A Survey on Coping With Intentional Interference in Satellite Navigation for Manned and Unmanned Aircraft

Ruben Morales-Ferre, *Student Member, IEEE*, Philipp Richter, *Member, IEEE*, Emanuela Falletti, Alberto de la Fuente, and Elena Simona Lohan, *Senior Member, IEEE*

***Abstract*—Intentional interference in satellite navigation is becoming an increasing threat for modern systems relying on Global Navigation Satellite Systems (GNSS). In particular, critical applications such as aviation can be severely affected by undetected and un-mitigated interference and therefore interference management solutions are crucial to be employed. Methods to cope with such intentional interference enclose interference detection, interference mitigation, interference classification, and interference localization. This paper offers a comprehensive survey of interference management methods developed in the last four decades by the research community. After reviewing the main concepts of GNSS-based navigation, the interference and interference management solutions are classified, with a particular focus on the two major threats in GNSS navigation, namely jamming and spoofing. Mathematical models, comparative tables for various interference management solutions, such as detection, localization, mitigation, and classification, as well as comparative numerical results based on several selected algorithms are also presented. We especially focus on algorithms relying on omni-directional antennas, which do not require additional specific antennas to be installed on the aircraft and thus reduce the costs of retrofit and installation.**

***Index Terms*—Aviation, drones, GNSS, interference, jamming, meaconing, SatNav, spoofing.**

List of Acronyms

AAC	Airline Administrative Control
AANET	Aeronautical Ad-hoc Networking
ACARS	Aircraft Communication Addressing and Reporting System
ACAS	Aircraft Collision Avoidance System
ADC	Analog-to-Digital Converter
ADS	Automatic Dependent Surveillance
ADS-B	Automatic Dependent Surveillance-Broadcast
ADS-C	Automatic Dependent Surveillance-Contract
AGC	Automatic Gain Control
AM	Amplitude Modulation
AMACS	All-purpose Multi-channel Aviation Communication System
ANF	Adaptive Notch Filter
AoA	Angle of Arrival
AOC	Aeronautical Operational Control
APNT	Alternative Positioning, Navigation, and Timing
AR	Auto-Regressive
ARAIM	Advanced Receiver Autonomous Integrity Monitoring
ARNS	Aeronautical Radio Navigation Service
ASAS	Airbone Separation Assurance System
ATC	Air Traffic Control
ATM	Air Traffic Management
ATS	Air Traffic Services
AWGN	Additive White Gaussian Noise
B-AMC	Broadband Aeronautical Multi-Carrier Communications
BPSK	Binary Phase Shift Keying
CDF	Cumulative Distribution Function
CDMA	Code Division Multiple Access
CME	Consecutive Mean Excision
C/N_0	Carrier-to-Noise Ratio
COTS	Commercial Off-The-Shelf
CRPA	Controlled Radiation Pattern Antenna
CW	Continuous Wave
CWI	Continuous Wave Interference
D^3	Dispersion of Double Differences
DAB	Digital Audio Broadcasting
DEF	Digital Excision Filter
DF	Direction Finding
DFT	Discrete Fourier Transform
DFMC	Dual-Frequency Multi-Constellation
DGPS	Differential Global Positioning System
DME	Distance Measuring Equipment
DoA	Direction of Arrival
DoS	Denial of Service
DPA	Dual Polarization Antenna

Manuscript received February 13, 2019; revised July 12, 2019 and September 16, 2019; accepted October 8, 2019. Date of publication October 24, 2019; date of current version March 11, 2020. This work was supported by the SESAR Joint Undertaking through the European Union's Horizon 2020 Research and Innovation Programme under Grant 783183.[1] *(Corresponding author: Ruben Morales-Ferre.)*

R. Morales-Ferre and E. S. Lohan are with the Electrical Engineering Unit, Tampere University, 33720 Tampere, Finland (e-mail: ruben.moralesferre@tuni.fi; elena-simona.lohan@tuni.fi).

P. Richter was with Tampere University, 33720 Tampere, Finland (e-mail: philipp.richter@arcor.de).

E. Falletti is with the Space and Navigation Technologies Research Area, LINKS Foundation, 10138 Turin, Italy (e-mail: emanuela.falletti@linksfoundation.com).

A. de la Fuente is with GNSS, GMV Aerospace and Defence, 28760 Madrid, Spain (e-mail: afuente@gmv.com).

Digital Object Identifier 10.1109/COMST.2019.2949178

[1]This project is a partnership between GMV Innovating Solutions, Tampere University (former TUT, Tampere University of Technology), and LINKS Foundation (former ISMB, Istituto Superiore Mario Boella); more details at: https://www.sesarju.eu/node/3107.

DPE	Direct Position Estimation
DRSS	Received Signal Strength Difference
DS	Digital Sum
DSSS	Direct Sequence Spread Spectrum
DVB-T	Digital Video Broadcasting - Terrestrial mode
EGNOS	European Geostationary Navigation Overlay Service
EUROCAE	European Organisation for Civil Aviation Equipment
EVAIR	Eurocontrol Voluntary ATM Incident Reporting
FANET	Flying Ad-Hoc NETwork
FANS	Future Air Navigation System
FCI	Future Communications Infrastructure
FDD	Frequency-Division Duplexing
FDoA	Frequency Difference of Arrival
FFT	Fast Fourier Transform
FIR	Finite Impulse Response
FM	Frequency Modulation
FPD	Frequency Power Detector
FRA	Free Route Airspace
FSO	Free-Space Optical
GA	General aviation
GBAS	Ground-Based Augmentation Systems
GLRT	Generalized Likelihood Ratio Test
GNSS	Global Navigation Satellite System
GoF	Goodness of Fit
GPS	Global Positioning System
GSA	European GNSS Agency
GSM	Global System for Mobile communications
HF	High Frequency
HHT	Hilbert-Huang Transform
HRT	Hough-Radon Transform
HW	Hardware
IATA	International Air Transport Association
ICAO	International Civil Aviation Organization
IIR	Infinite Impulse Response
ILS	Instrument Landing System
INLS	Integrated Navigation and Landing System
INS	Inertial Navigation System
IPS	Internet Protocol Suite
IRU	Inertial Reference Unit
ISDB	Integrated Services Digital Broadcasting
JNR	Jammer-to-Noise Ratio
JSR	Jammer-to-Signal Ratio
KLT	Karhunen-Loève Transform
L-DACS	L-band Digital Aeronautical Communication System
LAAS	Local Area Augmentation System
LAN	Local Area Network
LHCP	Left-Hand Circularly Polarized
LMS	Least Mean Squares
LOS	Line of Sight
LS	Least Squares
LTE	Long-Term Evolution
MANET	Mobile Ad-hoc Network
MCAR	Multi-Correlator output with Auto Regressive modelling
MHWN	Multi Hop Wireless Networks
MLE	Maximum Likelihood Estimator
MLS	Microwave Landing System
MOPS	Minimum Operational Performance Standards
MPDR	Minimum Powerless Distortion-less Response
MSTFT	Modified Short Time Fourier Transform
MUSIC	MUltiple SIgnal Classification
NASA	National Aeronautics and Space Administration
NavAids	Navigational Aids
NDB	Non-Directional Beacon
NF	Notch Filter
NLOS	Non Line of Sight
NMA	Navigation Message Authentication
OFDM	Orthogonal Frequency Division Multiplexing
PBM	Pulse Blanking Method
PD	Probability of Detection
PDF	Probability Density Function
PDM	Power Distortion Monitoring
PDoA	Power difference of Arrival
PLD	Power Law Detector
PNT	Positioning, Navigation, and Timing
PPM	Pulse-Position Modulation
PRN	Pseudo Random Noise
PSD	Power Spectrum Density
PVT	Position Velocity and Time
PWAM	Passive Wide Area Multilateration
QZSS	Quasi-Zenith Satellite System
RA	Resolution Advisory
RAIM	Receiver Autonomous Integrity Monitoring
RDS	Running Digital Sum
RF	Radio Frequency
RFI	Radio Frequency Interference
RHCP	Right Hand Circular Polarized
RMSE	Root Mean Square Error
RNSS	Radio Navigation Satellite Service
RSS	Received Signal Strength
RTCA	Radio Technical Commission for Aeronautics
RTK	Real Time Kinematic
SatNav	Satellite Navigation
SBAS	Satellite-Based Augmentation Systems
SCA	Spreading Code Authentication (SCA)
SCC	SuCcessive spoofing Cancellation
SEDLL	Spoofing Estimating Delay Lock Loop
SESAR	Single European Sky Air traffic management Research
SJNR	Signal-to-Jamming-plus-Noise Ratio
SNR	Signal-to-Noise Ratio
SoS	Sum of Squares
SQM	Signal Quality Monitoring
STAP	Spatial-temporal Adaptive Processing
STFT	Short Time Fourier Transform
SSC	Spectral Separation Coefficient
SSR	Secondary Surveillance Radar
SV	Spatial Vehicle
SVD	Singular Value Decomposition
SVM	Support Vector Machines
SW	Software
TA	Traffic Advisory
TACAN	Tactical Air Navigation System

TDD	Time-Division Duplex
TDoA	Time Difference of Arrival
TIA	Telecommunications Industry Association
TMA	Terminal Manoeuvring Area
ToA	Time of Arrival
TPD	Time Power Detector
TV	Television
UAT	Universal-Access Transponder
UAV	Unmanned Aerial Vehicle
UHF	Ultra High Frequency
ULA	Uniform Linear Array
UWB	Ultra-Wideband
VANET	Vehicular Ad-hoc Network
VHF	Very High Frequency
VOR	VHF Omnidirectional Range
WAAS	Wide Area Augmentation System
WAM	Wide-Area Multi-lateration
WiMax	Worldwide interoperability for Microwave Access
WLAN	wireless LAN
WSN	Wireless Sensor Networks
ZMNL	Zero Memory Non-Linearity.

I. Introduction

FOUR decades of Satellite Navigation (SatNav) and the emergence of new SatNav systems have brought in new challenges in dealing with the interference encountered over the wireless channels by the receivers employed in the aviation industry.

The aviation domain is typically divided into two main categories: manned and unmanned aircraft. The manned aircraft category is the one which requires the presence of a human pilot on-board of the aircraft, while the unmanned aircraft category refers to the situation when no human pilot is present on-board and the aircraft is controlled remotely, through the wireless channels. The number of the Unmanned Aerial Vehicles (UAVs), popularly known as drones, has been significantly increasing in the past five years and business analysis predict that the drone market worldwide will grow to more than 50 billions dollars by 2025 [1]. The number of Global Navigation Satellite System (GNSS) receivers installed on drones by 2025 is also estimated to reach 70 millions and to represent more than twice of the number of GNSS receivers installed in all other professional applications combined, according to a recent GNSS Supervisory Authority (GSA) market report [2].

Navigation is an essential part of a flying aircraft and it will become even more important in the crowded sky of the near future where millions of drones will co-exist with manned aircraft. *Navigation* here refers to the joint ability of continuously locating and tracking an aircraft both from the ground and from on-board of the aircraft. Continuous access to the aircraft exact location is needed not only to allow the safe routing of tens of thousands of aircraft worldwide, but also to avoid collisions, to facilitate emergency aids, to enable higher data rates and better broadband access for on-board entertainment (e.g., through location-based optimization of the communication links), and to support future services such as aerial taxis and ad-hoc aerial networks [3].

Satellite navigation, thanks also to the augmentation systems such as Satellite-Based Augmentation Systems (SBAS) or Ground-Based Augmentation Systems (GBAS), has become one of the main technologies of navigation in modern aircraft, supplementing the on-board inertial navigation systems and providing worldwide en-route, terminal, and lateral/vertical guidance during the final approach [4]. While the aviation industry still relies on conventional instruments called Navigational Aids (NavAids) to ensure a safe navigation, the most precise positioning technology nowadays for aircraft is the satellite navigation technology. Examples of NavAids, listed with references in Table I, are: Distance Measuring Equipment (DME), Instrument Landing System (ILS), VHF Omnidirectional Range (VOR), and Non-Directional Beacon (NDB).

