Tampere measurements are less overlapped than the Nottingham and Nuremberg measurements, which explains why kurtosis is likely to be a good transform in Tampere data, but not in the

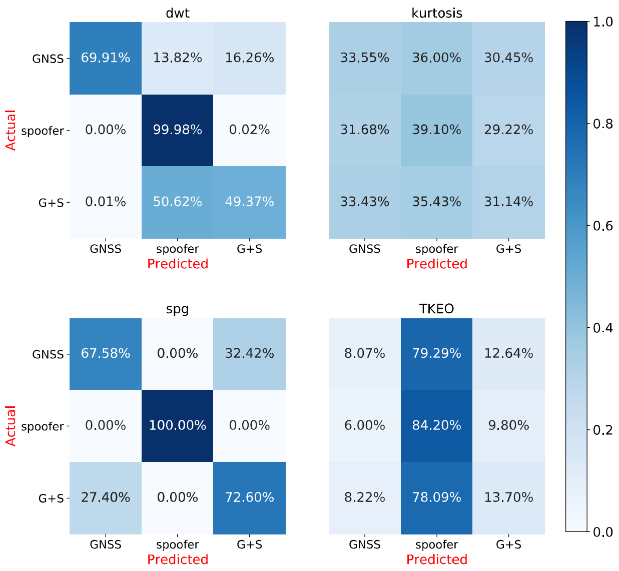


Fig. 7: The confusion matrix of pre-correlation methods for Nottingham measurements. The dwt, spg and TKEO are respectively short for discrete wavelet transform, spectrogram and teager kaiser energy operator. The 'G+S' denotes the mixture signals of GNSS and spoofer signals.

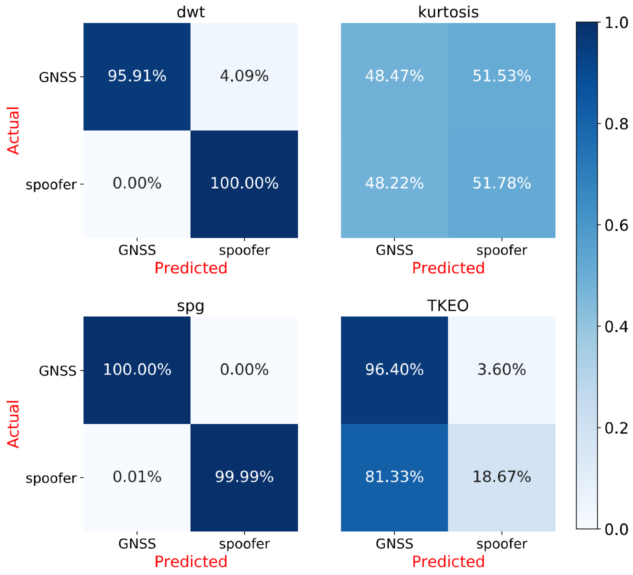


Fig. 8: The confusion matrix of pre-correlation methods for Nuremberg measurements.

other two scenarios. The reason of such differences may partly come also from the fact that the spoofer device was different in Tampere (Spectracom-based) compared to the spoofer device used in Nottingham and Nurember data (Spirent-based).

B. Classification with post-correlation data

We implemented two types of classifications, namely the benchmark comparison and the advanced comparison. In the benchmark comparison, we trained and tested the first two classes (pure GPS versus pure spoofer) that were defined at the beginning of this section. The benchmark comparison is only to validate whether we could differentiate the GPS signals from the spoofer signals by the post-correlation outputs in the supervised learning paradigm. In reality, the spoofer signals are supposed to be unknown, in other words, during the classifications we face a certain amount of data without prior label knowledge. To study the feasibility of machine learning methods on this situation, we further carried on an advanced comparison, that trained the classifier on the first two classes (pure GPS and pure spoofer) and tested on the third class (mixture of GPS and spoofer). Clearly, not all the signals from the third class have been learnt with a label, as we do not have exactly the same PRN codes in the three classes.

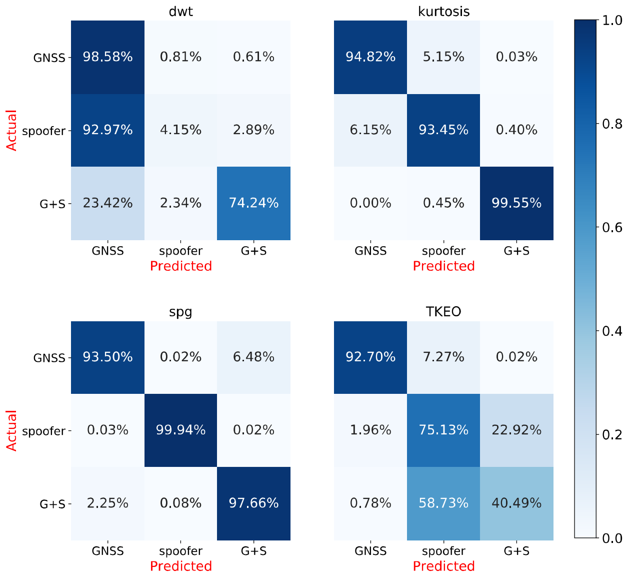
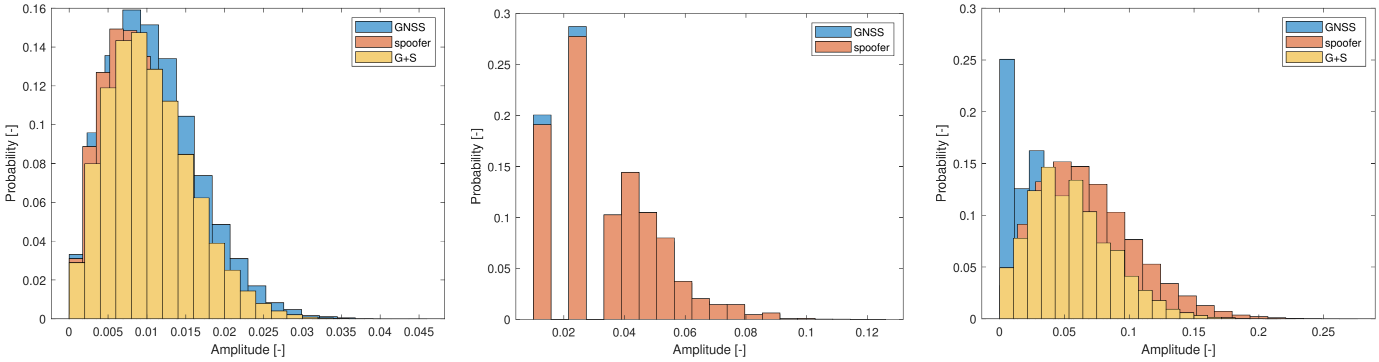


Fig. 9: The confusion matrix of pre-correlation methods for Tampere measurements.

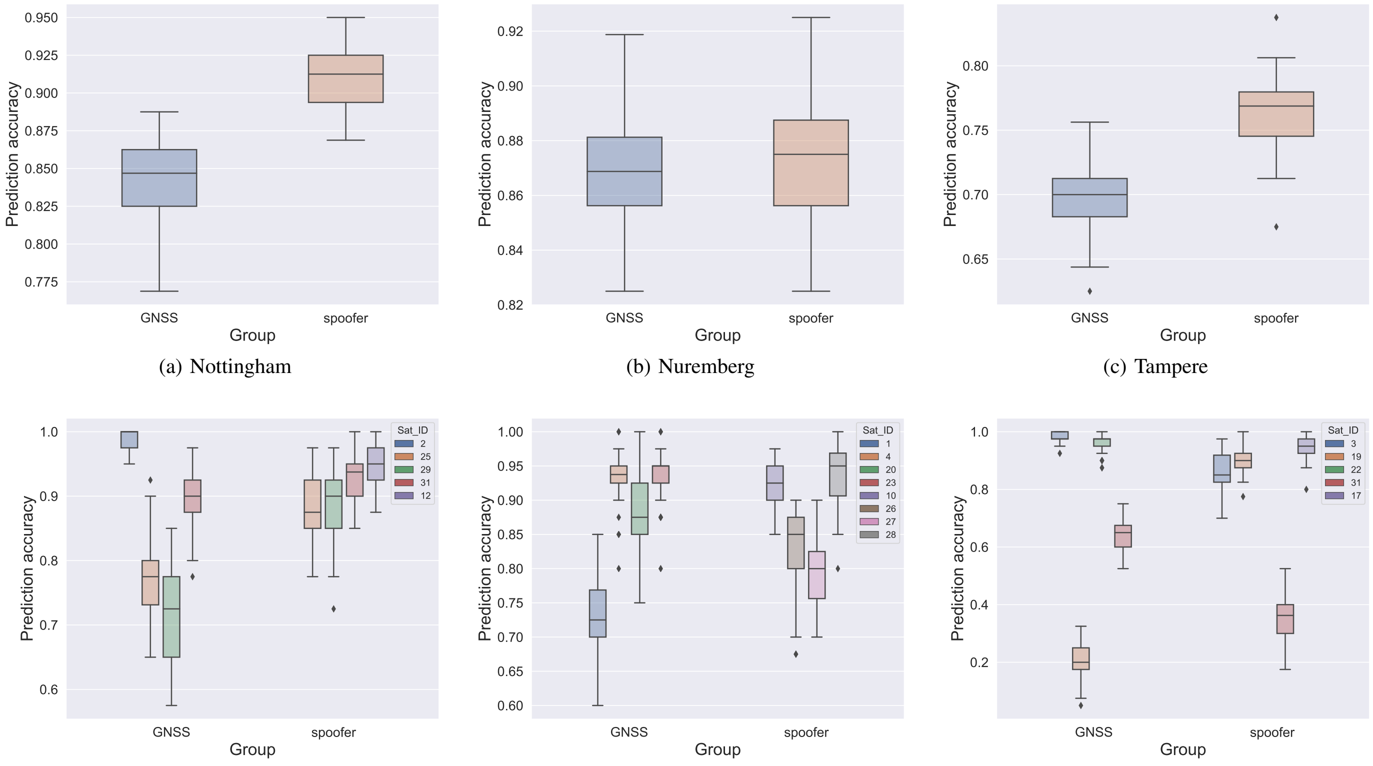
1) Benchmark comparison: We crop the outputs of post-correlation around the peak value and store them as image format. In this comparison, there are 500 images per signal to be trained, and 40 images per signal to be tested with total 50 Monte Carlo runs. 20 components for PCA process and RBF kernel for SVM are set in the machine learning, and the grid search is utilised for SVM parameters fine tuning. The mean values of prediction accuracy are shown in Table II, the details of prediction accuracy is indicated by boxplot in Fig. 11. Here within the testing data pool, we calculate the prediction accuracy of a certain signal sample being with this very signal label, whose association with the data sample is known to the classifier. In general, the combination of post-correlation transform and SVM works for all three measurements. In both Nottingham and Nuremberg measurements, the prediction accuracy is over 80%, which is a promising result. In the Fig. 11 (d)(e)(f), we could see that the worst classification scnario for Nottingham and Nuremberg measurements is as low as around 60% prediction accuracy. Whereas in the Tampere measurements, the lowest prediction accuracy is merely above 5%.

We also observe that, comparing the Tampere results with the Nottingham and Nuremberg results, there is a possible link between C/N_0 values in general and prediction accuracy: higher C/N_0 values –in both Nottingham and Nuremberg measurements compared to the Tampere measurements– lead



(a) Nottingham (b) Nuremberg (c) Tampere

Fig. 10: The histogram of I/Q samples' amplitude distribution.



(a) Nottingham (b) Nuremberg (c) Tampere

(d) Nottingham (e) Nuremberg (f) Tampere

Fig. 11: Prediction accuracy versus signals group for the benchmark comparison. The prediction accuracy of GNSS (or spoofer) being identified as the GNSS (or spoofer). (a)(b)(c) are the prediction accuracy of total GNSS (or spoofer) signals being identified as GNSS (or spoofer); (d)(e)(f) are the prediction accuracy of individual GNSS (or spoofer) signal being identified as GNSS (or spoofer).