Satellite navigation systems can be global, referred to as GNSS and able to provide positioning worldwide, or local, such as Quasi-Zenith Satellite System (QZSS) in Japan. Currently, there are four GNSSs: the U.S. Global Positioning System (GPS), the Russian Glonass, the European Galileo, and the Chinese Beidou systems. GPS and Glonass systems are already fully operational. Galileo declared starting the delivery of its Initial Services on 15th of December 2016 and it currently has 26 satellites in sky (as of July 2019), with 22 of them already fully operational. Beidou also has 25 satellites in sky (as of August 2018), with 23 of them operational. According to International Civil Aviation Organization (ICAO) Annex 10 [5], currently only GPS L1 frequency band and Glonass G1 frequency band are authorized in aviation, although in the future GPS L5 and Galileo E1/E5a frequency bands are expected to be used too.

The number and sources of GNSS *interference* have been growing at an alarming rate in the past few years, as the International Air Transport Association (IATA) safety report [6] and the Eurocontrol voluntary Air Traffic Management (ATM) incident report system [4], [7] pointed out recently. The low power of the GNSS signals and an increasing dependence of many modern wireless systems on satellite-based navigation attribute to that development. For example, within a time span of only three months (between March and May 2016) and at only one airport (Manila airport, in Philippines), more than 50 GPS interference incidents were reported [8]. In 2017, the GPS receivers on board of several Norwegian aircraft were jammed for an entire week in a small geographical area closed to Russia borders [9]. Again in 2018, jamming incidents have been observed in northern Finland and the Finnmark during a NATO military drill and warnings about large-scale GPS signal disruptions were issued to the civil aviation authorities [10]. According to [7], 47 times more GPS outages occurred during year 2017 compared to 2014, mainly due to various interference such as spoofing and jamming in the GPS signal.

Fig. 1 illustrates the main scenario under consideration in this survey: a scenario with a ground-placed interferer which is sending signals, shown as red arrow, into the GNSS bands

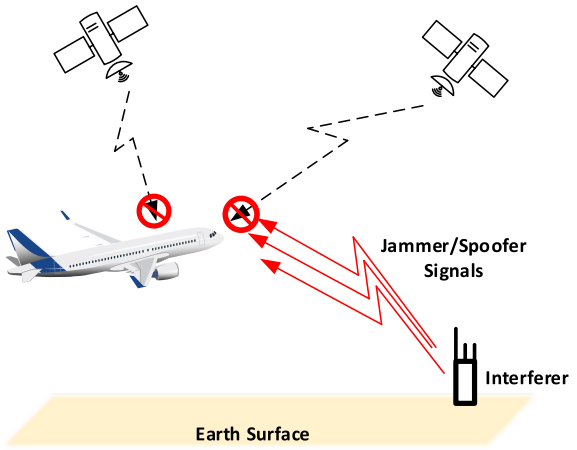


Fig. 1. Illustration of an interference scenario.

of a GNSS receiver on-board of an aircraft. The ground interference is the most typical interference location. If the interferer signal strength is powerful, the satellite signals, here illustrated in dashed lines and coming from the satellites on sky, will be destroyed by the interference and the receiver on-board of the aircraft will not be able to rely on the GNSS signals.

The rest of the paper is organized at follows. Section II defines the terminology used in this paper, describes how an astute interference management can increase aircraft safety, surveys various navigation solutions used in manned and unmanned aircraft, and gives a brief overview of SatNav principles, including the main functionalities of a GNSS receiver. Section III gives an overview of the interference classes, with a particular attention to the two main intentional interference types, namely jamming and spoofing. Section III also summarizes the related works, especially the existing surveys, which treat various types of interference. We also illustrate in a table-format how this survey brings together, for the first time in the literature, the different aspects of interference in SatNav, with focus on aviation applications. Section IV presents generic mathematical models of different types of interference encountered in SatNav as well as a detailed description of various intentional interference types. Sections V to VIII describe the main algorithms proposed in the literature so far for the detection (Section V), direction finding and localization (Section VI), classification (Section VII), and mitigation (Section VIII) of various interference types in SatNav, by pointing out their suitability and limitations when applied in aviation domain. Detailed comparisons are provided between various algorithms existing in the literature and a comprehensive discussion is included regarding the interference classification, which is a research field not yet thoroughly studied in the context of SatNav or aviation. Section IX summarizes the multitude of the performance metrics used in the literature to characterize various algorithms proposed as interference countermeasures and points out the fact that no unified analysis is currently available for the different types of algorithms and interference. We also include in Section IX several unified performance studies comparing several selected algorithms for interference detection and localization, based on both simulations and in-lab measurements. The algorithms selected for these comparative studies are the most promising ones from our extensive literature searches, according to the tradeoffs between complexity, accuracy, and feasibility analysis, under the constraint of being useful in the aviation context. Section X presents the design recommendations for dealing with interference in SatNav receivers used in aviation, under the constraint that the complexity of additional receivers to be installed on-board of an aircraft must be kept to a minimum. Section XI discusses the open challenges, the main future trends in navigation for aircraft, and the open research directions in this field. Finally, Section XII provides the conclusions.

II. Satellite Navigation Principles and Terminology

A. The Role of SatNav in Aviation and How Interference Management Can Improve Safety

Aircraft navigation has evolved over the times from magnetic compasses and beacons-based solutions, such as VOR, DME, Tactical Air Navigation System (TACAN), to GNSS and Inertial Navigation System (INS) solutions [11]. For example, DME is used to measure the distance between the aircraft and the DME station usually located in the runaway. TACAN is the combination of VOR and DME systems in a single ground station. A comprehensive overview of all these solutions is outside the scope of this paper, but Table I summarizes the main solutions of navigation for aircraft, pointing out additional references where interested readers can find out more about each of the listed technologies. From the SatNav point of view, navigation systems other than GNSS are known as Alternative Positioning, Navigation, and Timing (APNT) systems. In civil aviation, the major concern is about safety, followed by availability [12]; translated to the SatNav domain, this means that the technology is required to guarantee a certain (very high) degree of reliability and that SatNav is not the sole means for navigation. Thus, civil aviation applications rely on the use of Augmentation Systems, whose role is that of improving accuracy via differential corrections and monitoring the reliability of the information used for Positioning, Navigation, and Timing (PNT) [12], [13]. The principal augmentation system for civil aviation is the SBAS, which offers wide-area coverage (i.e., continental) for en-route and non-precision approach navigation. There exist some different SBAS worldwide, which are broadcast by geostationary satellites. They broadcast primary GNSS data, which include ranging, integrity and correction information provided by a network of ground monitoring stations. The main purpose of SBAS is to provide integrity assurance, but the use of SBAS corrections also increases the accuracy and reduces position errors to less than 1 meter. European Geostationary Navigation Overlay Service (EGNOS) is the European version of this system and the Wide Area Augmentation System (WAAS) is the United States equivalent. Other countries such as China, Japan, India and South Korea have launched their own augmentation systems or planned to do so. To support precision approach operations,

TABLE I
SURVEYS OF NAVIGATION SOLUTIONS FOR MANNED AND UNMANNED AIRCRAFT. (TECHNOLOGIES RELYING ON SATNAV ARE TYPESET IN BOLDFACE)

Survey	Year	Surveyed technologies	Aviation scenario
[18]	1947	VOR	any aircraft
[19]	1960	magnetic compass, radar	any aircraft
[20]	1965	VORTAC (combined VOR and TACAN stations) and ILS	any aircraft
[21]	1973	**GPS**, INS, VOR, TACAN, DME	any aircraft
[22]	1988	**GPS**, INS	any aircraft
[23]	1992	**GPS**, Loran-C, Omega, VOR/DME, VORTAC, TACAN, MLS, ILS, **Transit**, and radio beacons	any aircraft
[24]	1994	**GPS**, INS, INLS	any aircraft
[25]	1996	**GPS**, **DGPS**	unmanned aircraft
[4]	2012	INS, DME, UAT, VOR	any aircraft
[12]	2012	**GNSS**, **SBAS**, **GBAS**	any aircraft
[26]	2016	**GNSS**, DME and optimized DME, PWAM, pseudolites, VOR	aircraft as particular case of any transportation mode
[27]	2017	TV and audio signals (FM, AM, DAB, terrestrial ISDB), WLAN signals	UAVs in urban environments
[28], [29]	2017, 2019	5G positioning	UAVs
[30]	2019	Proprietary solutions such as Deckfinder, relying partially on **GNSS**	UAVs. General aviation (GA)

SBAS must be complemented by another local Differential Global Positioning System (DGPS) augmentation, known as Local Area Augmentation System (LAAS) or GBAS, which relies on a differential/ground network in addition to the GPS receivers on board of the aircraft [14].

The domain of commercial drones is slightly different, more focused on high accuracy and less constrained by regulations [2]. In drone domain, Real Time Kinematic (RTK) solutions are used to improve the position accuracy to centimeter-level. In addition, more recent solutions also include terrestrial-augmented signals, such as Television (TV), radio broadcast signals or WLAN signals, which are typically suitable for low-altitude vehicles only.

What clearly appears is that, as emphasized in Table I, *the SatNav solutions are key navigation solutions in modern aircraft.*

A consequence of the low power of SatNav systems, and in particular of GNSS signals used in GNSS-based navigation, is their weakness to interferences. For example, a low power (10 dBm) interference radiated by a low cost (10 Euro) jammer can block any GNSS signal within 100 m radius around the jammer, provoking the loss of GNSS navigation. In general, jamming devices can take different shapes and sizes, being typically portable/mobile. Civil, mass-market jammers can be fed by the car cigarette lighter receptacle or small batteries, their power consumption is relatively low, nevertheless, they may disrupt GNSS signal reception over distances of tens of kilometres [15]. Military jammers (electronic warfare units) are commonly high power jammers mounted on vehicles, able to cover even several thousand kilometres [15].

The consequence of GNSS jamming is the unavailability of GNSS-based navigation, which has multiple negative potential impacts on aircraft systems (navigation, Automatic Dependent Surveillance-Broadcast (ADS-B) surveillance, etc.), and therefore operational impacts specially in congested Terminal Manoeuvring Area (TMA). The number of unintentional GNSS jamming events is increasing, according to Eurocontrol Voluntary ATM Incident Reporting (EVAIR) safety bulletins based on voluntary reports of pilots in Europe. Current mitigation action implemented in commercial aircraft consists in the installation of on-board avionics providing less-precise backup navigation, e.g., conventional NavAids and Inertial Reference Unit (IRU) during loss of GNSS. Implementing additional interference mitigation solutions as those surveyed by us here can enhance the GNSS receiver performance and improve the safety of passengers.The use of conventional NavAids has been for example studied in the references given in Table I for non-GNSS solutions. Some IRU-based solutions for aircraft were described in [16]. However, these are outside the scope of our paper, as the focus here is on modern aircraft navigation solutions, based on GNSS.

Another kind of interference in SatNav is spoofing, namely the counterfeit transmission of GNSS signals radiated by a user, either intentionally malicious or unintentionally. A spoofer can make the aircraft to navigate using the counterfeit signal instead of the true one transmitted by the satellites, thus the aircraft might be re-routed on a wrong route and might create serious safety hazards to passengers and pilots. The consequence of GNSS spoofing [17] is a misleading information, i.e., an integrity issue, leading to higher severity hazards than jamming. The reported events of GNSS spoofing in aviation are still rather rare, but more and more spoofing incidents have been observed from land observations units over the past years.

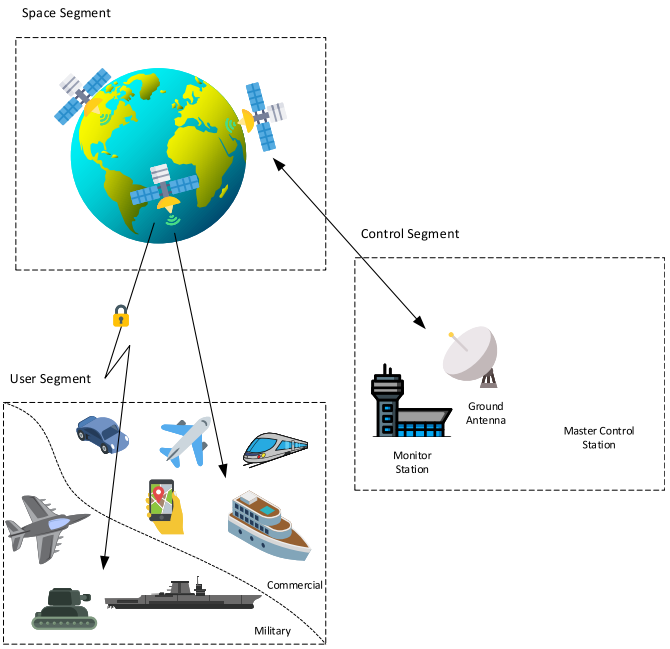


Fig. 2. GNSS three-segment architecture.

The low incidence of reported spoofing events is also partly due to the fact that such spoofing events cannot be reported by pilots because the spoofing is not currently detected or monitored on-board of the aircraft.

Therefore it is crucial to endow the future aircraft with the capability to detect, localize, mitigate and possibly classify the presence of a jamming or a spoofing signal. our survey paper gives a comprehensive overview into these interference management issues.

In addition to the safety and security aspects, if proper interference management is performed, the reduction of the number and duration of GNSS outages, and their associated traffic disruption events, will reduce the number and duration of flight delays, diversions and cancellations, and thus it will produce an increase of capacity.

B. Brief Description of SatNav Principles

The existing SatNav systems are composed of three segments: Space Segment, Control Segment and User Segment, as illustrated in Fig. 2. The Space Segment comprises the set of satellites in the space, while the Control Segment monitors the satellite operations and uplink (i.e., from ground to the satellite) commands if necessary, such as orbit or time corrections. The User Segment covers the equipment required to receive the satellite signals, e.g., a GNSS receivers installed on board of an aircraft, and computes the Position Velocity and Time (PVT) solution.

Each GNSS satellite transmits signals at several L-band frequencies between 1 GHz and 1.6 GHz approximately. The frequencies bands and their specific terminologies (i.e., L1, L2, G1, G2, etc.) of the global SatNav systems are depicted in Fig. 3. These bands are shared with other Aeronautical Radio Navigation Service (ARNS) and are known to the GNSS community under the name of Radio Navigation Satellite Service (RNSS) bands. We remind the reader that the SatNav is a wider term, encompassing the GNSS core constellation, the augmentation systems, and the local satellite systems. However, as all these additional systems rely on the same basic principles as GNSS, the terms SatNav and GNSS will be used interchangeably for the rest of the paper.

Some of the GNSS frequency bands are protected for governmental or commercial uses, such as the L2 for GPS or E6 for Galileo. It means that only authorized devices can use them. Other broadcast signals from the satellites are accessible to all GNSS receivers, meaning that they share some of the open bands, such as L1 for GPS or E1 for Galileo. Each GNSS signal is composed of.

1) Carrier: It is a radio-frequency sinusoidal signal that carries the data information at a determined frequency band in order to transmit the information through space as an electromagnetic wave.

2) Ranging Code or Spreading Code: It is a binary code, called Pseudo Random Noise (PRN), that has properties of a random signal. The different PRN codes are designed to have good auto-correlation properties but almost zero cross-correlation, thus, they allow the different satellites to transmit at the same time and frequency, as in Code Division Multiple Access (CDMA) concept used in communications [31]. The good correlation properties enable precise time measurements that translate into precise range measurements from the satellite to the receiver. Different codes of different lengths are used for each signal of each SatNav system.

3) Navigation Data: It is a message that contains information about the satellites, most importantly being the health status, the satellite position information at a given time (ephemeris), the satellite clock bias, the almanac (a reduced-precision ephemeris), and additional complementary information. The navigation message uses a much smaller data rate than the spreading code.

More details about GNSS signals and their composition can be found for example in [32] and [33]. An unified mathematical analysis for all GNSS modulations used in the GNSS open frequency bands can be found in [34].

The SatNav positioning is based on distance measurements through the so-called *trilateration* mechanism, when three measurements are used, or *multilateration* mechanism, when more than three measurements are used. Assuming that perfect time measurements are available, we can write the following,

$$r^{(k)} = c \cdot \Delta t^{(k)}, \tag{1}$$

where $r^{(k)}$ is the distance between the k-th satellite and the GNSS receiver, c is the speed of light and $\Delta t^{(k)}$ is the time it takes the signal to travel from the k-th satellite to the receiver. Thus, the true geometric distance $r^{(k)}$ can be computed from the signal's propagation time. The propagation time at its turns is obtained from the correlation of the incoming PRN code with its local replica.

The range $r^{(k)}$ in equation (1) is ideal, without error. In practice, both the receiver and satellite clocks have certain biases, deteriorating the range estimate. We denote the receiver

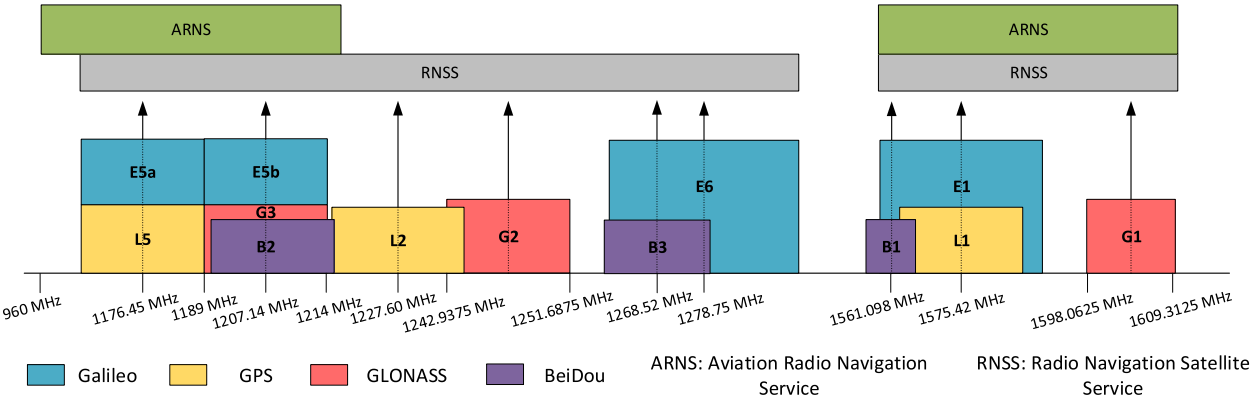


Fig. 3. GNSS frequency bands for GPS, Galileo and Glonass. It also shows which specific bands are used for other Aviation Radio Navigation systems, such as beacons-based navigation.

clock bias by τ_u and the satellite clock bias by τ_s. Further errors are caused by the propagation channel, such as the random delays introduced by the troposphere and ionosphere, multipath delays, etc. Thus, the measured range differs from the true geometric range. The measured range from the k-th satellite to the GNSS receiver is called a pseudorange $\rho^{(k)}$ and it can be expressed by

$$\rho^{(k)} = \sqrt{(x^{(k)} - x_u)^2 + (y^{(k)} - y_u)^2 + (z^{(k)} - z_u)^2} + c \cdot \tau_u + \zeta, \quad (2)$$

where $(x^{(k)},\ y^{(k)},\ z^{(k)})$ and $(x_u,\ y_u,\ z_u)$ denote the k-th satellite's position and the user position (in Cartesian coordinates), respectively, and ζ is a lumped sum of the rest of the errors occurring during the wireless propagation, such as satellite clock bias, the atmosphere effects, the multipath, the interference, and the background noise. The satellites positions $(x^{(k)},\ y^{(k)},\ z^{(k)})$ are transmitted in the navigation message. Therefore, the only unknowns in the equations are the user position $(x_u,\ y_u,\ z_u)$ and the receiver clock bias τ_u. Thus, we need at least four satellites to compute four pseudoranges and to be able to determine the four unknowns of the system of equations (2). These non-linear equations can be solved by employing closed-form solutions (e.g., Least Squares), iterative techniques based on linearisation (e.g., iterative Least Squares) or various types of Kalman filters (e.g., extended Kalman filter). The receiver position solution (2) is given in Cartesian coordinates. Then these Cartesian coordinates are transformed to geodetic coordinates; the geodetic system presents the location on the earth by its latitude, longitude, and altitude. For more details about how the user position is determined and about the various sources of errors in GNSS, the reader is referred to [32] and [33].

C. Brief Description of the Main Blocks of a SatNav Receiver

The main objective of a SatNav/GNSS receiver is to determine the PVT solution based on the received signals coming from the constellation of different satellites in view. Fig. 4 shows the block diagram of a typical SatNav receiver.

1) Antenna(s): The antenna is the first element in the GNSS receiver chain. Its aim is to collect the transmitted signal by the satellites and to make it available for the rest of the receiver blocks. Multiple antennas or antenna arrays are also possible in GNSS. A good survey of the desired features for GNSS antenna arrays can be found in [35]. Some authors consider the antennas as a part of the receiver front-end block, but in the case of multi-band GNSS, antennas tuned to a certain frequency band may come with its own front-end, thus we have plotted antennas and front-end as separate entities in Fig. 4.

2) Front-End: It is the block after the GNSS antenna, typically composed of a band-pass filter, a low-noise amplifier, a frequency converter either to an intermediate frequency or to the baseband, and possibly additional filtering stages (e.g., anti-aliasing filters).

3) Analog-to-Digital Converter (ADC): The ADC separates the analog waveform from the digital samples and performs the analog-to-digital conversion. The signal at the output of the ADC block is the signal in the so-called *pre-correlation domain*, i.e., before any correlation is performed at the receiver side. As we will show later on, most of the methods that deal with interference in SatNav are implemented in the pre-correlation stage. Strictly speaking, the ADC also belongs to the front-end, but since it plays an important role in separating the front-end techniques from the pre-correlation techniques, we decided to emphasize it separately in the block diagram of Fig. 4.

4) Acquisition Module: The objective of the acquisition module is to determine the satellites in view of the receiver and to calculate a rough estimate of parameters needed in PVT computation, such as the index of the satellites, also called Spatial Vehicles (SVs) in SatNav terminology, the coarse time-delay estimate from the satellite to the receiver, and the coarse Doppler shift estimate of the satellites in sky. These estimates will be used by the tracking modules as initial values. Acquisition in GNSS relies on correlations between the received signal and several time-shifted and frequency-shifted PRNs code replicas at the receiver. Good surveys about the GNSS acquisition can be found for example in [36]–[38].

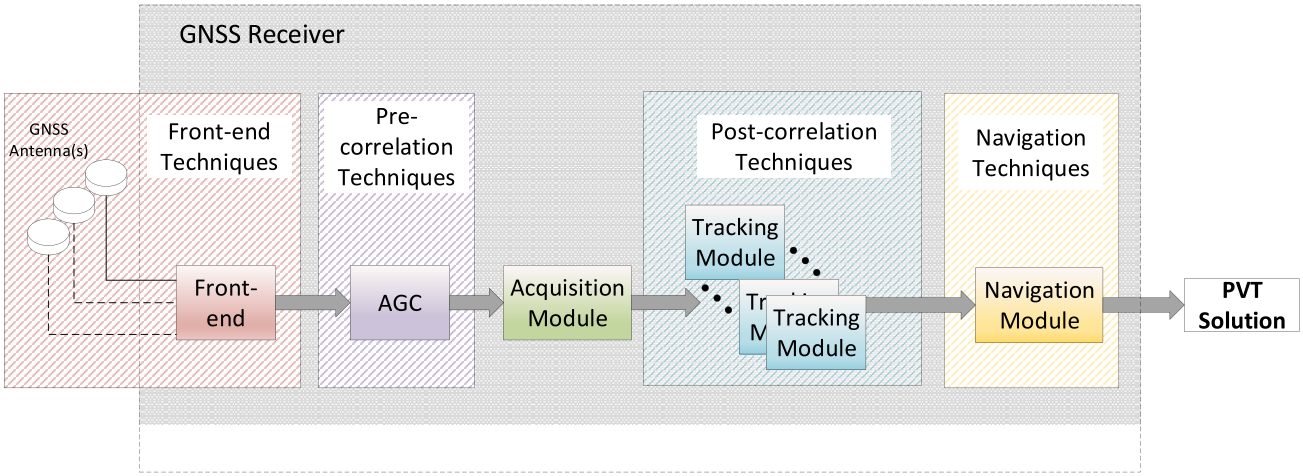


Fig. 4. Simplified block diagram of a typical SatNav receiver. The different stages shown in white boxes (front-end, pre-correlation, post-correlation, and navigation) also reflect our topology of the interference management approaches.