TABLE II: Prediction results (mean value), benchmark case

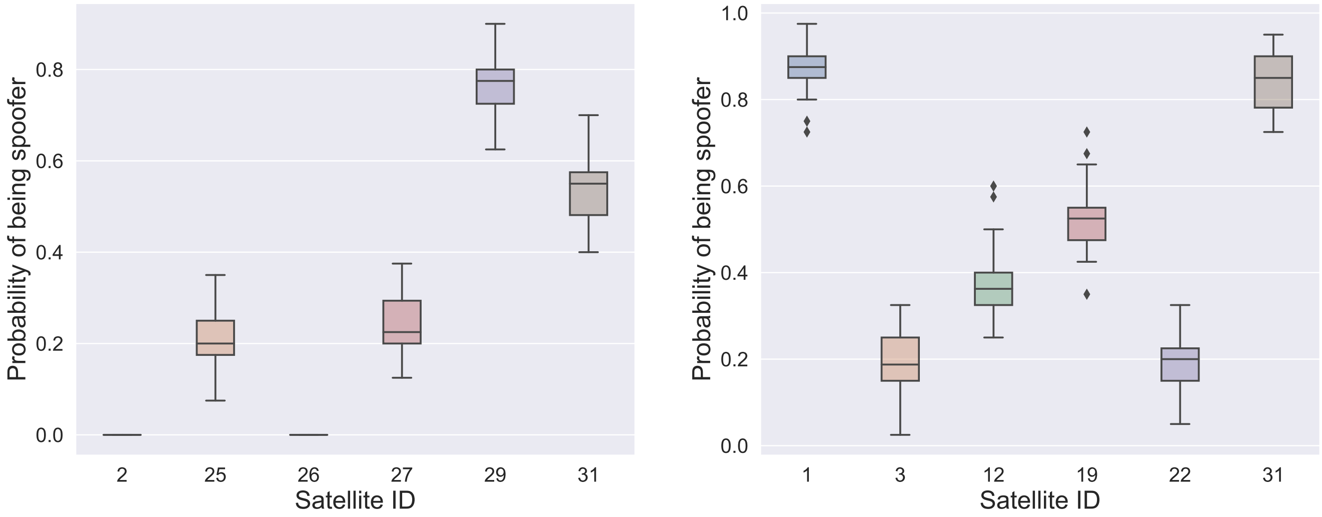
		Measurements		
		Nottingham	**Nuremberg**	**Tampere**
Prediction accuracy	**GNSS**	84.38%	87.05%	69.64%
	spoofer	91.06%	87.10%	76.34%

to a better prediction performance. This observation weakens the thought that it is the noise that dominates the difference between classes (in other words, it is again unlikely that the noise is the main differentiating factor, but rather the intrinsic hardware features at each transmitter). In the Nottingham measurements, satellite ID 25, 29 and 31 are present in both GNSS and spoofer classes, and the C/N_0 difference between GNSS and spoofer in satellite ID 25 and 29 is around 1 dB. In the Tampere measurements, satellite ID 3, 19 and 31 are present in both GNSS-only and spoofer-only scenarios, and the C/N_0 difference between GNSS and spoofer in satellite ID 19 and 31 is around 1 dB as well. We emphasize that

TABLE III: Prediction results (mean value), advanced comparison

		Measurements											
		Nottingham						**Tampere**					
Satellite ID		2	25	26	27	29	31	1	3	12	19	22	31
Probability	**GNSS**	100%	78.90%	100%	76.05%	23.75%	46.30%	13.15%	80.80%	62.50%	47.40%	80.45%	15.85%
	spoofer	0%	21.10%	0%	23.95%	76.25%	53.70%	86.85%	19.20%	37.50%	52.60%	19.55%	84.15%

[*] we marked the spoofer signal using blue colour.



(a) Nottingham

(b) Tampere

Fig. 12: Probability versus satellite ID for advanced comparison. In the Nottingham measurements, satellite ID 27 is spoofer signal; in the Tampere measurements, satellite ID 12 is spoofer signal.

the C/N_0 values are produced by our basic estimator, and therefore a small difference between two C/N_0 values can be seen as negligible. The results show that signals of satellite ID 25 and 29 in the Nottingham measurements have much better differentiation than signals of satellite ID 19 and 31 in the Tampere measurements, and these results imply that difference in noise levels do not have strong correlation with the prediction accuracy.

2) Advanced comparison: This comparison focuses on whether we could learn from the first two classes (i.e., do the training on GPS-only and spoofer-only classes) and perform classification on the third class, where both GNSS and spoofer signals are present (i.e., do classification on a third class which was not used in training). Due to the lack of the third class in Nuremberg measurements, we only perform this advanced comparison on the Nottingham and Tampere measurements. There are 1000 images per signal to be trained and 40 images per signal to be tested with total 50 Monte Carlo runs. The same machine learning setup from the previous sub-section of *Benchmark comparison* is applied here as well. In order to remove the spoofer signals, we have to include at least five 'satellite' signals in the testing data pool (i.e., assuming only one spoofer is in the mix). In this work, we used six 'satellite' signals in the testing phase. The results are shown in Table III and details are expressed using boxplot in Fig. 12.

Before we further analyse the results, the criteria of removing spoofer signals need to be set. Possible strategies are listed here:

1. Remove the signal with the highest probability being a spoofer;
2. Remove the signals with the probability of being a spoofer over a certain threshold;
3. Select the signals with the first four highest probability being GNSS;
4. Select the signals with the probability of being GNSS over a certain threshold.

Based on the current results shown in Table III, applying strategy (2) or (4) could remove the spoofer signal from the mixture; applying strategy (1) and (3) will keep the spoofer signal in the mixture. As a result, if we put our trust in the *advanced comparison* methods, we need complementary methods to form the PVT solution when not enough number of signals remain after spoofer's removal.

The *advanced comparison* scenario falls between supervised learning and unsupervised learning categories. The currently used supervised learning method (SVM) does not perform very well on the *advanced comparison*. A semi-supervised learning or unsupervised learning method (e.g., one-class SVM) needs to be investigated in the future work.

V. Conclusions and Way Forward

This work studied the RF fingerprinting in the GNSS context, for spoofer identification, with measurement-based signals. A generic diagram of a transmitter for GNSS signals was first proposed to identify the possible sources of RF fingerprints in the transmitter. A methodology for RF fingerprinting has been developed in this work with a clear definition of a conceptual 'classifier'. The RF fingerprinting concept was applied on measurements data, collected in Nottingham, Nuremberg, and Tampere. We proposed a flow chart of RF-fingerprinting-based anti-spoofing PVT solution combining pre- and post-correlation classifications results. Both the pre- and post-correlation classifications are capable of differentiating between GNSS and spoofer signals, with an average classification probabilities of spoofer versus GNSS up to 99.99% with pre-correlation data and up to 87.72% (i.e., Nottingham measurements) with post-correlation data. The lower classification accuracy with post-correlation data is explainable by the fact that post-correlation data offers a deeper distinction between classes than pre-correlation data (not only saying if spoofer is present or not, but also identifying the spoofing PRN codes) and by the fact that the correlator or despreader acts a smoother (or destroyer) of some features, and thus RF features are harder to be distinguished in the post-correlation domain than in the pre-correlation domain (due to the additional filtering stages).

The results so far are based on supervised learning (SVM algorithm), though in the *advanced comparison* with post-correlation data not all the associations between samples and labels are known to the classifier. The future work will concentrate on the following research questions: 1) are we able to classify RF fingerprints in GNSS with partial knowledge between samples and labels? 2) are we able to use this knowledge to perform RF fingerprinting in another location if we have knowledge of GNSS signal features in the measurements of one location?

The main identified challenges in RF fingerprinting in GNSS are: the highly demanding computational complexity with pre-correlation data (i.e, I/Q samples), the possible noise artifacts when spoofers have very different noise levels compared to GPS signals, the smoothing out of RF features in the post-correlation domain while the presented method is the only one possibility of post-correlation, and the need of a good C/N_0 level (e.g., higher than 45 dB-Hz) for reliable accuracy results.

While still in incipient phases, the RF fingerprinting in the context of GNSS holds good promises towards GNSS-signal authentication, especially when combined with additional authentication methods such as Open Service - Navigation Message Authentication (OSNMA) in Galileo or other PVT-based authentication methods.

Acknowledgment

This research was partly funded by the European Space Agency (ESA) in the project FINESSE ("Fingerprinting GNSS for authentication"). The opinions expressed herein reflect the authors' view only. Under no circumstances shall ESA be responsible for any use that may be made of the information contained herein. This work was also partly supported by the Academy of Finland, under the project ULTRA (328226). The Authors would also like to thank Tim Whitworth, formely at GMV-NSL, Andy McKeown at GMV-NSL, and Matti Ala-Poikela from TAU for their help in raw data collection.

References

[1] N. Soltanieh, Y. Norouzi, Y. Yang, and N. C. Karmakar, "A review of radio frequency fingerprinting techniques," *IEEE Journal of Radio Frequency Identification*, vol. 4, no. 3, pp. 222–233, 2020.

[2] D. Reising, J. Cancelleri, T. D. Loveless, F. Kandah, and A. Skjellum, "Radio Identity Verification-Based IoT Security Using RF-DNA Fingerprints and SVM," *IEEE Internet of Things Journal*, vol. 8, no. 10, pp. 8356–8371, 2021.

[3] W. Wang, I. Aguilar Sanchez, G. Caparra, A. McKeown, T. Whitworth, and E. S. Lohan, "A survey of spoofer detection techniques via radio frequency fingerprinting with focus on the gnss pre-correlation sampled data," *Sensors*, vol. 21, no. 9, 2021.

[4] N. S. Aminuddin, M. H. Habaebi, S. H. Yusoff, and M. R. Islam, "Securing wireless communication using RF fingerprinting," in *2021 8th International Conference on Computer and Communication Engineering (ICCCE)*, pp. 63–67, 2021.

[5] Fraunhofer IIS, "Flexiband USB Front-end." https://www.iis.fraunhofer.de/de/ff/lv/lok/gnss/simulationtest/flexiband.html/. [accessed 18.10.2021].

[6] M. Sun, L. Zhang, J. Bao, and Y. Yan, "Rf fingerprint extraction for gnss anti-spoofing using axial integrated wigner bispectrum," *Journal of Information Security and Applications*, vol. 35, pp. 51–54, 2017.

[7] Y. Jiang and Y. Xing, "Satellite spoofing identification method based on radio frequency feature extraction," *Journal of Physics: Conference Series*, vol. 1069, p. 012079, Aug. 2018.

[8] X. Zhu, T. Hua, F. Yang, G. Tu, and X. Chen, "Global positioning system spoofing detection based on support vector machines," *IET Radar, Sonar & Navigation*, Oct. 2021.

[9] "Ohb system ag- galileo -european satellite navigation system (space segment)." OHB brochure, https://www.ohb-system.de/files/images/mediathek/downloads/190603_OHB-System_Galileo_FOC-Satellites_2019-05.pdf, accessed 20.2.2021, 2021.

[10] NI Corp., "Global Synchronization and Clock Disciplining with NI USRP-293x Software Defined Radio." https://www.ni.com/fi-fi/innovations/white-papers/20/global-synchronization-and-clock-disciplining-with-ni-usrp-293x-.html, Oct. 2020.

[11] A. M. Ali, E. Uzundurukan, and A. Kara, "Assessment of features and classifiers for bluetooth rf fingerprinting," *IEEE Access*, vol. 7, pp. 50524–50535, 2019.

[12] M. Kose, S. Taşcioğlu, and Z. Telatar, "Rf fingerprinting of iot devices based on transient energy spectrum," *IEEE Access*, vol. 7, pp. 18715–18726, 2019.

[13] C. Bertoncini, K. Rudd, B. Nousain, and M. Hinders, "Wavelet fingerprinting of radio-frequency identification (rfid) tags," *IEEE Trans. on Industrial Electronics*, vol. 59, no. 12, pp. 4843–4850, 2012.

[14] T. Jian, B. C. Rendon, E. Ojuba, N. Soltani, Z. Wang, K. Sankhe, A. Gritsenko, J. Dy, K. Chowdhury, and S. Ioannidis, "Deep learning for rf fingerprinting: A massive experimental study," *IEEE Internet of Things Magazine*, vol. 3, no. 1, pp. 50–57, 2020.