5) Tracking Module: The main goal of the tracking module is to refine the initial time-delays and Doppler shifts provided by the acquisition module, and to continuously track changes in any of these values. The tracking of a satellite starts only if the acquisition is successful, as some visible satellites may fly at very low orbits with respect to the receiver position on Earth or be in Non Line of Sight (NLOS) conditions, i.e., absence of a direct Line of Sight (LOS) between the satellite and receiver due to the presence of tunnels, buildings, trees, etc. During the tracking stage, accurate time-delay and Doppler shift estimates from each satellite in sky are continuously obtained, allowing the GNSS receiver to follow the dynamics of the aircraft. As at least four satellites are needed to form a position estimate, there should be at least four tracking channels in parallel, each tracking channel corresponds to one satellite.

6) Navigation Module: The aim of the navigation module is to solve the aircraft PVT solution, based on the values tracked by the tracking module and combining the information coming from all available satellites in sky.

The next section discusses in more detail the different interference types in SatNav.

III. Interference Overview

A. Interference Definitions and Classifications

Interference can be defined as any disruption of an electronic system or device due to external electromagnetic emissions at a Radio Frequency (RF) of interest, according to [39]–[41]. We remind the readers that the RF bands relevant for GNSS were shown in Fig. 3.

Interference can be classified according various different criteria. We adopt here a classification similar to [39]–[42]. This classification is shown in Fig. 5.

A top-level classification is according to the source of the interference, namely artificial versus natural interference [40]. In the artificial case, the interference is produced by various wireless transmitters, while in the natural case, the interference is due to various wireless channel effects.

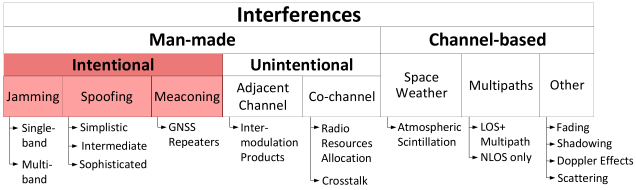


Fig. 5. Interference top-level classification.

Artificial interference can be further classified into intentional or unintentional interference, according to whether it was generated by a malicious transmitter or not. Intentional interference include jamming, spoofing, and meaconing. We further categorise unintentional interference into adjacent channel and co-channel interference. Adjacent channel interference is due to a RF emission into a different channel that leaks energy into the channel under consideration, e.g., inter-modulation products. Co-channel interference is caused by an emission of a transmitter that uses the same channel, e.g., radio resource allocation problem or cross-talk. Natural interference is due to interactions of the RF wave with obstacles on the wireless channels (e.g., through reflection, diffraction, refraction, scattering, scintillation, etc.). This can cause multi-path propagation (i.e., delayed and attenuated copies of the same signal), or ionospheric and tropospheric delays and attenuation. Space weather effects in the ionosphere, causing scintillation, are an other source of natural interference that are specific for satellite communication and navigation systems. Fading, shadowing, and Doppler effects over the wireless channel can also be seen as a form of natural interference, in Fig. 5 we collect them under the terminology of *Other*. The bottom level in Fig. 5 gives examples belonging to the different interference classes. For works on mitigating the effects of natural interference we refer to [43]–[45].

The main emphasis of our paper is on intentional interference, as emphasized in Fig. 5. *Jamming* refers to broadcasting interference signal(s) deliberately into the frequency bands of the signal of interest, typically at a higher power compared to the signal of interest. *Spoofing* refers to the

situation when a transmitter, typically installed on the ground, is sending counterfeit signals towards the receiver with the effect of tricking its user. *Meaconing* is a particular case of spoofing, it refers to re-broadcasting (i.e., 'copying') an authentic navigation signals by a malicious transmitter.

The unintentional interference includes for example out-of-band emissions of other RF systems, that are commonly harmonics of broadcast systems, but also signal leakage from Ultra-Wideband (UWB) systems, personal electronic devices, or RF systems installed close to the receiver. Many unintentional interferences can be still modelled as a 'jammer', thus jamming countermeasures are also applicable in the context of dealing with unintentional interference.

B. Literature Landscape on Intentional Interference in GNSS

This section introduces the intentional interferences in more detail and presents briefly the existing works that overview the topics of jamming and spoofing. Studies around jamming occur in a much wider context than spoofing, as the disruption of a radio link is much easier than manipulating the information link carries; whereas spoofing is specific to GNSS.

1) Jamming in the Literature: Jamming is the simplest-to-generate attack against SatNav systems among the artificial interferences. GNSS jammers broadcast an interference signal in one or several of the frequency bands used by the GNSS signals. This attack can be categorized as Denial of Service (DoS) attack, since the true GNSS signal transmission is not modified or altered. The true signal is still available but it is masked by the jammer signal, whose power is usually orders of magnitude higher than the signals coming from the satellites. The GNSS signals coming from the satellites are below the noise level, because of the large transmitter–receiver distance (around twenty thousand kilometre) that causes a high signal attenuation.

The legislation regarding the use of jammers has not yet been harmonized worldwide. A recent survey [46] showed that in Europe there are active efforts towards making the use and possession of jammers illegal, but the legal provisions are still scattered and non-unified, especially at worldwide level.

There is not a single classification for jamming signals. A possible classification is given in [47] and [48], in which the jammer signals are split in four classes according to the difficulty of detecting them. More details on jammer signals types will be given in Section IV.

Jamming has been previously studied in various contexts. Surveys on jamming attacks and possible countermeasures are available in the contexts of Wireless Sensor Networks (WSN) [49]–[52], Multi Hop Wireless Networks (MHWN) [53], Orthogonal Frequency Division Multiplexing (OFDM) communications [54] and Long-Term Evolution (LTE) cellular communications [55]. Potential benefits of jamming in WSN have also been surveyed [56].

While works that survey the field of jamming in SatNav are not available, the studies in [48], [57]–[60] give nonetheless a good overview of issues caused by jamming and potential solutions as detailed below.

The authors of [48] address the negative impact of jamming on the GNSS receiver performance and present three classes of jamming detection: at Automatic Gain Control (AGC) level, at digital pre-correlation signal processing level, and at post-correlation domain level. However, no comparative performance analysis between these three different detection classes is provided, the main take-away message being that the interference detection can be done at different stages of the receiver.

Gao *et al.* [57] give a broad overview about increasing the robustness of GNSS in the presence of jamming and discuss INS/GNSS-coupled navigation, spatial filtering, and time-frequency filtering vector tracking. Again, no comparative performance between the different algorithms is given and the conclusions state that any of the studied approaches is beneficial for GNSS and they can detect or mitigate jamming.

Jamming mitigation based on beamforming techniques with multi-antenna GNSS receivers is the focus of [58]. While all the tested multi-antenna Controlled Radiation Pattern Antenna (CRPA) techniques are shown to be much better than single-antenna techniques, no winning technology among the studied beamformers was selected. Amin *et al.* [59] discuss the use of sparse arrays and sparse sampling to mitigate jamming in the context of GNSS. They use a co-array framework on single and multiple-antenna/CRPA receivers for improved beamforming, in order to estimate the jamming signal's Angle of Arrival (AoA) and to suppress it. In [60] the localization of jammers is addressed, and different approaches based on AoA, Time Difference of Arrival (TDoA), Frequency Difference of Arrival (FDoA) and Received Signal Strength (RSS) were described and compared qualitatively. No quantitative analysis in terms of performance metrics was provided.

2) Spoofing and Meaconing in the Literature: Spoofing is a more complex attack against SatNav systems than jamming. Spoofing attacks simulate or modify the true GNSS signals and rebroadcast it back. By doing this, the attacker can modify the PVT solution at his/her will. The awareness about the vulnerability of satellite positioning to signal forgery dates back to 2001–2003, with the well known Volpe report [61] and the paper [62]. But it is in the last ten years, since the proof that a spoofer fooling the civil GPS signals can be developed with low cost components [63], that the public interest has raised and literature production about GNSS spoofing aspects has significantly increased. More details on spoofing signals types and their mathematical models will be given in Section IV.

In chronological order, [64]–[71] represent in the authors' opinion the most updated technical surveys currently available on the topic of spoofing. In these works it is possible to recognise a common approach to address the subject: the type of forgery is discussed first, by describing *a)* the possible alterations induced on the GNSS signals and *b)* the Hardware (HW) and Software (SW) ways to inject them, together with considerations about the technical difficulties to execute the attack. Secondly, the vulnerability of the state-of-the-art signals and

receivers is addressed. Finally, the vast panorama of the counteracting measures is investigated and classified according to various metrics.

Understanding the mechanism for which the spoofer can introduce false information in the received signal is the first step to design proper countermeasures. For this reason all the previous surveys discuss a classification of the possible characteristics of the falsified signal, in terms of:

- methods and technologies to generate it [64],
- options to inject it in the received signal ensemble [64], [65],
- modifications induced on the received signal [65], [69]–[71],
- assessment of the level of technical difficulty to carry the spoofing attack [65], [69], [71].

The studies [65], [69], [70] provide the mathematical formulation of various types of attacks, leading to their classification [65], [71]: the major distinction is made between *meaconing* and various options of *spoofing*, which basically differ for either the signal content they aim at altering, or the strategies they implement to achieve their goals. The classification adopted here follows, in a slightly simplified manner, the mentioned references.

The complexity of the equipment setup necessary to carry out a GNSS spoofing attack is recognized as a non-negligible factor in the assessment of the potential danger: attacks with high level of associated complexity are less likely to be implemented on a large scale, or to low-revenue (under the spoofer's perspective) applications. In this light, [65], [69], [71] discuss evaluations of costs/difficulty associated to different kinds of attack.

The vulnerability of a receiver to a spoofing attack is explicitly addressed in [64], [65], which analyse the conditions in which a receiver may be deceived by false signals. Reference [64] investigates the vulnerability of the signal structure, identifying which signal components could be victims of forgery, namely the data bits and the pseudorange measurements. To obtain its goal, the malevolent spoofer takes advantage of the vulnerability of the civil GNSS at the signal processing level, since the signal structure is publicly known.

The survey [65] identifies the receiver vulnerabilities depending on the signal processing stage in which the receiver operates at the time of the onset of the attack; from that analysis, the tracking stage results the less vulnerable condition for a receiver, while the cold start offers the widest opportunities to the spoofer to succeed. This is the reason for which a feasible spoofing scenario often includes a preliminary jamming phase, used to force the receiver in a re-acquisition phase which leaves more room to vulnerability. In this light, [65] highlights the significant difference between *tracking receivers* and *snapshot receivers*; the former continuously estimate the frequency, delay, and phase of the signal, i.e., they extensively use prior knowledge about the signal; on the contrary the later sample the incoming signal in non-adjacent time windows and use each ordered set of samples to produce an estimate of the signal parameters. As a consequence, with respect to vulnerability, snapshot receivers behave like the acquisition stage of tracking receivers, and so they are particularly vulnerable to spoofing [65].

What is apparent from all the mentioned surveys is that in most cases vulnerability is a matter of lack of cross-checks and monitoring measures: since spoofing attacks realistically leave traces, the winning game should be the implementation of a number of "check points" in the receiving chain, where different metrics can be monitored in order to extract clues on the presence of non-authentic signals [40].

Finally, with a remarkable effort of correlating the many aspects discussed so far, [69] presents an instructive assignment of 'implementation costs' to spoofing attacks and defence techniques, also ranking the effectiveness of each technique against each attack; in this way a receiver manufacturer should be enabled to decide which spoofing defence to implement in its receiver, consciously trading-off among implementation costs, achievable level of protection and likelihood of the non-protected attacks.

C. Classifications of Interference Management Solutions in GNSS

We start this section with a classification of countermeasures to GNSS interference and conclude our overview with the possible countermeasures to interference. The discussion in this sub-section is also summarized in Fig. 6, which explains in a visual manner in which sections of this paper we address each countermeasure.

One possible classification of the interference countermeasures found in the literature is the following: *a)* countermeasures at the *user level* and *b)* countermeasures at the *system level*.

User-level techniques represent the huge majority, because they are built on the algorithms implemented in the receivers, as a product of the designers' ingenuity. Such techniques are first identified as *detection* or *mitigation* techniques, where the former category refers to algorithms that focus on discriminating between interference and the desired signals without performing countermeasures, while the latter "neutralizes the detected spoofing signals and helps the victim receiver to retrieve its positioning and navigation abilities" [64]. The first stages towards applying a countermeasure to the interference present in GNSS are the *modeling* of various possible interference classes and the interference *detection*, shown in Fig. 6. The next steps, also illustrated in Fig. 6 and ordered from lower to higher capability are *direction finding/localization*, *characterization/classification*, *monitoring/mitigation*. The classification shown in Fig. 6 is also similar to the one in [70], where the authors use detection, characterization/classification, monitoring, and mitigation. The purpose of each of the stages illustrated in Fig. 6 is as follows.

1) Interference Modeling: refers to the ability of modeling the interference mathematically, according to certain parameters, such as the interference bandwidth, interference carrier frequency, etc.

2) Interference Detection: refers to the ability to detect the presence of an interferer in the useful signal. The jammer

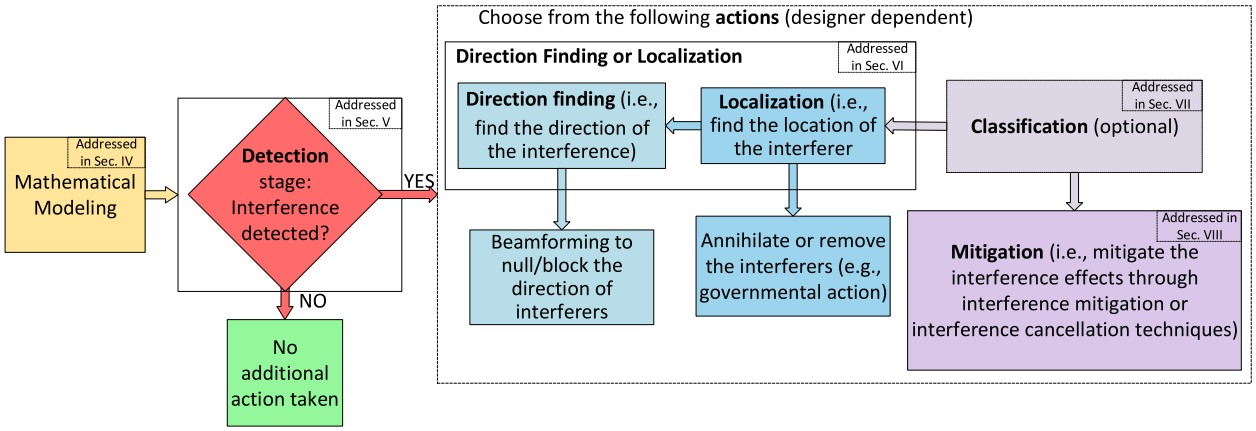


Fig. 6. Stages in dealing with artificial interference in Satellite Navigation. These stages are also reflected in the structure of Sections V-VIII of this paper.

detection problem can be typically reduced to the classical detection problem of a signal in noise [72], [73], where the jammer becomes the 'useful signal' and the GNSS becomes the 'noise'. The spoofing detection is a matter of smarter signal processing than the jammer detection, based on the idea that the perfect forgery is practically unfeasible and the injection of non-authentic signals in a receiver leaves traces [74]–[76]. Such traces can be detected with astute signal processing methods, as described later in Section V.

3) Interference Direction Finding: refers to the ability of finding the angles or directions of the interference source. Such information could help for example in blocking all sources coming from that particular direction.

4) Interference Localization: refers to a more accurate estimation of the interference source, in terms of its accurate latitude, longitude, and altitude. Knowing the exact location of the interferer can enable robust interference removal methods, such as governmental procedures to get rid of the interference sources coming from that particular location;

5) Interference Classification: refers to the ability of acquiring knowledge about the type and characteristics of the interferers (e.g., carrier frequencies, modulation types, etc.). Such knowledge can enable more efficient interference mitigation algorithms;

6) Interference Mitigation: refers to various methods of diminishing or cancelling out the interference. This step can be in fact use in conjunction with any of the above-mentioned steps, or it can be also applied as a separate step.

We remark that some of the steps illustrated in Fig. 6 can be skipped out completely, according to the designer and to the operation conditions and assumptions. For example, in the case of a dual-frequency GNSS receiver where the interferer affects only one of the two frequencies, the receiver can operate only with an interference detection scheme: if the detector indicates that the interference is present in only one frequency band, the receiver will switch to a single-frequency operation, otherwise the receiver will operate in a dual-frequency mode. An other example is to find the direction of the Radio Frequency Interference (RFI) source and suppress its signal through beamforming. In that case, localizing the source might not be necessary anymore.

Among the *system-level techniques*, it is worth mentioning the European system Galileo, which plans to introduce an authentication service in some of its signals, so as to implement a *system-level* anti-spoofing approach. A description of the principles of the *cryptographic defence* which is at the basis of the authentication services can be found in [70], while [71] offers deeper details on specific techniques, in particular the Navigation Message Authentication (NMA) and Spreading Code Authentication (SCA); it also presents an interesting *threat analysis*, i.e., an evaluation of the robustness of such techniques against a list of types of attack. Also the GPS standardization committee has recently started to work on the definition of an authentication component for its newer L1C signal, a modernized civilian signal in L1 frequency band.

Another possible classification of interference countermeasures or management solutions is according to the block diagram in Fig. 4, where the classification of the countermeasures follow the GNSS receiver stages, namely:

- Front-end techniques,
- Pre-correlation techniques,
- Post-correlation techniques,
- Navigation techniques.

In our paper we will group the following sections according to the top-level classification shown in Fig. 6, and then, under each section, we will follow the algorithm classification according to the receiver stages shown in Fig. 4, as, in our opinion, such approach gives the clearest understanding to a potential designer regarding the interference countermeasures.

D. Current Gaps in the Existing Literature

Table II summarizes the main existing surveys and articles on GNSS interference management solutions and compares the work provided in our survey with existing work. Empty entries in the table means a not-available or not-applicable information.

As seen in Table II, typically, the existing surveys focus on only one of the two main interference types (i.e., jamming and spoofing) in GNSS and very often only one or two steps of the four interference countermeasures illustrated in Fig. 6. A few studies cited in Table II also address co-channel

TABLE II
SUMMARY OF RELEVANT WORK ABOUT GNSS ARTIFICIAL INTERFERENCE. THE ✓ AND ✗ SYMBOLS IN THE SECOND COLUMN CORRESPOND TO THE REFERENCES LISTED IN THE FIRST COLUMN

Relevant research papers and other surveys	Specific for aviation	Year	Intentional interference in SatNav		Unintentional interference in satnav		Generic interference type
			Jamming	Spoofing and Meaconing/Repeaters	Adjacent-band interference/Out-of-band emission and harmonics frequency interference	Co-channel interference in GNSS bands	
[77]	✓	1971					Passive emitter localization
[78]	✗	1983					Continuous Wave Interference (CWI) interference suppression
[79]	✗	1984	Jamming mitigation				
[80]	✓	1998	Backup systems to deal with jamming in GNSS				
[81]	✗	2000					Wideband interference suppression
[82], [83]	✓,✓	2000–2002	Jamming detection and localization				
[84]	✗	2003			UHF/VHF interference localization		
[85]–[87]	✓,✗,✓	2005, 2005, 2012	Jamming mitigation				
[88]	✓	2008	Jamming detection				
[89]–[91]	✓,✗,✓	2008, 2015, 2018	Jamming mitigation			Radar, JTIDS/MIDS and DME/TACAN interference mitigation	
[92]	✗	2009		Spoofing effect on positioning			
[93]	✗	2010			Interference assessment of DVB-T within GNSS bands		
[94]	✗	2011	Signal characterization of jammer types				
[64]	✗	2012		Spoofing characterization and anti-spoofing techniques			
[95]	✗	2012			LTE harmonics interference avoidance in GNSS		
[60], [96], [97]	✗	2012, 2015, 2017					Interference detection and localization for generic RFI interference
[98]	✗	2013	Jamming detection and localization				
[65], [99], [100]	✗,✗,✗	2014, 2017, 2018		Spoofing assessment and mitigation			
[101]	✓	2016	Jamming mitigation			Self-interference from UAV's on-board system	
[48], [97]	✗,✗	2016, 2017	Jamming detection				
[59], [102]	✗✗	2016, 2017	Jamming direction finding and mitigation				
[103]	✗	2016	Jamming localization	Spoofing and meaconing localization			
[68], [69], [71]	✗,✗,✗	2016,2017		Spoofing/meaconing detection, classification, and/or mitigation			
[70]	✗	2016	Jamming detection and mitigation	Spoofing/meaconing detection and mitigation			
[104]	✗	2017			Interference assessment of LTE for different classes of GNSS receiver		
[105]	✗	2018	Jamming mitigation				
Our Survey	✓	–	Jamming detection, localization, classification, and mitigation	Spoofing and meaconing detection, localization, classification, and mitigation	RF harmonics detection, localization, classification, and mitigation	Wideband detection, localization, classification, and mitigation	Generic interference modelling, detection, localization, classification, and mitigation

and adjacent channel interference in GNSS. Less than one fifth of the listed surveys in Table II focus on aircraft-oriented interference countermeasures and no literature survey exist, to the best of the authors' knowledge, that summarizes the various interference types encountered in GNSS and that explicitly deals with the four stages to counteract this interference,

namely detection, localization, classification, and mitigation. For clarity, we have lumped together the direction finding and localization algorithms, as the direction finding can be seen as a particular case of the localization (when only the interference direction is estimated, but not its exact location).

Ioannides *et al.* [70] study the impact of jamming and spoofing on critical infrastructure relying on GNSS. They also overview several detection and mitigation measures at receiver and system-level and they discuss policy and regulatory actions. However, no performance metrics are investigated in [70] and no comparative performance analysis between different algorithms is given. The conclusions in [70] is that jamming and spoofing are major threats in GNSS nowadays and that there is a high need in the research communities to study and provide efficient countermeasures to them in the future.

By contrast with the published related work over the 15 last years, as summarized in Table II, our survey addresses in detail various algorithms proposed to deal with any type of interference in GNSS and discusses their suitability for various interference types as well as their suitability to be used in aviation context. In addition, unified mathematical models of GNSS interference and performance comparisons between several algorithms based on similar performance metrics are lacking from the current literature and our survey also addresses this lack.

IV. Modelling Artificial Interferences

Let us consider the signal $r(t)$ reaching a GNSS receiver on-board of an aircraft. Such a signal can be modeled generically as

$$r(t) = g(t) + j(t) + s(t) + \xi(t), \tag{3}$$

where $g(t)$ represents the signals of interest for the GNSS receiver transmitted by the GNSS satellites, $j(t)$ is a possible jamming signal including adjacent-band interference (e.g., harmonics from other systems close to GNSS bands) and $s(t)$ denotes a possible spoofing signal. The background noise over the wireless propagation channel is modeled as AWGN and denoted by $\xi(t)$.

A. Jamming Signal Models

According to literature, e.g., [47] and [48], the following jammer classes can be encountered. The first four classes are classified according to the difficulty to detect them, from lowest to highest difficulty, while the last one incorporates the jammer types not fitting in the first four classes.