[15] G. Reus-Muns and K. R. Chowdhury, "Classifying uavs with proprietary waveforms via preamble feature extraction and federated learning," *IEEE Trans. on Vehicular Techn.*, vol. 70, no. 7, pp. 6279–6290, 2021.

[16] W. Nie, Z.-C. Han, M. Zhou, L.-B. Xie, and Q. Jiang, "Uav detection and identification based on wifi signal and rf fingerprint," *IEEE Sensors Journal*, vol. 21, no. 12, pp. 13540–13550, 2021.

[17] E. D. Kaplan and C. Hegarty, *Understanding GPS/GNSS: principles and applications*. Artech House, 2017.

PUBLICATION

7

Location-Based Beamforming Architecture for Efficient Farming Applications with Drones

W. Wang, N. Okati, I. Tanash, T. Riihonen and E. S. Lohan

*2019 International Conference on Localization and GNSS (ICL-GNSS)*2019, 1–6
DOI: 10.1109/ICL-GNSS.2019.8752698

Location-based Beamforming Architecture for Efficient Farming Applications with Drones

Wenbo Wang, Niloofar Okati, Islam Tanash, Taneli Riihonen, and Elena-Simona Lohan
Faculty of Information Technology and Communication Sciences, Tampere University, Finland
Emails: {firstname.lastname}@tuni.fi

***Abstract*—This paper proposes a drone-based architecture with location-based beamforming (LBBF) and edge computing support for efficient crop harvesting and management in order to reduce the food waste in the food chain in farming applications. Monitoring the crop is a crucial part in the food chain. In this work, for monitoring purpose we consider synthetic aperture radar (SAR) mounted on the unmanned aerial vehicles (UAVs). In order to provide the edge computing information with good reliability, small latency and good throughput, we introduce a LBBF technique for the uplink connectivity. Firstly, the LBBF algorithm is proposed for the scenario where a single user is connected to the base station under analog beamforming scheme. Secondly, in the context of LBBF, we apply an optimization of the antenna size under the uniform rectangular array (URA) assumption. Thirdly, we implement a numerical analysis to compare LBBF with the traditional channel state information (CSI)-based beamforming. We show that the LBBF outperforms the CSI-based beamforming in the noisy environments according to the investigated performance metrics, namely the reliability of the connectivity and the capacity. In addition, the LBBF also has smaller latency than CSI-based beamforming.**

***Index Terms*—Farming, location-based beamforming (LBBF), unmanned aerial vehicles (UAVs)**

I. Introduction

As the world's population is predicted to reach nearly nine billion people by 2050 according to the Food and Agriculture Organization of the United Nations, 70% more food production will be needed despite only 5% more land could be used. To cope with this reality, the agriculture industry must adopt new technologies in order to meet the increasing demand for food. Maximizing crop yield and minimizing food losses are the main goals of any agricultural community especially that one third of the food produced in the world gets lost or wasted. A new significant move in today's modern farming is the use of unmanned aerial vehicles (UAVs), i.e., 'drones', which can be used when combined with remote sensors to determine crop progress as well as crop deficiencies and the presence of disease and water monitoring.

Due to above mentioned objectives, there is a need for timely and reliable images to keep track of the agricultural predictions, crop health, and to make decisions to maximize the crop yield. Synthetic aperture radar (SAR) is a type of radar which is used for imaging. It utilizes the relative motion of the radar antenna over an observing target region [1]. The capability of SAR to provide imaging, even during the night time and through fog coat, has made it an important tool for remote sensing applications, i.e., land and crop monitoring in agriculture [2].

Usually, SAR is mounted on traditional aerial systems, e.g., aircrafts and helicopters which are very expensive. Hence, using SAR technology with drones will reduce the costs and resources. Moreover, improving the performance metrics in a drone network can lead to better image quality.

In this paper, we propose a drone-based architecture for efficient farming in Fig. 1. A monitoring drone patrols the fields according to scheduled scan route, for each time instant it reports to the edge computing node, which is located in the warehouse. The automated fleet vehicles operate coordinately by listening to the edge computing node. The base stations here plays a role as a bridge to build connections among monitoring drones, automated fleet vehicles and the edge computing node. The monitoring drone carries many duties, for example, the fire alarm, the notice of maturity etc. The automated fleet vehicles are assigned to each field, for example, to harvest, by following orders given by the edge computing node. The edge computing node processes the data collected by monitoring drones, automated fleet vehicles etc. The machine learning techniques are applied in the edge computing node. It also gives orders to drones and vehicles in the networks. Some of these applied scenarios are in great need of good communication qualities, such as high reliability and high data rate (or capacity).

Nowadays, the location information of drones is available for acquisition all the time. This fact makes the implementation of the location-based beamforming very convenient and efficient, comparing with the CSI-based beamforming and the codebook-based beamforming. Our proposed efficient farming architecture has high demand of communication qualities, namely high reliability, high capacity and low latency. Among CSI-based beamforming, codebook-based beamforming and location-based beamforming, in 'noisy' environment, good reliability and capacity could be achieved by codebook-based beamforming and location-based beamforming, while low latency could only be reached by location-based beamforming. Therefore, the LBBF becomes a good candidate in our considerations.

Many articles discuss the benefits from the location information in communications, [3] investigates multi-connected Industrial Internet of Things (IIoT) devices under 28 GHz operating frequency, and concludes that with the usage of location information the data rate is improved. [4] points out that in the ultra-dense networks (UDNs), the capacity metric of the location-based beamforming outperforms that in the full-band CSI based beamforming. [5] compares the full CSI based

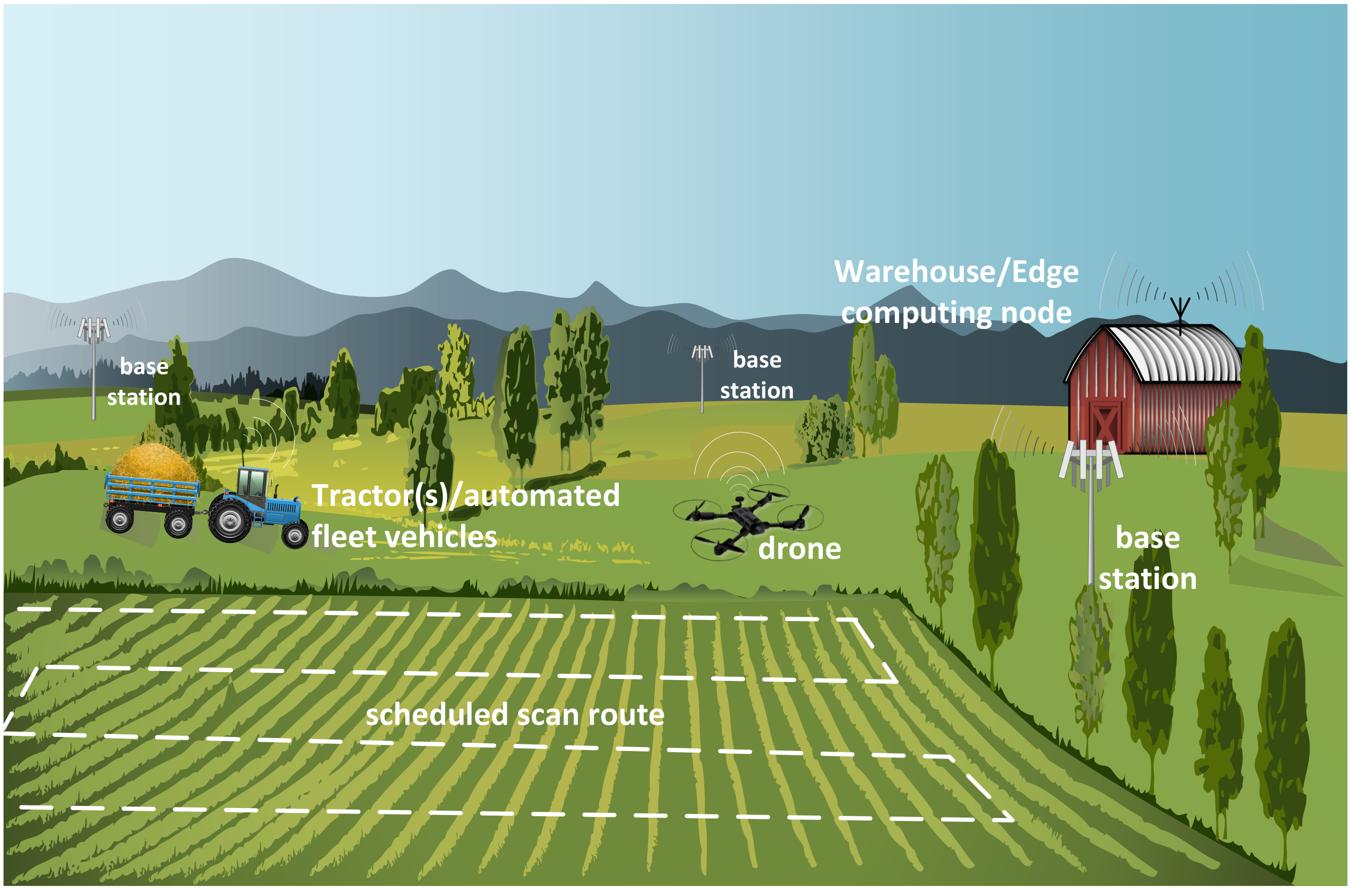

Warehouse/Edge computing node
base station
base station
base station
Tractor(s)/automated fleet vehicles
drone
scheduled scan route

Fig. 1. An example of the drone-based architecture for efficient farming. The drone moves according to the scheduled scan route, it reports to the edge computing node all the time. The location-based beamforming technique is applied in the current architecture. The tractor reports to the edge computing node as well.

beamforming with position aided beamforming, achieving the similar performance the position aided beamforming needs fewer pilot signals than the full CSI based beamforming.

The following sections are organized as: Section II proposes a location-based beamforming algorithm for scenarios with uplink, analog beamforming scheme and single user. In order to have a good performance in LBBF, an optimization of uniform rectangular array (URA) is implemented in Section II-B. Section III applied several numerical analysis in the comparisons between LBBF and CSI-based beamforming, different location errors, different pilot symbols (i.e., for the purpose of estimating the channel state), together with metrics like outage probability, capacity and latency are discussed. Section IV concludes this work and discusses the future possibilities.

II. Location-based Beamforming for Drone-based Farming Architecture

Based on the architecture shown in Fig. 1, we consider the uplink transmission, a single drone moving according to the scheduled scan route and analog beamforming structure. We first propose an algorithm for location-based beamforming and then, in Section II-B, we implement a weak optimization of designing URA in terms of array size.

A. Algorithm for Location-based Beamforming

In the location-based beamforming, a few assumptions have been considered beforehand,

- The location information of the user is available at each time instant (e.g., the GNSS receiver mounted on the user device provide the location information),
- The location information of the ground base station is available at each time instant (e.g., via the GNSS positioning),
- The tracking algorithm could be performed in the ground base station, such that the base station predicts the location of user for the next time instant.