1) Class I, Continuous Wave (CW) Jammers: The simplest type of jammers and the most studied ones are those based on CW modulation. CW modulations typically refer to signals with bandwidth up to 100 kHz. CW class includes the amplitude modulated and frequency modulated jammers, and they typically are the easiest jamming signals to deal with. Class I includes the single-tone and multi-tone jammers. A multi-tone jammer, see Eq. (5), consists of $k = 1, \ldots, K$ of single tones (Eq. (4)) and is characterized by P_{J_k}, f_{J_k} and θ_{J_k}, the power at the antenna, and the corresponding frequency and phase of the k-th jammer component. In addition, the class I also includes single- and multi-tone Frequency Modulation (FM) jammers (see Eq. (6) and (7)), for which the frequency is time dependent. This incorporates β_k into the signal model, the modulation index of the k-th tone.

2) Class II, Single Saw-Tooth Chirp Jammers: The second category of jammers contains signals whose frequency is modulated linearly over time. They are constructed by sweeping linearly through a certain frequency range in a certain time period after which the process is started again at the initial frequency. They are also known as swept CW signals, or simply (saw-tooth) chirp jammer. As a side note, this type of jammers have a similar mathematical modeling as the signals used in most radar systems, but with a different carrier frequency. Class II contains linear FM signals (saw-tooth chirps), here also named Single Chirp for the sake of brevity. The Single Chirp is modeled by Eq. (8). The parameters are the jamming power P_J, the starting frequency of the sweep f_J (at time $T_{\text{sweep}} = 0$), the minimum and maximum frequency of the frequency sweep $f_{\min}$ and $f_{\max}$ and the sweep period T_{sweep}, which is the time it takes the jammer to sweep from $f_{\min}$ to $f_{\max}$. The variable $b = \pm 1$ is a flag determining if we have an up-chirp ($b = 1$) or a down-chirp ($b = -1$), θ_J denotes the initial phase of the jammer and $f_q(t) = 2\pi f_J t + \pi b \frac{(f_{\max} - f_{\min})}{T_{\text{sweep}}} t^2$ is the instantaneous frequency of the jamming signal.

3) Class III, Multi Saw-Tooth Chirp Jammer: A third category of jammers is the category of multi saw-tooth chirps, representing the weighted sum of two or more single-chirp jammers, transmitted at the same time. Class III includes multi-component linear chirp signals, named as Multi-Chirp in Table III. The parameters of Eq. (8) are: b_k, a flag (± 1) indicating an up or down chirp; f_{J_k} the frequency of the k-th chirp and θ_{J_k}, the initial phase of k-th chirp.

4) Class IV, Chirp Signals With Frequency Bursts: A fourth category of jammers is the chirp with frequency bursts, when the frequency bursts are used to expand the frequency band affected by the jammer. The jamming signals in class IV are also frequency modulated signals, but the modulating signal takes more complex functions. The signals of class IV are described by Eq. (9). The main parameter for a class IV jammer type is the instantaneous frequency of the jamming signal $f_q(t)$, which typically has a periodic pattern.

5) Class V, Other Jammer Types: This class of jammers contains the jammer type not fitting in any of the above mentioned classes, such as jamming signals that are active only during repetitive periods of time with an active period of a pulse called 'duty cycle' (these are the DME-like or pulse jammers), or narrowband noise jammers.

The corresponding baseband models of these jammer classes are given by us in Table III in a unified manner.

An example of the Power Spectrum Density (PSD) and the corresponding spectrogram of a single Amplitude Modulation (AM)-tone jamming signal at 1.023 MHz is shown in Fig. 7(a) and Fig. 7(b), respectively. An example of the PSD and spectrogram for multi-tone FM is shown in Fig. 7(e) and Fig. 7(f), respectively. The PSD and the spectrogram of an up-chirp jammer with 10.6 MHz sweep range and 8.64 μs sweep period,

TABLE III
JAMMING SIGNAL MODELS. THE SUBSCRIPTS IN THE CASE OF SINGLE-COMPONENT SIGNALS ARE DROPPED FOR CLARITY

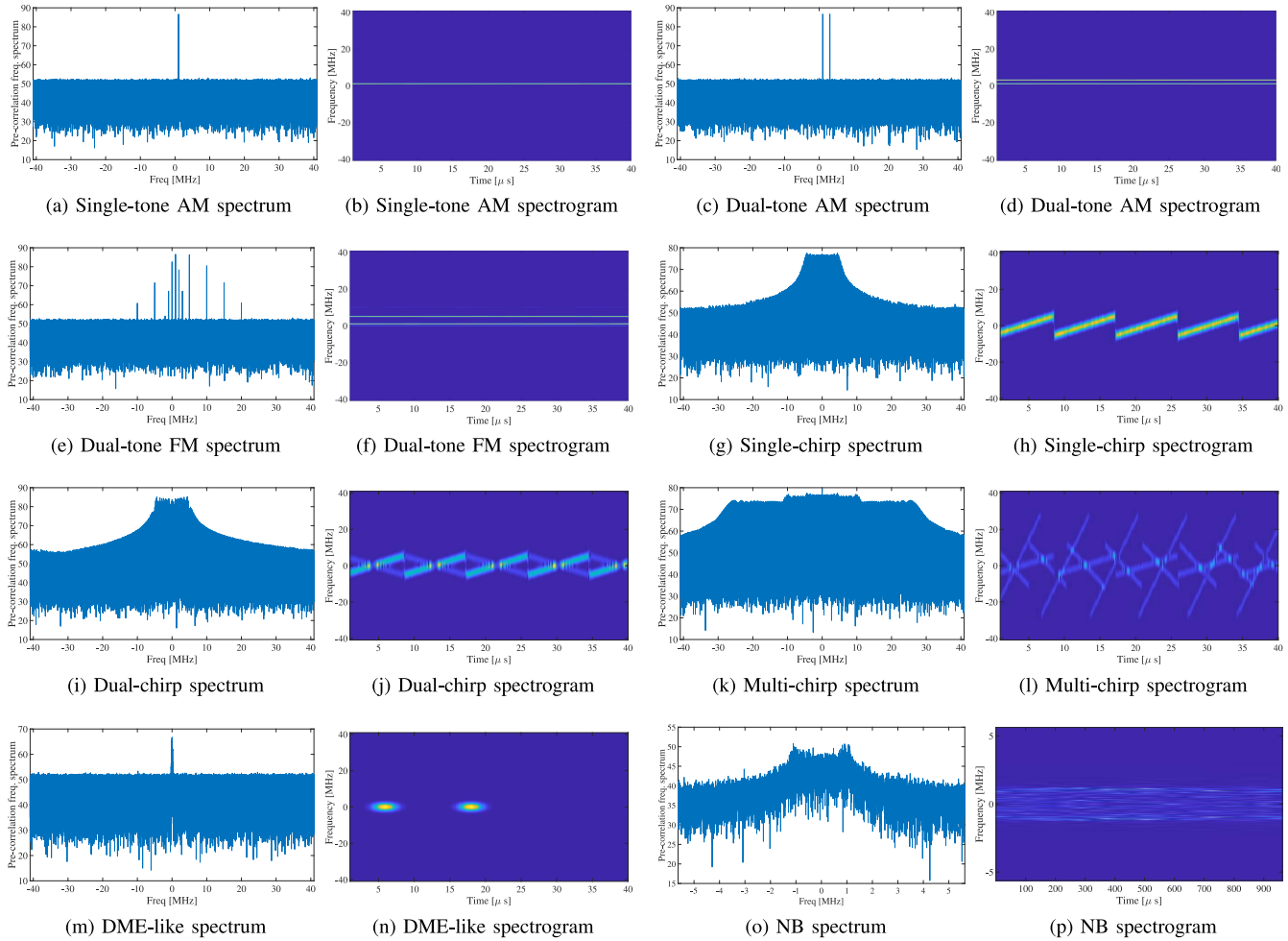
Jammer class	Jammer Type	Jammer baseband model		Unknown Parameters
Class I	Single-Tone AM	$j(t) = \sqrt{P_J} \cdot \exp(j(2\pi f_J t + \theta_J))$	(4)	f_J, P_J, θ_J
	Multi-Tone AM	$j(t) = \sum_{k=1}^{K} \sqrt{P_{J_k}} \exp(j(2\pi f_{J_k} t + \theta_{J_k}))$	(5)	f_{J_k}, P_{J_k}, θ_{J_k}, and K, with $k = 1, 2, \ldots, K$
	Single-tone FM	$j(t) = \sqrt{P_J} \cdot \exp(j(2\pi f_J t + \beta \cdot \sin(2\pi f_J t)))$	(6)	f_J, P_J, β
	Multi-Tone FM	$j(t) = \sum_{k=1}^{K} \sqrt{P_{J_k}} \exp(j(2\pi f_{J_k} t + \beta_k \cdot \sin(2\pi f_{J_k} t)))$	(7)	f_{J_k}, P_{J_k}, β_k, and K, with $k = 1, 2, \ldots, K$
Class II	Single Chirp	$j(t) = \sqrt{P_J} \cdot \exp(j(2\pi f_J t + \pi b \frac{(f_{\max} - f_{\min})}{T_{\text{sweep}}} t^2 + \theta_J))$ $= \sqrt{P_J} \cdot \exp(j(f_q(t)t + \theta_J))$		f_J, P_J, b, T_{sweep}, $f_{\min}$, $f_{\max}$
Class III	Multi-Chirp	$j(t) = \sum_{k=1}^{K} \sqrt{P_{J_k}} \exp(j(2\pi f_{J_k} t + \pi b_k \frac{(f_{\max_k} - f_{\min_k})}{T_{\text{sweep}_k}} t^2 + \theta_{J_k}))$	(8)	f_{J_k}, P_{J_k}, b_k, T_{sweep_k}, $f_{\min_k}$, $f_{\max_k}$, and K, with $k = 1, 2, \ldots, K$
Class IV	Chirp Signals with Frequency Bursts	$j(t) = \sqrt{P_J} \exp(j(f_q(t)t + \theta_J))$	(9)	Shape and parameters of $f_q(t)$, P_J, θ_J
Class V	DME-like/Pulse Jammer	$j(t) = \sqrt{P_J} p_\tau(t) \otimes \sum_{k=1}^{K} \delta\left(t - \frac{k}{f_{r_k}}\right) \cdot \exp(j2\pi f_{J_k} t)$	(10)	τ, P_J, f_J, f_r, K
	Narrowband Jammer	$j(t) = \sqrt{P_J} \cos\left(2\pi f_J t + \beta \int_0^t n(\zeta) d\zeta + \theta_J\right)$	(11)	P_J, f_J, β, θ_J shape and statistics of $n(\cdot)$

is shown in Fig. 7(g) and Fig. 7(h). The PSD and spectrogram for a dual-chirp and a multi-chirp signal are illustrated in Fig. 7(i), Fig. 7(j), Fig. 7(k) and Fig. 7(l), respectively. Comparing the PSDs of the multi-chirp with that of the single-chirp in Fig. 7(g), we can observe that their PSDs cannot be distinguished and, thus, we cannot pinpoint the type of a chirp signal based on solely on the spectrum. This is due to the fact that chirps are non-stationary signals. Only time-frequency analysis, such as the spectrogram, can help distinguishing different chirps. From class V type of jammers, we exemplify a pulsed tone (or DME-like) jammer and a narrowband jammer. The DME-like jammer refers to interference signals that are active only during repetitive periods of time. The active period of a pulse is called duty cycle. This jammer type is modeled by Eq. (10), where $p_\tau(t)$ is a rectangular pulse of width τ (the duty cycle), f_r is the pulse repetition frequency, $\delta(t)$ is the Dirac pulse and $\otimes$ is the convolution operator. Fig. 7(m) and Fig. 7(n) show examples of the PSD and the spectrogram for DME-like jammers. Last but not least, a narrowband jammer is a generic jammer with a narrowband spectrum, obtained for example by transmitting a previously modulated RF carrier wave with random amplitude or frequency changes. The narrowband-noise jammer can be modeled as shown in Eq. (9), where β is the modulation index and $n(\zeta)$ represents a stationary random process with zero mean and σ_ζ^2 variance.

B. Spoofing and Meaconing/Repeater Models

The authors of [64] identify three classes of spoofing generation techniques, derived from [106].