Under the above assumptions, we propose a simple implementation procedure for the location-based beamforming in Algorithm 1. The location-based beamforming in Algorithm 1 concerns single user connection in the uplink communication, the analog beamforming scheme is applied. However, it could be easily modified to work in the downlink communication,

Algorithm 1 Location-based beamforming (uplink, analog beamforming, single user)

```
Require: initial location of the user (drone) $[x_0, y_0, z_0]$, the
    location of connected base station $[x_{\mathrm{BS}}, y_{\mathrm{BS}}, z_{\mathrm{BS}}]$
    set the steering angle of base station towards to the initial
    location of the user $[x_0, y_0, z_0]$;
    for t=1:T do
        1. the base station implements a tracking algorithm to
        predict the location of the user at the next time instant
        $[\tilde{x}_{\mathrm{t}}, \tilde{y}_{\mathrm{t}}, \tilde{z}_{\mathrm{t}}]$, and adjust the steering angle accordingly;
        2. adapt the tracking algorithm with the new incoming
        location information $[x_{\mathrm{t}}, y_{\mathrm{t}}, z_{\mathrm{t}}]$,
    end for
```

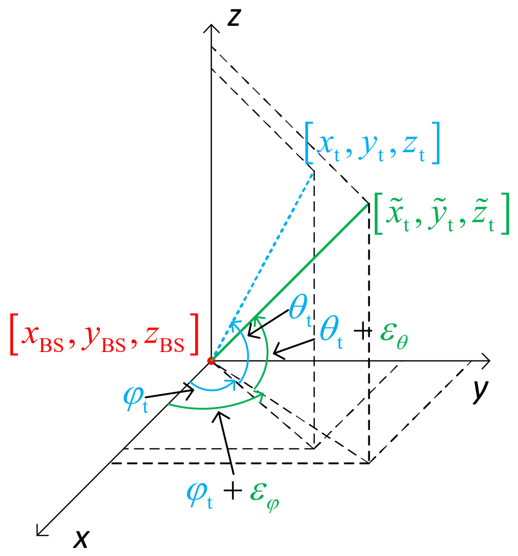

z
$[x_t, y_t, z_t]$
$[\tilde{x}_t, \tilde{y}_t, \tilde{z}_t]$
$[x_{BS}, y_{BS}, z_{BS}]$
θ_t
$\theta_t + \varepsilon_\theta$
φ_t
y
$\varphi_t + \varepsilon_\varphi$
x

Fig. 2. The angle difference between steering direction and the user direction. At time instant t, φ_{t} is the azimuth angle, θ_{t} is the elevation angle, $[x_{\mathrm{BS}}, y_{\mathrm{BS}}, z_{\mathrm{BS}}]$ is the location of the base station, $[x_{\mathrm{t}}, y_{\mathrm{t}}, z_{\mathrm{t}}]$ is the location of the user, $[\tilde{x}_{\mathrm{t}}, \tilde{y}_{\mathrm{t}}, \tilde{z}_{\mathrm{t}}]$ is the predicted location of the user. ε_φ is the angle difference in the azimuth angle, ε_θ is the angle difference in the elevation angle.

for the multi-user cases, we recommend hybrid beamforming schemes.

B. Optimization of Uniform Rectangular Array

In beamforming techniques, particularly under narrow beam situations, one factor that significantly affects the gain of the antenna array is the angle difference between steering direction and the user direction. Fig. 2 shows the angle difference, $[x_{\mathrm{t}} - x_{\mathrm{BS}}, y_{\mathrm{t}} - y_{\mathrm{BS}}, z_{\mathrm{t}} - z_{\mathrm{BS}}]$ is user direction, $[\tilde{x}_{\mathrm{t}} - x_{\mathrm{BS}}, \tilde{y}_{\mathrm{t}} - y_{\mathrm{BS}}, \tilde{z}_{\mathrm{t}} - z_{\mathrm{BS}}]$ is the steering direction. We rewrite $\theta_{\mathrm{t}} + \varepsilon_\theta$ as $\tilde{\theta}_{\mathrm{t}}$, $\varphi_{\mathrm{t}} + \varepsilon_\varphi$ as $\tilde{\varphi}_{\mathrm{t}}$.

In order to provide the optimal size of URA size, we define two metric: instant directivity $D_{\tilde{\theta}_{\mathrm{t}},\tilde{\varphi}_{\mathrm{t}}}(\theta_{\mathrm{t}}, \varphi_{\mathrm{t}})$ and directivity ratio $R_{\mathrm{L,M,N}}$. L, M, N in $R_{\mathrm{L,M,N}}$ denotes the number of antenna elements in X-axis, Y-axis and Z-axis respectively.

Considering a URA with the identical isotropic antenna elements and half-wavelength inter-element spacing, the instant directivity is,

$$D_{\tilde{\theta}_{\mathrm{t}},\tilde{\varphi}_{\mathrm{t}}}(\theta_{\mathrm{t}}, \varphi_{\mathrm{t}}) = \frac{4\pi |AF_{\tilde{\theta}_{\mathrm{t}},\tilde{\varphi}_{\mathrm{t}}}(\theta_{\mathrm{t}}, \varphi_{\mathrm{t}})|^2}{\int_0^{2\pi}\int_0^{\pi} |AF_{\tilde{\theta}_{\mathrm{t}},\tilde{\varphi}_{\mathrm{t}}}(\theta, \varphi)|^2 \cos\theta \mathrm{d}\theta \mathrm{d}\varphi} \tag{1}$$

where $AF_{\tilde{\theta}_{\mathrm{t}},\tilde{\varphi}_{\mathrm{t}}}(\theta_{\mathrm{t}}, \varphi_{\mathrm{t}})$ is the array factor at $(\tilde{\theta}_{\mathrm{t}}, \tilde{\varphi}_{\mathrm{t}})$ steering angle and yields to,

$$AF_{\tilde{\theta}_{\mathrm{t}},\tilde{\varphi}_{\mathrm{t}}}(\theta_{\mathrm{t}}, \varphi_{\mathrm{t}}) = \frac{\sin(\frac{L}{2}\alpha)\sin(\frac{M}{2}\beta)\sin(\frac{N}{2}\gamma)}{LMN\sin(\frac{1}{2}\alpha)\sin(\frac{1}{2}\beta)\sin(\frac{1}{2}\gamma)} \tag{2}$$

where α, β and γ are

$$\begin{cases} \alpha = \pi\big(\cos\theta_{\mathrm{t}}\cos\varphi_{\mathrm{t}} - \cos\tilde{\theta}_{\mathrm{t}}\cos\tilde{\varphi}_{\mathrm{t}}\big) \\ \beta = \pi\big(\cos\theta_{\mathrm{t}}\sin\varphi_{\mathrm{t}} - \cos\tilde{\theta}_{\mathrm{t}}\sin\tilde{\varphi}_{\mathrm{t}}\big) \\ \gamma = \pi\big(\sin\theta_{\mathrm{t}} - \sin\tilde{\theta}_{\mathrm{t}}\big) \end{cases} \tag{3}$$

The directivity ratio is

$$R_{\mathrm{L,M,N}} = \frac{D_{\tilde{\theta}_{\mathrm{t}},\tilde{\varphi}_{\mathrm{t}}}(\theta_{\mathrm{t}}, \varphi_{\mathrm{t}})}{D_{\tilde{\theta}_{\mathrm{t}},\tilde{\varphi}_{\mathrm{t}}}(\tilde{\theta}_{\mathrm{t}}, \tilde{\varphi}_{\mathrm{t}})} \tag{4}$$

combining (1) and (4), the latter reduces to

$$R_{\mathrm{L,M,N}} = |AF_{\tilde{\theta}_{\mathrm{t}},\tilde{\varphi}_{\mathrm{t}}}(\theta_{\mathrm{t}}, \varphi_{\mathrm{t}})|^2 \tag{5}$$

The instant directivity shows the gain that the user could actually achieve, under mismatch between user direction and steering direction. The directivity ratio shows how far it is from the achieved gain to the radiated gain. If the instant directivity values of two different size URA are very close, the one with higher directivity ratio is preferable. That is, a high directivity ratio reflects that a good usage of current antenna array is achieved. The high value of instant directivity is welcomed, however it should be achieved together with relatively good directivity ratio. We need to prevent the signal falling into the minor lobes, since the low directivity ratio might imply the radiation from the minor lobes.

In order to obtain the optimal URA size for certain angle errors, we applied a numerical analysis based on the parameters in Table I, the URA antenna elements are mounted on the X-Y plane.

TABLE I
PARAMETERS OF NUMERICAL ANALYSIS IN URA SIZE OPTIMIZATION

Parameters	**Values**
URA size	$2^n \times 2^n \quad (n = 1, 2, 3, \cdots)$
Angle errors	$2^\circ/5^\circ$
Carrier frequency	1.9 GHz

Fig. 3 shows the average instant directivity $D_{\tilde{\theta}_{\mathrm{t}},\tilde{\varphi}_{\mathrm{t}}}(\theta_{\mathrm{t}}, \varphi_{\mathrm{t}})$ over $[-\pi/2, \pi/2]$ elevation and $[-\pi, \pi]$ azimuth. In both the elevation and azimuth, we apply the same angle error. At 2° angle error, the average instant directivity reaches its maximum with 32×32 URA size. While at 5° angle error, the average instant directivity reaches its maximum with 8×8 URA size.

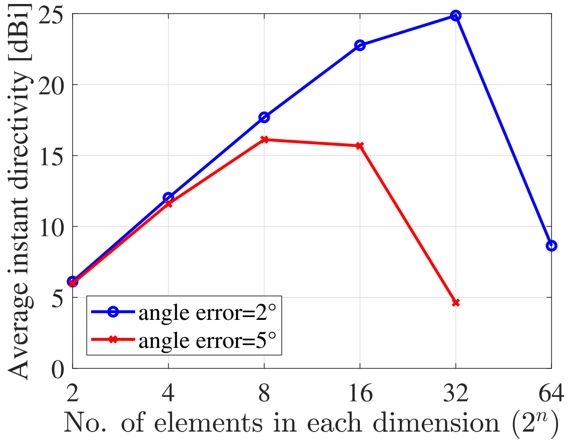


Fig. 3. The average instant directivity (unit:dBi) over $[-\pi/2, \pi/2]$ elevation and $[-\pi, \pi]$ azimuth. The same angle error value applies to both elevation angle error and azimuth angle error. Total number of antenna elements is $2^n \times 2^n$.

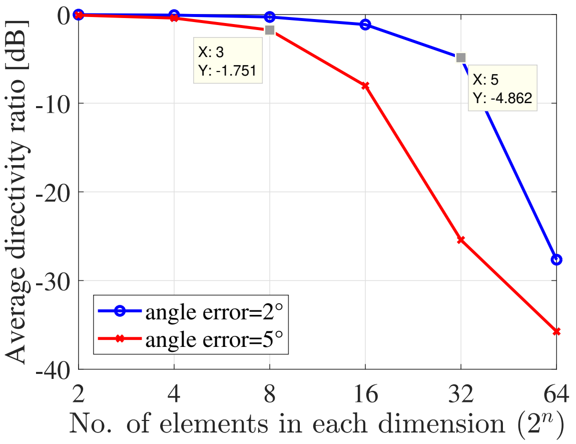


Fig. 4. The average directivity ratio (unit:dB) over $[-\pi/2, \pi/2]$ elevation and $[-\pi, \pi]$ azimuth. The same angle error value applies to both elevation angle error and azimuth angle error. Total number of antenna elements is $2^n \times 2^n$.

Fig. 4 shows the average directivity ratio $R_{\mathrm{L,M,N}}$ over $[-\pi/2, \pi/2]$ elevation and $[-\pi, \pi]$ azimuth. At 2° angle error, the average directivity ratio is $-4.862\,\mathrm{dB}$ with 32×32 URA size. At 5° angle error, the average directivity ratio is $-1.751\,\mathrm{dB}$ with 8×8 URA size. As the rule of thumb, the side lobe level is more than 10 dB smaller than the main lobe level. Therefore, at 2° angle error with 32×32 URA size, signals could achieve the highest gain (among all the possible $2^n \times 2^n$ URA size) without falling into the radiation of minor lobes; at 5° angle error with 8×8 URA size, signals as well achieve the highest gain without falling into the radiation of minor lobes.

III. Comparison of Beamforming Techniques

Using time division duplex (TDD) scheme, we compare the location-based beamforming with the CSI-based beamforming and the no beamforming cases.

A. Performance Metrics

The comparisons are based on performance metrics, namely the outage probability and capacity. In [6], the outage probability P_{out} is defined as,

$$P_{\mathrm{out}} = Pr(PL \geq P_{\mathrm{T}} + G_{\mathrm{T}} - L_{\mathrm{T}} + G_{\mathrm{R}} - L_{\mathrm{R}} - P_{\mathrm{R_{min}}}) \quad (6)$$

where PL is the path loss, P_{T} is the transmitted power, G_{T} is the gain in the transmitter, L_{T} is the loss in the transmitter, G_{R} is the gain in the receiver, L_{R} is the loss in the receiver, $P_{\mathrm{R_{min}}}$ is the receiver sensitivity, all the parameters mentioned here are in dB/dBi.

The data capacity C is defined as [6],

$$C = \eta B_W \log_2(1 + \mathrm{SNR}) \quad (7)$$

where $0 < \eta < 1$ is the efficiency factor, B_W is the signal bandwidth (unit: Hz), SNR is signal-to-noise ratio in linear scale. The SNR in decibel scale is given in (8),

$$\mathrm{SNR} = P_{\mathrm{R}} + 174 - 10\log_{10}(B_W) - \mathrm{NF} \quad (8)$$

where P_{R} is the received power (unit: dB), NF is the noise figure (unit: dB) in the receiver.

B. Numerical Analysis

The simulation scenario is based on the Fig. 1. The monitoring drone scans a $400\,\mathrm{m} \times 300\,\mathrm{m}$ rectangular area, one base station is employed and placed at the X-Y plane origin (i.e., $[0, 0, 35]$ in the Cartesian coordinate system, 35 is the height of the base station) of the simulation area. We use the DJI Mavic 2 Enterprise [7] as the reference, the maximum effective isotropic radiated power (EIRP) of Mavic 2 Enterprise is 26 dBm, EIRP is defined as,

$$\mathrm{EIRP} = P_{\mathrm{T}} + G_{\mathrm{T}} - L_{\mathrm{T}} \quad (9)$$

The maximum ascent velocity is 4 m/s, the maximum descent velocity is 3 m/s, the cruise velocity is 13 m/s, the cruise altitude is 52 m. Fig. 5 is the simulated scan route of the monitoring drone, our numerical analysis is based on this movement pattern.

In the simulation of CSI-based beamforming, we use 300 (and 1000) Binary Phase Shift Keying (BPSK) modulated uplink pilot symbols to estimate uplink channel (i.e., to estimate the angle of arrival (AoA) of incoming signal). It is assumed that the pilot symbols are ahead of signals of interest, using the channel state information the pilot symbols carried, the antenna array adjusts the steering angle to receive the signals of interest. The signal scheme in this simulation is indicated in Fig. 6.

In the simulation of location-based beamforming, it is assumed the locations of the drone are scheduled, location errors occur due to the air turbulence of the drone. In other words, the base station knows the location of the drone for each time instant, however the true locations of the drone under air turbulence are unknown.

During the comparison analysis, the quasi-LTE uplink parameters are used. Besides, two location error cases (small

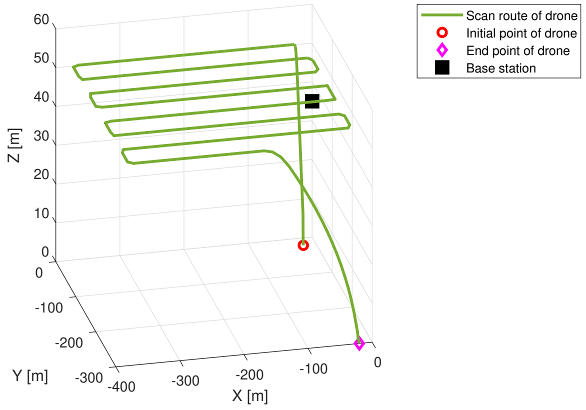


Fig. 5. The scan route of monitoring drone. The red circle is the initial point, the magenta diamond is the end point, the black filled square is the position of the base station.

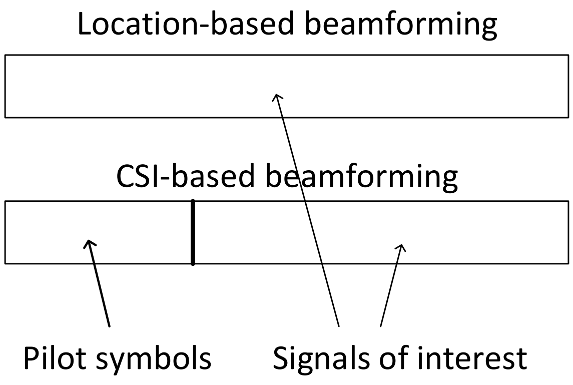


Fig. 6. The signal scheme in location-based beamforming and CSI-based beamforming.

TABLE II
PARAMETERS OF NUMERICAL ANALYSIS IN COMPARISONS BETWEEN LB BEAMFORMING AND CSI-BASED BEAMFORMING TECHNIQUES

Parameters	**Values**
Location errors	$\mathcal{N}(0, 0.1^2)$ and $\mathcal{N}(0, 2^2)$ [m]
Channel SNR	-5 dB, 'noisy' channel
Channel noise	$\mathcal{CN}(0, 1)$ (linear scale)
Interference	N/A
Carrier frequency	1.9 GHz, band #33
No. pilot symbols	300 and 1000
Pilot symbols	BPSK symbols
URA size	16 × 16 on X-Y plane
Base station receiver loss L_{R}	4 dB
Base station noise figure NF	5 dB
Uplink bandwidth B_{W}	1 MHz
Efficiency factor η	0.7
Path loss model	3GPP Rural Macro (RMa) [8]
Average building height	15 m
Average street width	10 m
Maximum ascent velocity of drone	4 m/s
Maximum descent velocity of drone	3 m/s
Cruise velocity of drone	13 m/s
Cruise altitude of drone	52 m

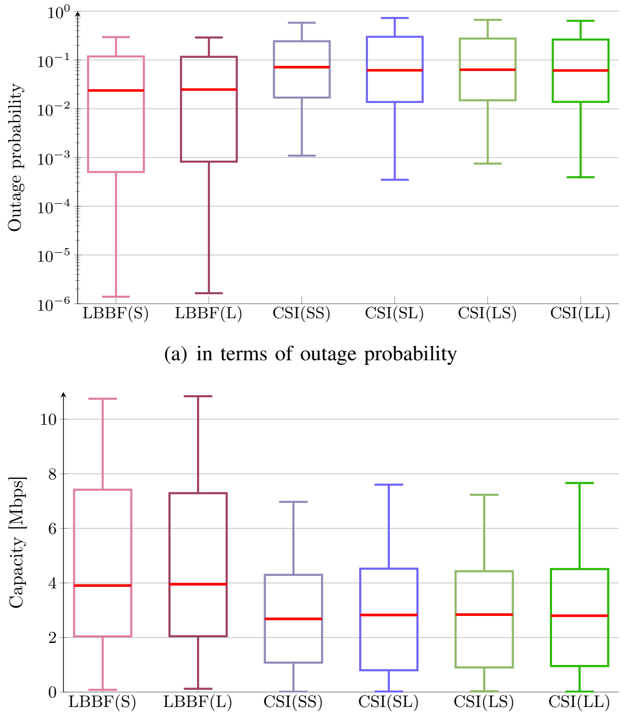
air turbulence versus large air turbulence), 'noisy' channel situation and two number of pilot symbols (large number of pilots versus small number of pilots) are studied. By considering a reasonable angle error range (i.e., from 2° to 5°), we choose 16 × 16 URA. The details of parameters in simulation see Table II.

We analyze the outage probability and the capacity for the entire route in Fig. 5 in the uplink. For each time instant during the route, the outliers are determined by considering 10% of total data are outliers.

Figure 7(a) presents the the outage probability comparisons between LBBF and CSI-based beamforming. Under the optimal size of URA antenna array, the location errors have no significant effects on the reliability. As Fig. 7(a) shows the outage probability comparisons in CSI-based beamforming between 300 and 1000 pilot symbols, we could tell that in the 'noisy' environment, the reliability of the CSI-based beamforming varies little, though large number of pilot symbols applied. The reliability of LBBF does not suffer from the channel noise level, therefore, in the 'noisy' environments, the LBBF outperforms the CSI-based beamforming in terms of outage probability.

Figure 7(b) shows the capacity comparisons between LBBF and CSI-based beamforming. Even though the introduction of the karge location errors, the capacity metrics in LBBF is still larger than that in CSI-based beamforming, the median values in LBBF are about 1.5 Mbps greater than that in CSI-based beamforming. Fig. 7(b) also shows the capacity comparisons in CSI-based beamforming between 300 and 1000 pilot symbols. Similar results like Fig. 7(a), the CSI-based beamforming is vulnerable to the channel noise, in the 'noisy' environment, large number of pilot symbols will not significantly improve the capacity performance. Therefore, in the 'noisy' environment, the LBBF provides better capacity than the CSI-based beamforming.

In noisy environment, the LBBF shows better performance in both reliability and capacity metrics than CSI-based beamforming. Besides, for the incoming signals, due to collecting large number of pilots to estimate AoA (i.e., Fig.6), the CSI-based beamforming has disadvantages in latency performance. If we denote symbol rate of pilot symbols as R_{sym} symbol/s, in our study, the CSI-based beamforming is $300/R_{\mathrm{sym}}$ seconds delayed with 300 pilot symbols; $1000/R_{\mathrm{sym}}$ seconds delayed with 1000 pilot symbols.



(a) in terms of outage probability

(b) in terms of capacity

Fig. 7. Performance comparison between location-based beamforming (LBBF) and CSI-based beamforming. The LBBF(S) is the LBBF under location errors $\sigma^2 = 0.01$, the LBBF(L) is the LBBF under location errors $\sigma^2 = 4$, the CSI(SS) is the CSI-based beamforming using 300 pilot symbols under location errors $\sigma^2 = 0.01$, the CSI(SL) is the CSI-based beamforming using 1000 pilot symbols under location errors $\sigma^2 = 0.01$, the CSI(LS) is the CSI-based beamforming using 300 pilot symbols under location errors $\sigma^2 = 4$, the CSI(LL) is the CSI-based beamforming using 1000 pilot symbols under location errors $\sigma^2 = 4$. The channel SNR is $-5\,$dB.

IV. Conclusions and Future Work

We proposed a drone-based architecture for efficient farming. This paper focuses on the study how much the location-based beamforming technique improves the communication qualities hence benefits the efficient farming applications. From our study, in order to achieve high directivity in LBBF, 32×32 URA is recommended when the angle errors (in both elevation and azimuth) are around to 2°, 8×8 URA is recommended when the angle errors are around 5°. In the 'noisy' environments, comparing with the CSI-based beamforming, the LBBF shows advantage in terms of reliability and capacity, besides the LBBF naturally has smaller latency than the CSI-based beamforming. Therefore, the LBBF is a good candidate technique to be employed in the proposed efficient farming architecture.

The efficient farming is a very big picture, in this paper we only discussed a small piece of this application. In the future, we will discuss the choice of sensors mounted on the drone, for example, the multi-spectral cameras is also a good candidate, and a well designed unsupervised machine learning algorithm needs to be proposed to process the collected data from the sensors.

Acknowledgement

This work was supported by the Academy of Finland project 313039.

References

[1] J. Curlander, R. McDonough, and S. A. Radar, "Systems & Signal Processing", A Wiley-Interscience publication, J," *Kong Editor*, 1991.

[2] V. C. Koo, Y. K. Chan, V. Gobi, M. Y. Chua, C. H. Lim, C. S. Lim, C. Thum, T. S. Lim, Z. Ahmad, K. A. Mahmood, *et al.*, "A new unmanned aerial vehicle synthetic aperture radar for environmental monitoring," *Progress In Electromagnetics Research*, vol. 122, pp. 245–269, 2011.

[3] E. S. Lohan, M. Koivisto, O. Galinina, S. Andreev, A. Tolli, G. Destino, M. Costa, K. Leppanen, Y. Koucheryavy, and M. Valkama, "Benefits of Positioning-Aided Communication Technology in High-Frequency Industrial IoT," *IEEE Communications Magazine*, vol. 56, no. 12, pp. 142–148, 2018.

[4] P. Kela, M. Costa, J. Turkka, M. Koivisto, J. Werner, A. Hakkarainen, M. Valkama, R. Jantti, and K. Leppanen, "Location based beamforming in 5G ultra-dense networks," in *2016 IEEE 84th Vehicular Technology Conference (VTC-Fall)*, pp. 1–7, IEEE, 2016.

[5] M. Koivisto, A. Hakkarainen, M. Costa, P. Kela, K. Leppanen, and M. Valkama, "High-efficiency device positioning and location-aware communications in dense 5G networks," *IEEE Communications Magazine*, vol. 55, no. 8, pp. 188–195, 2017.