1) Simplistic Spoofing Attacks: The simplest spoofing attacks against GNSS can be carried out by means of a GNSS signal generator connected to a transmitting antenna.



(a) Single-tone AM spectrum (b) Single-tone AM spectrogram (c) Dual-tone AM spectrum (d) Dual-tone AM spectrogram

(e) Dual-tone FM spectrum (f) Dual-tone FM spectrogram (g) Single-chirp spectrum (h) Single-chirp spectrogram

(i) Dual-chirp spectrum (j) Dual-chirp spectrogram (k) Multi-chirp spectrum (l) Multi-chirp spectrogram

(m) DME-like spectrum (n) DME-like spectrogram (o) NB spectrum (p) NB spectrogram

Fig. 7. Spectra and spectrograms of common jamming signals in baseband. All graphs contain a signal mixture of jamming signal and Galileo E1 signal, where the C/N_0 is 50 dB and the JSR is 40 dB.

A receiver could be fooled by such signal generator, especially if the target receiver is jammed and forced to reacquire the satellites. Such spoofing attack may be quite expensive, due to the fact that it requires specific HW such as a GNSS signal generator, which can be expensive (e.g., up to hundreds of thousands of dollars) and it is not easily portable. In addition, such attack can be easily detected, since generally it does not synchronize the spoofing signals with the signals from the GNSS satellites in view. Therefore pseudorange, C/N_0 and Doppler jumps can occur and inconsistencies can be found to signal a spoofing attack. In the civil aviation context, such non-aligned signal ensemble received from a distant spoofer could be a possible scenario because of two reasons: 1) the fine alignment of the forged signals with respect to a very distant user in movement is difficult to achieve; 2) the spoofing attack could address non-civilian targets while just erroneously reaching civilian ones.

2) Intermediate Spoofing Attacks: This category contains more complex attacks than the previous one. They combine a GNSS receiver with a digital processor and a transmitting RF front-end. The spoofer is able to synchronize the frequency and align the code-phase between the real and the counterfeit signals. When the signals from the satellites are tracked by the attacker receiver, the attacker receiver has a perfect knowledge of both the Doppler shift and the spreading code delay of the legit satellite. In principle, any GNSS receiver, properly modified, can be converted into a spoofer device. This type of spoofer is able to adjust the signal strength of the counterfeit signals, in order to simulate signal levels compatible with satellite transmissions. The aircraft receiver is not able to distinguish the counterfeit signal from the genuine one, since the spoofer accurately reproduces the code phase, frequency, and navigation data bits. The navigation bit reproduction requires a procedure of bit prediction and estimation to perform the attack in real-time. Today an intermediate spoofing attacks can be built with SW parts and RF components readily available on the market for limited cost; nonetheless, a deep knowledge of GNSS signal processing is required to correctly setup the signal processing chain. In the civil aviation context, such kind of attacks is less probable for the time being, because: 1) the fine signal alignment requires the on-board presence of a cumbersome equipment, to receive, process and rebroadcast the forged signal; 2) if the forgery source is distant from the aircraft, the compensation or the aircraft dynamics can be quite difficult; 3) GNSS jamming and spoofing monitors should be installed and active in the airport area, where either

TABLE IV
SPOOFING BASEBAND SIGNAL MODELS

Spoofer class	Baseband signal model (per satellite)		Unknown parameters
Simplistic Spoofer	$s(t) = \sqrt{P_s} \sum_n d_n c_n (t - \tau_{\text{sp}}) \exp(j2\pi \Delta f_{\text{sp}} t + \Psi)$	(12)	P_s, d_n, τ_{sp}, Δf_{sp}
Intermediate Spoofer	$s(t) = \sqrt{P_s} \sum_n \hat{b}_n c_n \left(t - \hat{\tau} - \tau_{\text{sp}}\right) \exp(j2\pi \left(\hat{f}_D + \Delta f_{\text{sp}}\right) t + \hat{\Psi})$	(13)	P_s, τ_{sp}, Δf_{sp}
Sophisticated Spoofer	$s(t) = \sum_{k=1}^{K} \sqrt{P_s^{(k)}} \sum_n \hat{b}_n c_n \left(t - \hat{\tau} - \tau_{\text{sp}}^{(k)}\right) \exp(j2\pi \left(\hat{f}_D^{(k)} + \Delta f_{\text{sp}}^{(k)}\right) t + \hat{\Psi}^{(k)} + \Phi^{(k)})$	(14)	K, $P_s^{(k)}$, $\tau_{\text{sp}}^{(k)}$, $\Delta f_{\text{sp}}^{(k)}$, $\Phi^{(k)}$
Meaconer	$s(t) = \sqrt{P_s} \sum_n b_n c_n \left(t - \tau - \tau_{\text{sp}}\right) \exp(j2\pi f_D \left(t - \tau - \tau_{\text{sp}}\right) + \Psi)$	(15)	P_s, τ_{sp}

the aircraft could be still or the take-off/landing paths are more predictable.

3) Sophisticated Spoofing Attacks: Sophisticated spoofing consists of a coordinated and synchronized attack carried out by different spoofing devices [106]. This type of attack is the most complex to implement and deploy, and the most expensive and difficult to perform. It is also the hardest to defend against. In this attack, the spoofing devices act as a beamforming antenna array, simulating the different AoAs for different satellites. This can be accomplished either by keeping each spoofer fixed and transmitting the signals of all satellites with appropriately calculated delays compatible with the receiving antenna, or by having each spoofer transmitting the signal of exactly one satellite and mechanically moving the spoofer around the target receiver. Implementing sophisticated attacks based on multiple intermediate spoofers is possible, but very hard to manage. In the civil aviation context, as well as in many other contexts, the likelihood of such an attack is considered particularly low, because of the technical complexity required by the implementation and the logistic problems implied by the simultaneous operation of multiple spoofing devices, especially in dynamic scenarios.

4) Meaconing: Meaconing is a particular case of spoofing, consisting in the interception and re-broadcast of true GNSS signals (or the recording and playback) with enough gain to overwhelm the true signal at the target antenna. This attack does not modify the signals, so the target receiver's PVT solution becomes the PVT solution of the meaconer, with a rebroadcasting delay. Although the arrival of the signal at the target GNSS receiver is delayed, the aircraft receiver might not be able to compute its true PVT solution. Through a meaconing attack even an encrypted GNSS signal (such as the military L2 in GPS or E6 in Galileo) can be attacked, since a meaconing attack only rebroadcasts the authentic signals. This kind of attack is generally easy to implement, since it only requires a few RF components. In the civil aviation context, meaconing has a certain probability of being encountered, not only as an attack explicitly targeting the aircraft, but also as an 'uninformed' interference caused with other purposes. For example, if the GNSS repeaters used in hangars are not accurately shielded electromagnetically, they can be perceived as 'uninformed' meaconers in airport areas. Also anti-drones meaconers in military sensible zones (e.g., borders, contended sea areas) could affect civil aircraft along their flights.

Table IV summarises the mathematical models of the signals generated by the various types of spoofers discussed above. The given equations refer to the signal model for one forged satellite at a time; to be effective, spoofers simultaneously produce many such signal models, one for each satellite in view.

Eq. (12) shows the signal model for a simplistic spoofer attack, where P_s is the spoofer power, mimicking the power of the authentic satellite signal; n is the index of the current data bit; d_n are the data bits generated by the spoofer; in the simplistic attack they are different from the true b_n data bits sent by the satellites on sky; $c_n(t)$ is the pseudo-random code that modulates the n-th data bit, possibly including BOC modulation, corresponding to an authentic satellite code; notice that the summation over n cover non-overlapping waveforms in time; $\tau_{\text{sp},n}$ is time delay introduced by the spoofer; it may vary with the time, although for simplicity of notation the dependence on the time t is dropped here; Δf_{sp} is the frequency shift introduced by the spoofer in the simplistic and intermediate attacks; as for τ_{sp}, it may be a function of the time; finally Ψ is the carrier phase offset for the selected satellite to forge. Eq. (13) shows the model for an intermediate spoofer attack where $\hat{b}_n$ is the estimated data bit (at the spoofer end) of the n-th transmitted bit of the selected satellite to forge, $\hat{\tau}$ is the spoofer estimated value of the true code delay, $\hat{f}_D$ is the spoofer estimated value of the true Doppler frequency shift and $\hat{\Psi}$ is the estimated carrier phase at the spoofer's end. Eq. (14) shows the model for a sophisticated spoofer attack

executed with K coordinated and synchronized transmitters, where the superscript (k) indicates a quantity measured or estimated by the k-th spoofer. Such quantities are the same found in eq. (13), apart for the additional phase term $\Phi^{(k)}$ used to adjust the relative geometrical term among transmitters. Finally, in eq. (15) a meaconer or a repeater is a simplified version of an intermediate attack, when the exact signal received from a satellite is delayed with an unknown delay τ_{sp} and amplified with the spoofer amplitude $\sqrt{P_s}$.

C. Adjacent-Channel Interference Models

The adjacent-channel interference is typically due to RF harmonics from nearby frequency bands into the GNSS signals. For example, signals such as LTE or Digital Video Broadcasting - Terrestrial mode (DVB-T) can leak harmonics into the GNSS bands. Such harmonics are typically modeled as AM or FM tones, see Eqs. (4) to (7). thus the jamming countermeasures for AM/FM tones are also applicable here.

D. Co-Channel Interference Models

Co-channel interference is due to (typically unintentional) interference transmitted into the same frequency band as the GNSS signals. The most common example here is the wideband interference, for examples coming from the other GNSS satellites transmitting in the same frequency bands. Such interference is typically modelled as an additional Gaussian term which basically increases the noise variance of the $\xi(t)$ AWGN component of Eq. (3). Other co-channel interferers can be due to other navigation systems used in aviation, such as DME or TACAN, which share some of the GNSS frequency bands. The DME unintentional interference model is exactly the same as for the DME-like/pulse jammer, shown in Eq. (10), with the difference that the model parameters τ, P_J, f_J, f_r, K are known in this case.

V. Interference Detection Mechanisms

A. Classical Detection Problem and Its Applicability

The detection of a single type of interferer can be formulated as the well-known classical binary detection problem [72], when a received signal may or may not contain an interference signal. These two cases are considered as two hypotheses. The hypothesis H_0 stands for the interference-free scenario and hypothesis H_1 reflects the case when the interferer is present.

In order to find a decision rule to distinguish between H_0 and H_1 hypothesis, one can rely on the Probability Density Functions (PDFs) under H_1 and H_0 (if known) of a measurable *test statistic*. An illustration of PDF is given in Fig. 8.

We remark that the PDF of the received signal samples for H_0 is Gaussian, but the PDF for H_1 may not fit a Gaussian distribution and it is dependent on the interference type. Given that the interference signal (and thus its PDF) is typically unknown, the power of the received signal is often used as a test statistic. For H_1 the power of the interferer signal $i(n)$ is typically much stronger than $w(n)$. For this reason, the resulting PDF corresponds mostly to $i(n)$. On the contrary, H_0 must fit a Gaussian distribution, since $r(n)$ under H_0 is mainly noise-like, as a superposition of a weak CDMA signal (i.e., the GNSS signal) and an Additive White Gaussian Noise (AWGN) noise.

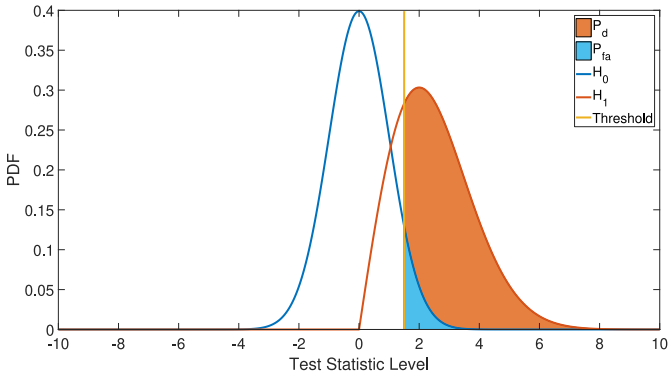


Fig. 8. Illustration of the PDF under H_0 and H_1 and an example of a detection threshold.