[6] W. Wang and E. S. Lohan, "Applicability of 3GPP Indoor Hotspot Models to the Industrial Environments," in *2018 8th International Conference on Localization and GNSS (ICL-GNSS)*, pp. 1–5, IEEE, 2018.

[7] "Mavic 2 Enterprise Specification." https://www.dji.com/fi/mavic-2-enterprise/info, 2019. [Online; accessed 04-Mar.-2019].

[8] 3GPP- Technical Specification Group Radio Access Network, "Study on 3d channel model for lte (release 12)." 3GPP TR 36.873 V12.7.0 (2018-01-05), 2018. [Online; accessed 04-Mar.-2019].

PUBLICATION

8

Converging Radar and Communications in the Superposition Transmission
W. Wang, B. Tan, E. S. Lohan and M. Valkama

*2021 17th International Symposium on Wireless Communication Systems (ISWCS)*2021, 1–6
DOI: 10.1109/ISWCS49558.2021.9562169

Converging Radar and Communications in the Superposition Transmission

Wenbo Wang*, Bo Tan*, Elena Simona Lohan*, Mikko Valkama*,
**Faculty of Information Technology and Communication Sciences*, Tampere University, Finland
{wenbo.wang, bo.tan, elena-simona.lohan, mikko.valkama}@tuni.fi

Abstract—**This paper proposes a superposition transmission scheme for the future Radio Frequency (RF) convergence applications. The scheme is discussed under the assumption of a mono-static broadcasting channel topology. Under communications quality-of-service (QoS) constraints, the joint performance region of communications sum rate and radar estimation error variance is studied. Two radar signal waveforms, namely linear FM and parabolic FM, are used to investigate how signal shapes may influence the estimation accuracy. Both waveforms are generated with rectangular envelope. In the end, a numerical analysis is applied, which concludes that a moderate communications QoS promises a good communications fairness while with the limited radar performance degradation.**

Index Terms—**joint radar and communications, superposition transmission, power domain, RF convergence, co-design**

I. Introduction

The booming wireless communication applications bring the need for more radio emitters and more spectrum resources, meanwhile causing a spectral congestion problem with legacy radar systems. At the same time, emerging applications, such as connected autonomous vehicles (CAV) and autonomous drones and robots, urge that the radio sensing and communications functions taking place in the common spectrum simultaneously. The above reasons drive the research on the convergence of two radio frequency (RF) systems when sensing and communication tasks will co-exist and be tackled in a joint manner. According to Bliss *et al.* in [1] and [2], the RF convergence can be categorised into three integration levels: **coexistence**, **cooperation** and **co-design**. In the coexistence level, radar and communication signal sources do not share any *a priori* information and consider the signal from the counter party as interference. In the cooperation level, a certain level of knowledge is shared between the radar and communications systems for a more effective interference cancellation. In the co-design level, the radar and the communication systems are designed from sketch for mutual/common benefits and by maximizing the use of spectral, time, and spatial resources.

In order to develop a highly integrated RF convergence system, the current research works often target to coordinate the signals in frequency, time, or spatial dimensions. The co-design in time domain can be traced back to 1960s, when pulse interval modulation (PIM) was proposed for embedded information on the radar pulses [3]. In the frequency domain, the orthogonal frequency-division multiplexing (OFDM) waveform is often used for the dual-function design. In [4], authors demonstrated a vehicle detection function, which was implemented based on the OFDM communications signal. The recent research work in [5] embraces the full-duplex circuit, which reduces the direct signal leakage and enables the detection of reflected Long-Term Evolution (LTE) and 5G New Radio (NR) OFDM signals from the drones and vehicles. In the spatial domain, multiple-input and multiple-output (MIMO), generalized to both phase coherent and spatial independent antenna arrays, is the main instrument to achieve the RF convergence. MIMO provides a high degrees-of-freedom (FoD) to differentiate and reduce the mutual interference between communications user and radar target by applying transmitting/receiving beamforming. MIMO configuration also achieves a high information rate, by leveraging the waveform diversity, and a high detection rate and resolution with a large physical aperture. [6] demonstrates a typical co-design based MIMO configuration, which leverages the null space of the communications for radar transmission.

In this paper, we envision a power-domain paradigm (called superposition transmission), in which the signal is fully superposed on frequency, spatial, and time domains for radar and communications co-design. To initiate the discussion, a mono-static broadcasting channel (MBC) topology [2], which can be referred to downlink broadcasting communications channel, is used in this paper, as shown in Fig. 1. This scenario is a typical downlink case according to 3GPP standards (3GPP TR36.859 [7]). However, our case is different from the pure communications scenario in [7]. The communications users 1 and 2 are also treated as radar targets (reflecting the radio signal) when receiving downlink data from the access node, and the transmitting power is split for achieving both communications and targets detection. This paper brings the following contributions to radar and communications co-design:

- A superposition waveform transmission method is tested for the first time, to the best of the Authors' knowledge, for radar and communications co-design. It releases the co-design from the constraint of the spectrum, space, and time orthogonality.

This research was partly funded by the SESAR Joint Undertaking (SJU) in project NewSense (Evaluation of 5G Network and mmWave Radar Sensors to Enhance Surveillance of the Airport Surface), Grant Number 893917, within the framework of the European Union's Horizon 2020 research and innovation program. The opinions expressed herein reflect the authors' view only. Under no circumstances shall the SJU be responsible for any use that may be made of the information contained herein. This work was also partly supported by the Academy of Finland, under the project ULTRA (328226, 328214).

- Our work studies the impact of the quality of service (QoS) from communications' point of view on the performance of joint system.
- The proposed concept is verified in an MBC topology, which contains downlink communication channels, monostatic radar configuration, and entities (nodes) with mixed radar target and communications terminal, as shown in Fig. 1. The topology fits future RF convergence applications, for example in the CAV and autonomous-drones scenarios.

The rest of the paper is organised as the follows Section II introduces the innovative setup of the superposition transmission of joint radar and communications system; Section III formulates the performance evaluation problem of the proposed dual-function system; Analytical analysis and Monte Carlo simulation are conducted and compared in Section IV; and the conclusions of the current work as well as a discussion about future works are given Section V.

II. System Model

Our purpose in this paper is to test a novel superposition-transmission-based RF convergence. Thus, we preclude spatial and spectral complexities by setting up an MBC topology scenario as shown in Fig. 1, where all nodes are configured as the single carrier (SC) single-input single-output (SISO). In this MBC setup, there is one dual-function station (DFS) transmitting dual-function waveform (DFW) to user 1 and user 2 simultaneously, in the fully overlapped spectrum. We assume that both users are the communications nodes, meanwhile well-separated (not colinear with DFS and fall in different range bins) radar targets. The DFW is the superposing of downlink communications signals s_1, s_2 (for user 1 and 2 respectively) and radar signal x (for both users), $\mathbb{E}(|s_1|^2) = \mathbb{E}(|s_2|^2) = \mathbb{E}(|x|^2) = 1$. The channel gains for user 1 and user 2 are h_1 and h_2 [1]. We use η_1 and η_2, for user 1 and user 2, to mimic the impacts of the radar cross-section (RCS) of users on the reflection signal strength. To be able to detect the reflected waveform from both users, the self-interference cancellation is conceived on the DFS. The recent experimental result in [5] have proved that jointly applying of analog and digital cancellations can successfully weep of the self-interference and detect targets. In this paper, the residual self-interference is treated as attenuated instant transmitting signals by giving a coefficient ξ. The radar signal is a composition of repetition. We assume that the radar signal is known at all users and can be decoded then subtracted from the received superposition signal. In addition to above assumptions, we further attach two loose conditions: ***i).*** the CSI is known at DFS and user terminal and ***ii).*** the system works in a fast fading channel. These two conditions are not essential in this work; however, will facilitate the discussion.

Inspired by the Multi-user Superposition Transmission (MUST) [7], at the same time-and-frequency resource block,

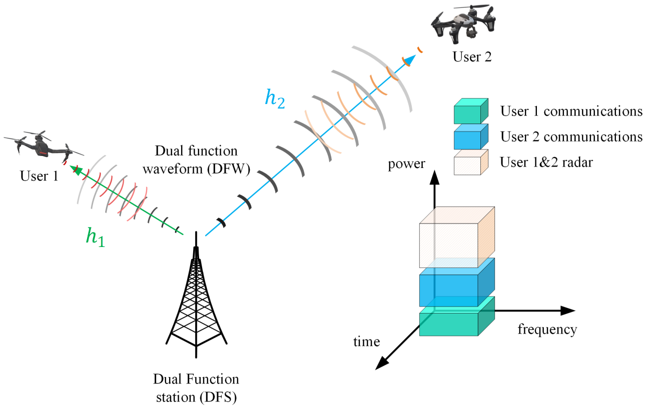


Fig. 1: The considered MBC topology and the illustration of resource block in our consideration.

we propose a power-domain division scheme for joint radar and communications system as illustrated in Fig. 1.

The total transmitted signals $S(t)$ are modeled by,

$$S(t) = \alpha_1 s_1(t) + \alpha_2 s_2(t) + \alpha_r x(t) \tag{1}$$

the power allocation coefficients for signals s_1, s_2, x are $\alpha_1^2, \alpha_2^2, \alpha_r^2$ respectively, and $\alpha_1, \alpha_2, \alpha_r \in [0, 1)$, without further specifications, we assume $\alpha_1^2, \alpha_2^2, \alpha_r^2 \neq 0$ and $\alpha_1^2 + \alpha_2^2 + \alpha_r^2 \leq 1$ for all the following analysis.

A. Communications

In the downlink, the received communications signals of user 1 $y_1(t)$ and user 2 $y_2(t)$ are respectively given by,

$$y_1(t) = |h_1| \, S(t) + n_1(t) \tag{2a}$$
$$y_2(t) = |h_2| \, S(t) + n_2(t) \tag{2b}$$

where $n_1(t) \sim \mathcal{N}(0, \sigma_1^2), n_2(t) \sim \mathcal{N}(0, \sigma_2^2)$ are additive white Gaussian noise (AWGN) at communications receivers of user 1 and user 2 respectively.

Since the superposition coding signals are transmitted, we follow the suggestion in [8] that user 1 and 2 have disparate channels. If we assume $|h_1|^2 > |h_2|^2$, equivalently user 1 is the stronger user and user 2 is the weaker user, in received signal y_1 user 1 could first use SIC to detect signal s_2, then reconstruct signal by subtracting s_2. In y_2, under $\alpha_2^2 > \alpha_1^2$ the signal s_2 can be decoded while s_1 is treated as interference.

The Signal-to-Interference-plus-Noise-Ratio (SINR) for user 1 and 2, γ_1 and γ_2 are respectively expressed as,

$$\gamma_1 = \frac{\alpha_1^2 \, |h_1|^2}{\sigma_1^2} \tag{3a}$$

$$\gamma_2 = \frac{\alpha_2^2 \, |h_2|^2}{|h_2|^2 \, \alpha_1^2 + \sigma_2^2} \tag{3b}$$

B. Sensing

At the DFS, the echoes z of the k_{th} target (user) are modeled as,

$$z_k(t) = \eta_k \, |h_k|^2 \, S(t - \tau_k) + \xi S_{\text{int}} + n_r(t) \tag{4}$$

where τ_k is the round-trip delay from the k_{th} target, $n_r(t) \sim \mathcal{N}(0, \sigma_r^2)$ is AWGN. ξS_{int} is the self-interference residue and

[1] The block fading assumption is made in this paper, which means the fading process is approximately constant for a certain observation times, usually number of symbol intervals

$\mathbb{E}(|S_{\text{int}}|^2) = 1$. According the recent works of the in-band self-cancellation [5] [9], $105 \sim 110$ dB is an achievable self-interference suppression level which indicates that in-band residue is very close to the receiver sensitivity (noise floor) if 0 dBm power emission is set on the transmitting path. Thus, the residue term ξS_{int} is ignored in the following derivation. In the radar signal model, the backscatters from the clutters is another negative impact fact which is assumed to be neutralized by the whitening filter before radar processing.

If the given radar task it to estimate the distance of the target (i.e., equivalently the time delay), an unbiased estimator has the minimum, which can be given by the Cramér-Rao lower bound (CRLB). In mathematical form we have,

$$\mathbb{E}\big[(\hat{\tau_k}-\tau_k)^2\big] \geq \frac{1}{\mathbb{E}\Big\{\Big[\frac{\partial}{\partial\tau_k}\log L\big(z(t);\tau_k\big)\Big]^2\Big\}} \tag{5}$$

where $L\big(z(t);\tau_k\big)$ is the likelihood function of τ_k.

By considering the reflected communications components as the interference, we obtain the logarithm of likelihood function,

$$\begin{aligned}&\log L\big(z(t);\tau_k\big) \\ &= C - \frac{1}{2\sigma_r^2}\Big(z(t) - \eta_k h_k^2 \alpha_k s_k - \eta_k h_k^2 \alpha_r x(t-\tau_k)\Big)^2\end{aligned} \tag{6}$$

where C is a constant without involving τ_k, hence the exact expression of C is not provided here. The partial derivative yields to,

$$\frac{\partial}{\partial\tau_k}\log L\big(z(t);\tau_k\big) = -\frac{\eta_k h_k^2 \alpha_r}{\sigma_r^2}\cdot n_r(t)\cdot x'(t-\tau_k) \tag{7}$$

straightforwardly,

$$\mathbb{E}\Big\{\Big[\frac{\partial}{\partial\tau_k}\log L\big(z(t);\tau_k\big)\Big]^2\Big\} = \frac{\eta_k^2 h_k^4 \alpha_r^2}{\sigma_r^2}\mathbb{E}\Big\{\big[x'(t-\tau_k)\big]^2\Big\} \tag{8}$$

Before further discussions, it is worth to mention the issue of handling the communications component in radar task. Communication components in the superposed waveform will also be reflected by the users and received by DFS. The reflected communications components can be used for enhancing the radar detection performance when it is adequately separated from the superposed waveform. Otherwise, the communications component will undermine the overall radar component (waveform) properties as the communications component is not well designed for detection purpose. To discuss the communication component for extra radar benefits will complicate our study as the benchmark of superposed waveform radar and communications co-design. Thus, in this work, the communication component is treated as interference for the detection task, the detection (radar) performance in this paper is a conservative estimation.

III. Problem formulation

The joint performance analysis is crucial in the evaluation of radar and communications co-design. In a communications system, we always put efforts to achieve maximum capacity (or sum-rate in multi-user scenario). In contrast, in radar systems, due to many shades of radar performance metrics, it is hard to determine the ultimate metric to evaluate radar systems comprehensively. In this section, we will discuss the formation of joint performance metrics hence the corresponding optimization problem.

A. Universalizing the evaluation metric

The communications rate of users 1 and 2 are denoted as R_1 and R_2, respectively, and they are upper bounded by,

$$R_1 \leq \log_2(1+\gamma_1) \tag{9a}$$

$$R_2 \leq \min\Big\{\log_2(1+\gamma_2), \log_2(1+\overline{\gamma}_2)\Big\} \tag{9b}$$

where $\log_2(1+\overline{\gamma}_2)$ is the upper-bound communication rate for SIC on user 1 to successfully decode s_2, $\overline{\gamma}_2$ is given by,

$$\overline{\gamma}_2 = \frac{\alpha_2^2\,|h_1|^2}{|h_1|^2\,\alpha_1^2 + \sigma_c^2} \tag{10}$$

Provided the channel gains assumption, the communication sum rate R_{sum} of users 1 and 2 is upper bounded by,

$$R_{\text{sum}} \leq \sum_{k=1}^{2}\log_2(1+\gamma_k) \tag{11}$$

In the radar system, as we mentioned in Section II-B, the CRLB is a popular metric used to evaluate the parameters estimation, which implies the performance of system. For time delay estimation [10], given (5) and (8) we can have,

$$\mathbb{E}\Big\{\big[x'(t-\tau_k)\big]^2\Big\} = 2EWB_{\text{rms}}^2 \tag{12}$$

where W is the bandwidth, $2E$ is the total received signal energy and B_{rms} is the root-mean-square (rms) bandwidth, given by,

$$2E = \int_0^T |x(t)|^2\,\mathrm{d}t \tag{13a}$$

$$B_{\text{rms}}^2 = \frac{4\pi^2\displaystyle\int_{-\infty}^{\infty} f^2\,|X(f)|^2\,\mathrm{d}f}{\displaystyle\int_{-\infty}^{\infty}|X(f)|^2\,\mathrm{d}f} \tag{13b}$$

where T is the radar receiving duration, $X(f)$ is the spectrum of signal $x(t)$. Hence,

$$\mathbb{E}\big[(\hat{\tau_k}-\tau_k)^2\big] \geq \frac{\sigma_r^2}{2\eta_k^2 h_k^4 \alpha_r^2 EWB_{\text{rms}}^2} \tag{14}$$

clearly $\frac{2EW}{\sigma_r^2}$ is the radar receiving Signal-to-Noise-Ratio (SNR). Until here, the total estimation error variance σ_ϵ^2 can be derived as,

$$\sigma_\epsilon^2 \geq \sum_{k=1}^{2}\frac{\sigma_r^2}{2\eta_k^2 h_k^4 \alpha_r^2 EWB_{\text{rms}}^2} \tag{15}$$

B. Optimization problems

The communications sum rate and the estimation error variance of radar system do not share the same unit of measurements. We can only consider the radar and communications co-design as two sub-problems,

$$\begin{aligned} \max_{\alpha_1,\alpha_2} \quad & R_{\text{sum}} \\ \text{s.t.} \quad & \alpha_1^2+\alpha_2^2 \le 1-\alpha_r^2, \\ & R_2 \ge R_{0,2} \end{aligned} \tag{16}$$

$$\begin{aligned} \min_{\alpha_1,\alpha_2,\alpha_r} \quad & \sigma_\epsilon^2 \\ \text{s.t.} \quad & \alpha_1^2+\alpha_2^2 \le 1-\alpha_r^2, \\ & R_2 \ge R_{0,2}, R_1 \ge R_{0,1} \end{aligned} \tag{17}$$

where $R_{0,2}, R_{0,1}$ are the minimum rate to guarantee the QoS for user 2 and user 1 respectively. α_r^2 is treated as a parameter in (16), given a certain tolerance of radar estimation error, we would like to achieve the sum rate maximum.

IV. Performance analysis

We derive the joint performance boundaries and the corresponding power allocations for communications users and radar function.

A. Optimal solutions

We first determine the feasible region for $\alpha_1^2, \alpha_2^2, \alpha_r^2$ from problem (16), then find some feasible points in problem (17).

1) Communications rate: in problem (16), R_{sum} is a binary logarithm function of the product between $1+\gamma_1$ and $1+\gamma_2$, and it will monotonically increase with this product. To find the optimum in (16), provided the constraint $R_2 \ge R_{0,2}$, it is of interest to investigate the monotonicity of the above product as a function f_1,

$$f_1 = (1+\gamma_1)(1+\gamma_2) \tag{18}$$

If we consider f_1 as the function of α_2^2, the following form is obtained,

$$f_1(\alpha_2^2) = 1+\frac{\alpha_1^4|h_1|^2|h_2|^2+\alpha_1^2|h_1|^2\sigma_2^2+\alpha_2^2|h_2|^2\sigma_1^2+\alpha_1^2\alpha_2^2|h_1|^2|h_2|^2}{\alpha_1^2|h_2|^2\sigma_1^2+\sigma_1^2\sigma_2^2} \tag{19}$$

and the first order partial derivative of (19) is,

$$\frac{\partial f_1}{\partial \alpha_2^2} = -\frac{(\left|h_1\right|^2\sigma_2^2 - \left|h_2\right|^2\sigma_1^2)(\left|h_2\right|^2\kappa+\sigma_2^2)}{\big[\left|h_2\right|^2(\kappa-\alpha_2^2)+\sigma_2^2\big]^2\sigma_1^2} \tag{20}$$

where $\kappa = 1-\alpha_r^2$ and $\alpha_1^2+\alpha_2^2=\kappa$. Since our assumption is $\left|h_1\right|^2 > \left|h_2\right|^2$, under $\sigma_1^2 \le \sigma_2^2$ (2) the $\frac{\partial f_1}{\partial \alpha_2^2}$ will always be negative for all the feasible values of α_2^2. Consequently R_{sum} in (16) will monotonically decrease with α_2^2 increasing, and reaches its maximum when $R_2 = R_{0,2}$ holds. Now we have,

$$\log_2(1+\frac{\alpha_2^2\left|h_2\right|^2}{\left|h_2\right|^2(\kappa-\alpha_2^2)+\sigma_2^2}) = R_{0,2} \tag{21}$$

the solutions of (21) are,

$$\alpha_1^2 = \frac{\kappa\left|h_2\right|^2 - \sigma_2^2(2^{R_{0,2}}-1)}{\left|h_2\right|^2 2^{R_{0,2}}} \tag{22a}$$

$$\alpha_2^2 = \frac{(2^{R_{0,2}}-1)(\kappa\left|h_2\right|^2+\sigma_2^2)}{\left|h_2\right|^2 2^{R_{0,2}}} \tag{22b}$$

under the solution (22), R_{sum} achieves its optimum. The results in (22) are also consistent with [11].

2) Radar estimation error: in problem (17), the minimum of σ_ϵ^2 monotonically decreases with α_r, the larger value of α_r^2 we give the smaller σ_ϵ^2 we have.

Under constraint $R_2 \ge R_{0,2}, R_1 \ge R_{0,1}$, we could have,

$$\begin{cases} \alpha_1^2 \ge \dfrac{(2^{R_{0,1}}-1)\sigma_1^2}{\left|h_1\right|^2} \\ \alpha_2^2 \ge (2^{R_{0,2}}-1)\big[\dfrac{(2^{R_{0,1}}-1)\sigma_1^2}{\left|h_1\right|^2}+\dfrac{\sigma_2^2}{\left|h_2\right|^2}\big] \end{cases} \tag{23}$$

the maximum of α_r^2 is achieved when α_1^2, α_2^2 in (23) are at minimum values. Based on [10], we present the energy E and rms bandwidth B_{rms} under two modulations of radar waveform: linear FM with rectangular envelope and parabolic FM with rectangular envelope.

3) Linear FM with rectangular envelope: for a linear frequency modulation (FM) signal with $\text{rect}(t/T)$ envelope, energy E_{linear} and rms bandwidth $B_{\text{rms}}^{\text{linear}}$ yield to,

$$E_{\text{linear}} = \frac{T}{2} \tag{24a}$$

$$B_{\text{rms}}^{\text{linear}} = \frac{\pi^2W^2}{3} \tag{24b}$$

hence (15) alters to,

$$\sigma_{\epsilon,\text{linear}}^2 \ge \sum_{k=1}^{2} \frac{3\sigma_r^2}{\pi^2\eta_k^2h_k^4\alpha_r^2TW^3} \tag{25}$$

4) Parabolic FM with rectangular envelope: for a parabolic FM signal with rectangular envelope, energy $E_{\text{parabolic}}$ and rms bandwidth $B_{\text{rms}}^{\text{parabolic}}$ yield to,

$$E_{\text{parabolic}} = \frac{T}{2} \tag{26a}$$

$$B_{\text{rms}}^{\text{parabolic}} = \frac{16\pi^2W^2}{45} \tag{26b}$$

hence (15) alters to,

$$\sigma_{\epsilon,\text{parabolic}}^2 \ge \sum_{k=1}^{2} \frac{45\sigma_r^2}{16\pi^2\eta_k^2h_k^4\alpha_r^2TW^3} \tag{27}$$

B. Numerical results

We implement a series of simulations to validate our theoretical analysis and to present joint performance in the radar and communications co-design explicitly. Table I lists the parameters in the simulations.

In the optimization problem (16) and (17), we expect to observe two behaviours of co-design system,

- Given the weak user QoS $R_{0,2}$ in (16), the trend of R_{sum} with σ_ϵ^2;

[2] in this paper, we will not provide discussions for the situation where σ_1^2 is much greater than σ_2^2.

TABLE I: Parameters in simulations

Parameters	Value	Parameters	Value
channel gain [3]$\lvert h_1\rvert^2$	-90 dB	channel gain $\lvert h_2\rvert^2$	-100 dB
noise in user 1 σ_1^2	-105 dBm	noise in user 2 σ_2^2	-105 dBm
noise in radar σ_r^2	-110 dBm	self-interference cancellation	110 dB
user 1 RCS η_1	0.1 m^2	user 2 RCS η_2	0.5 m^2
bandwidth W	20 MHz	Time-bandwidth product TW	1000

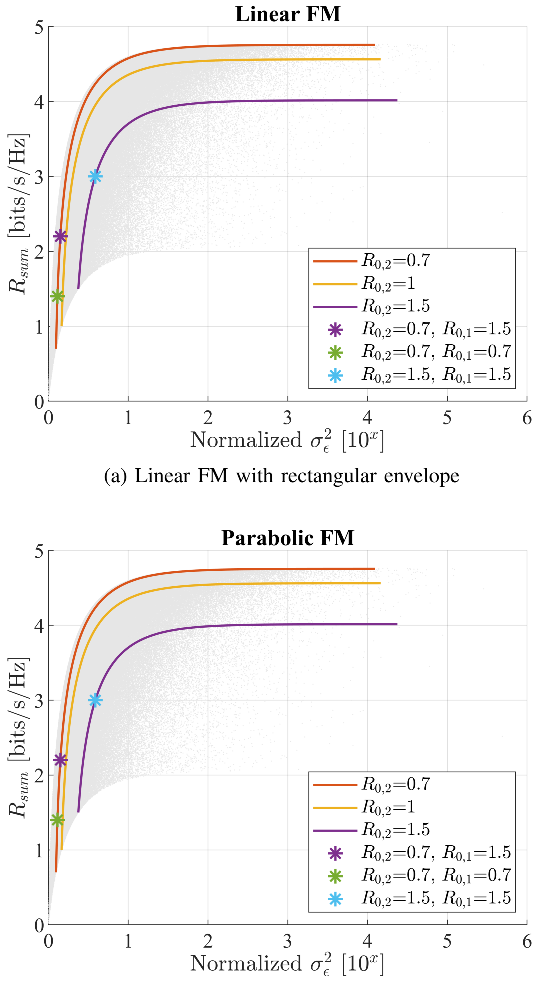
- Given respectively the weak and strong user QoS $R_{0,2}, R_{0,1}$ in (17), the minimum of σ_ϵ^2.

Fig. 2 presents the numerical results of optimization problems (16) and (17). Six cases are discussed in the figure, R_{sum} versus σ_ϵ^2 under $R_{0,2} = 0.7, 1, 1.5$ (unit:bits/s/Hz); minimum σ_ϵ^2 under $\{R_{0,2} = 0.7, R_{0,1} = 1.5\}$, $\{R_{0,2} = 0.7, R_{0,1} = 0.7\}$, $\{R_{0,2} = 1.5, R_{0,1} = 1.5\}$. The solid lines indicate the relationship between R_{sum} and σ_ϵ^2 under constraint $R_2 \geq R_{0,2}$. All star (i.e., *) markers show the minimum σ_ϵ^2 under constraints $R_2 \geq R_{0,2}, R_1 \geq R_{0,1}$. The grey dots background gives the feasible region of the relationship between R_{sum} and σ_ϵ^2. σ_ϵ^2 is normalized by the minimum of σ_ϵ^2 in the figures,

$$\min(\sigma_\epsilon^2) = \sigma_\epsilon^2|_{\alpha_r^2=1} \tag{28}$$

With the increase of QoS requirement in user 2 (the weak user), the radar performance drops rapidly. Comparing with user 2, the QoS requirement of user 1 (the strong user) has less influence in the degrades of radar estimation accuracy. As we can see from Fig. 2, horizontally the distance between purple star marker (i.e., $R_{0,2} = 0.7, R_{0,1} = 1.5$) and blue star marker (i.e., $R_{0,2} = 1.5, R_{0,1} = 1.5$) is much larger than that between purple star marker (i.e., $R_{0,2} = 0.7, R_{0,1} = 1.5$) and green star marker (i.e., $R_{0,2} = 0.7, R_{0,1} = 0.7$). Observing the solid lines in the figure, up to a point R_{sum} tends to converge no matter how much power we allocate to communications signals. This phenomenon also implies that the unreasonable large QoS requirement in the weak user could jeopardize the whole co-design system. By comparing Fig. 2a with Fig. 2b, we may conclude that under rectangular envelope linear FM and parabolic FM barely show difference on the performance of co-design system.

In the superposition transmission scheme, a moderate QoS requirement for the weak user (e.g., the user with lower channel gain) could benefit both communications and sensing. However, the performance of radar system abruptly drops when the QoS requirements of weak users increase over a certain threshold; in other words, from Fig. 2 the horizontal distance between the solid purple line (i.e., $R_{0,2} = 1.5$) and the solid orange line (i.e., $R_{0,2} = 1$) is much larger than the horizontal distance between the solid orange line (i.e., $R_{0,2} = 1$) and the solid red line the solid orange line (i.e., $R_{0,2} = 0.7$).



(a) Linear FM with rectangular envelope

(b) Parabolic FM with rectangular envelope

Fig. 2: R_{sum} Versus normalized σ_ϵ^2 under linear FM and parabolic FM. Normalized σ_ϵ^2 is given by the power of 10 to better scale up.

For a communications-priority system, in both Fig. 2a and Fig. 2b the upper-left corner of solid lines would be the optimal operation point, due to the convergence of sum rate for communications. At these points, the minimum radar estimation error variance also reaches after maximum achievable sum rate has been met.

To further reveal the communications system performance in the co-design system, we adopt Jain's fairness,

$$\mathcal{J}(x_1, x_2, \ldots, x_n) = (\sum_{i=1}^{n} x_i)^2 / \sum_{i=1}^{n} x_i^2 \tag{29}$$

Fig. 3 illustrates the fairness versus R_{sum} under different QoS requirement in weak user. Clearly, low QoS requirement leads to low fairness during most of R_{sum} values; high QoS case behaves even worse than low QoS case in the fairness, the highest reachable R_{sum} values is relatively far from the maximum. A moderate QoS requirement guarantees both high fairness and high R_{sum} value.

[3] the path loss is incorporated into the channel gain.

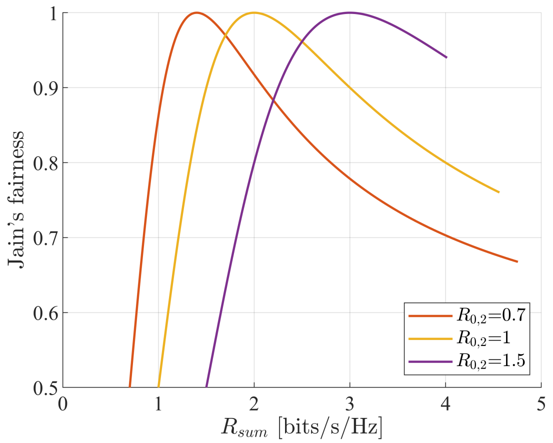


Fig. 3: The Jain's fairness between two users in communications, under various minimum QoS requirements of user 2.

As a result, a moderate QoS requirement for the weak user promises the good fairness of communications and low estimation errors of sensing.

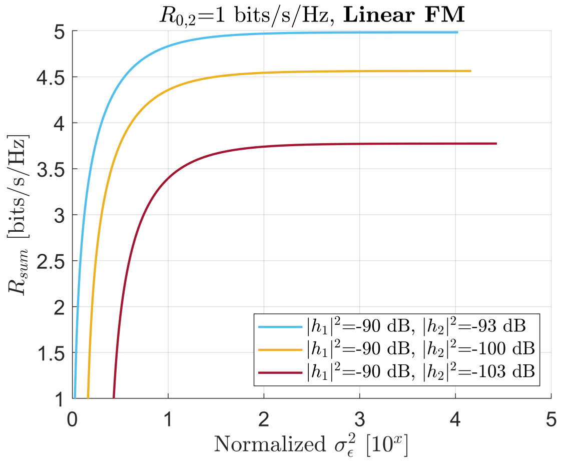


Fig. 4: R_{sum} Versus normalized σ_ϵ^2 under different level of asymmetry between two users' channel.

Fig. 4 demonstrates how the asymmetry of users' channel could affect the system performance. This numerical analysis shows that the asymmetry between two users' channel has impact on the system performance, the greater the level of asymmetry is, the larger degradation of the system is. The above result implies the impact of user grouping strategies on the overall system performance, which is that low level of asymmetry between users' channel compromises less on radar performance.

V. Conclusion

In this paper, the superposition transmission is proposed for radar and communication co-design in contrast with the conventional frequency, time, and spatial domain operations. The joint radar-and-communications performance is analysed in the mono-static broadcasting topology. A generic communications signal is utilized together with two specific radar signals, namely a linear FM and a parabolic FM radar signal. A moderate QoS requirement for a weak user balances both communications fairness and the overall system performance. Low level of asymmetry between users' channel implies better co-design system performance. Conservatively speaking, in the joint radar-and-communication system, the radar side has large demands on the power allocation, which leads to the low-to-moderate communications rates. This superposition transmission scheme, under current study, is not suitable for high data rate applications; whereas it is a good scheme for drones control and command signals, together with sensing functionality.

The current findings in this work can be seen as a bedrock for future extensions on ***i)*** computational complexity of the proposed superposition transmission joint system; ***ii)*** comparisons with prior works, for example, the joint system based on OFDM and MIMO; ***iii)*** unifying the performance metric of sensing and communications functions, for example, using the I-MMSE [12] as a bridge; ***iv)*** scalability to the multiple user (more than two) scenarios; ***v)*** application of SIC to remove communications signal components at the radar receiving.

References

[1] A. R. Chiriyath, B. Paul, and D. W. Bliss, "Radar-Communications Convergence: Coexistence, Cooperation, and Co-Design," *IEEE Transactions on Cognitive Communications and Networking*, vol. 3, pp. 1–12, 2017.

[2] B. Paul, A. R. Chiriyath, and D. W. Bliss, "Survey of RF Communications and Sensing Convergence Research," *IEEE Access*, pp. 252–270, 2017.

[3] R. M. Mealey, "A method for calculating error probabilities in a radar communication system," *IEEE Transactions on Space Electronics and Telemetry*, vol. 9, no. 2, pp. 37–42, 1963.

[4] C. Sturm and W. Wiesbeck, "Waveform design and signal processing aspects for fusion of wireless communications and radar sensing," *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1236–1259, 2011.

[5] C. Baquero Barneto, T. Riihonen, M. Turunen, L. Anttila, M. Fleischer, K. Stadius, J. Ryynänen, and M. Valkama, "Full-Duplex OFDM Radar With LTE and 5G NR Waveforms: Challenges, Solutions, and Measurements," *IEEE Transactions on Microwave Theory and Techniques*, vol. 67, no. 10, pp. 4042–4054, 2019.

[6] F. Liu, C. Masouros, A. Li, H. Sun, and L. Hanzo, "Mu-mimo communications with mimo radar: From co-existence to joint transmission," *IEEE Transactions on Wireless Communications*, vol. 17, pp. 2755–2770, 2018.

[7] 3GPP, *Study on Downlink Multiuser Superposition Transmission (MUST) for LTE*, Jan. 2016. v13.0.0 (Accessed Jun. 2020).

[8] D. Tse and P. Viswanath, *Fundamentals of wireless communication*. Cambridge university press, 2005.

[9] D. Bharadia, E. McMilin, and S. Katti, "Full duplex radios," in *Proceedings of the ACM SIGCOMM 2013 conference on SIGCOMM*, pp. 375–386, 2013.

[10] C. Cook, *Radar signals: An introduction to theory and application*. Elsevier, 2012.

[11] C. L. Wang, J. Y. Chen, and Y. J. Chen, "Power allocation for a downlink non-orthogonal multiple access system," *IEEE wireless communications letters*, vol. 5, no. 5, pp. 532–535, 2016.

[12] D. Guo, S. Shamai, S. Verdú, *et al.*, "The interplay between information and estimation measures," *Foundations and Trends® in Signal Processing*, vol. 6, no. 4, pp. 243–429, 2013.