A suitable threshold separates between the two hypotheses such that the probability of detection P_{d} is maximized and the probability of false alarm P_{fa} is minimized. The probability of detection P_{d} and the probability of false alarm P_{fa} are

$$\begin{aligned} P_{\text{d}} &= \Pr(T > \gamma | H_1) \\ P_{\text{fa}} &= \Pr(T > \gamma | H_0), \end{aligned} \tag{16}$$

where $\Pr(\cdot)$ denotes a probability, T denotes a test statistic and γ is a fix or adaptive threshold. The choice of the test statistic is challenging and this challenge limits the applicability of this direct hypothesis testing in the interference detection in GNSS. If the PDFs are known under both H_0 and H_1, the Generalized Likelihood Ratio Test (GLRT), can be applied, as shown in (17)

$$T = \frac{\max\limits_{\theta_1} p(r|H_1, \theta_1)}{\max\limits_{\theta_0} p(r|H_0, \theta_0)} \underset{H_0}{\overset{H_1}{\gtrless}} \gamma, \tag{17}$$

where $p(r|H_0, \theta_0)$ and $p(r|H_1, \theta_1)$ stand for the conditional PDFs under H_0 and H_1 hypotheses, respectively. The θ_0 and θ_1 are the unknown interferer parameters. For example, the work in [107] adopts the binary hypothesis theoretical framework to develop a detection method for the presence of signal replicas in the samples of the received signal based on a GLRT test.

The classical detection algorithms are rarely applied in the context of jamming detection in GNSS in realistic scenarios because of the typically unknown jammer PDF. Instead of applying the classical detection techniques, the GNSS interference detection algorithms rely on various assumptions about the interference type and channel type (e.g., single path, multipath). The next subsections discuss different interference detection algorithms encountered in GNSS, based on their placement in the GNSS receiver chain of Fig. 4.

B. Front-End Detection Techniques

Front-end detection techniques typically work for any interference type and are applied before the acquisition, in the first stage of the receiver diagram Fig. 4. In a front-end technique, the signal before the ADC is used. The

most encountered front-end detection technique is the *AGC detector* [108]–[110]. The AGC maintains the control of the power of the incoming signal to provide an appropriate power for the quantizer in order to minimize the quantization losses [108], [109]. The AGC of a GNSS receiver operates at the ambient noise levels, since the GNSS signal power is very low, due to the large distance between the SatNav satellites and the aircraft. In the presence of powerful interferers, and especially for jammers, the AGC decreases its gain to keep AGC output signal level stable and avoid large fluctuations. This change of the AGC level can be used to detect an interferer. An AGC interference detector typically counts an estimate of the AGC gain over *N* consecutive samples, and compares it with a predefined threshold that corresponds to the interferer-free case. If all the *N* samples are below a certain threshold, then the interference is declared present. The nominal level is manufacturer and antenna specific, and this nominal level needs to be known to determine an adequate detection threshold. Overall, if the designer has access to the AGC values, then the AGC detection for jammer detection is straightforward to implement and it does not require additional HW elements, thus it is perfectly suitable for aviation applications.

While the AGC detector can be in theory used also for spoofing or meaconing, in practice the AGC fluctuations due to a spoofer are much lower than those due to a jammer and they can be easily missed, unless the spoofer power is extremely high. An example of AGC monitoring fruitfully used to detect a meaconing attack was presented in [111]. However, for the above-mentioned reasons, the effectiveness of the AGC monitoring for the detection of attack of the intermediate spoofing type is expected to be more limited. The resulting recommendation is to perform a careful on-site calibration to compensate for the non-negligible temperature effect and other environmental conditions, and to use the method in complement with other monitoring techniques.

C. Detection Techniques at Pre-Correlation Level

The vast majority of interference detection methods are pre-correlation techniques (see Fig. 4 for the placement of a pre-correlation algorithms). A pre-correlation technique operates on the signal after the ADC but before the acquisition block and processes the I/Q samples of the signal. The following paragraphs summarize the main pre-correlation techniques for interference detection.

1) PDF Detector [110], [112], [113]: This method is based on the fact that the received signal before despreading and in the absence of interference should follow a Gaussian distribution. In the presence of an interferer, such as a jammer or a narrowband/co-channel interferer, the signal's distribution will deviate from that of a Gaussian distribution. Examples can be found in the Appendix, Figure 18.

There are many statistical tests to verify whether a PDF is Gaussian-like or not, such as Lilliefors Test [114], Jarque-Bera test [115], Anderson-Darling Test [115], [116], Chi-square goodness-of-fit test [116], Kolmogorov-Smirnov test [116], etc. The main drawback of any PDF-based methods is that they require long periods where interferers are present to reliably estimate the PDF. For highly dynamic jammers as well as for wideband interferers such as spoofers, such methods are likely to fail. Nonetheless, an example of Chi-square goodness of fit test applied to the baseband signal samples before correlation to detect the PDF distortion in the presence of spoofed signals is developed in [113].

2) Time Power Detector (TPD) [72], [117]–[122]: The Time Power Detector (TPD) is known under various names in the literature, such as Power Law Detector (PLD) [121] or energy detector [72], [122]. This method measures the received signal energy over a short period of time. Its test statistic is given by

$$T_{\mathrm{TPD}} = \frac{1}{JN} \sum_{j=1}^{J} \sum_{n=1}^{N} |r(n + (j-1)N)|^{2\nu}, \qquad (18)$$

where *N* is the number of samples of the considered short interval, *J* is the number of short intervals under the observations (thus the signal is observed in total over *JN* samples) and ν is a positive number that determines the power-law, e.g., $\nu = 1$ for the square-law detector and $\nu = 0.5$ for the amplitude detector. The measured power, typically normalized by the number of samples *N* and by the noise variance, is then compared with a suitable threshold. If the test statistic exceeds the threshold ($T_{\mathrm{TPD}} > \gamma$) the interferer is declared to be present. Stitz and Renfors [119] used TPD test statistic in combination with filter banks and applied it to sub-bands of the original signal. Once the sub-bands containing the jamming signal were detected, they were removed.

Examples of a TPD detector are given in the Appendix, Fig. 19. The TPD detector is suitable for many interferer types, as long their power exceeds that of the GNSS signal. However, TPD in the context of spoofing detection is likely less effective than for jamming detection, because the spoofing strength is expected to be comparable with respect to the authentic one, in order to act as much covertly as possible.

A different formulation of the TPD is used in [120] in order to deal better with spoofing signals. In [120], the power measurement metric is used in conjunction with a correlation distortion metric in order to distinguish among multipath, interference, spoofing, and nominal signal. The joint use of the two metrics can compensate the complementary limitations of each metric used individually: first, power monitoring is prone to false alarms, therefore its detection sensitivity must be reduced so that spoofing signals with a low increase of strength with respect to their authentic counterpart go undetected; in these conditions the correlation distortion monitoring should be able to detect the presence of the non-authentic signal. Secondly, the code correlation function is nearly undisturbed in case of high power attacks, while the power monitoring should be able to detect the significant increase of signal strength.

3) Frequency Power Detector (FPD) [72], [117]: The FPD is quite similar to the TPD detector, as, according to Parseval's theorem, the average power of a signal in time domain equals the average power in frequency domain. The periodogram is used to estimate the signal's spectral density for the FPD. Examples of FPD are shown in the Appendix, Fig. 20.

4) Detector Based on Welch's Method [117], [123]: Welch method can be also used to estimate the periodogram and the resulting detector can be seen as a variant of the FPD [117], [123]. Compared to the periodogram, Welch's method divides the input signal into overlapping pieces of a certain length, applies a window to these pieces and then computes the periodogram of each of them; this results in averaged periodograms. The size of each window has to be sufficiently small such that the frequency content can be assumed constant for each piece. Examples are shown in the Appendix, Fig. 21.

5) Kurtosis Detector [117], [124]–[126]: The kurtosis of a signal over *N* observation samples is defined as

$$\Gamma = \frac{\frac{1}{N}\sum_{n=1}^{N}(r(n)-\mu_r)^4}{\left(\frac{1}{N}\sum_{n=1}^{N}(r(n-)\mu_r)^2\right)^2}, \tag{19}$$

where $\mu_r = \frac{1}{N}\sum_{n=1}^{N} r(n)$ is the mean of the signal *r*(*n*). Here *r*(*n*) are the incoming pre-correlation samples at the aircraft GNSS receiver. In the absence of jamming, the Kurtosis is close to 3 (Gaussian distribution). In the presence of a jamming signal, the Kurtosis may deviate from value 3, the deviation dependents on the type of jamming [117], [124]. Fig. 22 from the Appendix shows an example of the Kurtosis detector.

6) Notch Filter Detector [127]–[130]: Notch filters have been traditionally used for jamming mitigation, but they have also detection capabilities, as shown recently [128]. Borio *et al.* [128] designed an Infinite Impulse Response (IIR) notch filter whose z-transform is

$$H_n(z) = \frac{1 - z_0(n)z^{-1}}{1 - k_a z_0(n) z^{-1}} \tag{20}$$

and which is adapted using a stochastic gradient approach. The term $z_0(n)$ is the notch filter's time-varying zero, whose angle determines the center frequency of the notch, and k_a is the pole contraction factor (a user-defined parameter between 0 and 1). The zero $z_0(n)$ is adapted to be in accordance with the with jammer instantaneous frequency in the complex plane. Its magnitude $|z_0(n)|$ can be used as detection metric. Again, an appropriate threshold must be found to distinguish the interference-free case from the jammer present case.

7) Detection Based on Multi-Antenna Arrays [131], [132]: This method consists on using the information provided by more than one antenna to detect the interference. A detector based on combining the signal from an antenna array with two Right Hand Circular Polarized (RHCP) antennas spaced at $\lambda/2$ in GPS L1 band was proposed in [131]. Antenna-based solutions are also discussed in Section VIII-A as they can also be employed for interference mitigation, but they are not very practical in the context of an aircraft, as they would increase the costs of the on-board equipment.

8) Hough-Radon Transform (HRT) [133], [134]: The HRT is a feature extraction method used to detect geometric shapes in images. It can be used to detect the different lines as they occur in time-frequency transforms as the spectrogram (see examples of spectrograms in Fig. 7). Thayilchira and Krishnan [133] and Erkucuk *et al.* [134] treated this spectrogram as an image, and applied the HRT to detect a chirp-like interference in the signal. The HRT can be especially useful as classifier for the different jammers. Nevertheless, to classify the jammer type, the JSR must be high enough so that the resulting image shows the lines clearly.

9) Singular Value Decomposition (SVD) Detector [135]: The decomposition of the covariance matrix of the received signal in singular values, so-called Singular Value Decomposition (SVD), and their analysis is the basis of this detector [135]. Studies in [135] show that the SVD detector has a good performance for CW jammers, but completely fails for chirp jammers. Aside from this, its performance is poor at low JSR.

D. Detection Techniques at Post-Correlation or Link Level

These techniques make use of the signal after the correlation with the reference code of a particular satellite, thus, they focus on a satellite-receiver link at a time. They are commonly implemented in the tracking module, as they use outputs of the correlators (recall Fig. 4). Nonetheless, they may additionally use the pre-correlation signal. Post-correlation analysis is widely the preferred and most powerful approach for spoofing monitoring. The reason for this is evidently in the structure of the spoofing signal, which intrinsically offers features suitable for acquisition and tracking. The following paragraphs list the various post-correlation detection techniques found in the literature.

1) Power Distortion Monitoring (PDM) [120]: A method called PDM was studied in [120]. It monitors both the power and the correlation function in order to detect sudden changes. The changes in power and the distortion of the correlation functions provide complementary information that not only allows to detect the presence of a jamming signal, but also the presence of GNSS multipath or spoofing. While jamming was detected reliably in [120], the authors noted that their method tended to mistake spoofing for jamming.

2) Multi-Correlator Banks [136]–[139]: The apparent similarity of a counterfeit signal with a signal replica generated by a multipath reflection is the reason for the adaptation of multipath mitigation techniques, such as multi-correlator banks to spoofing detection and monitoring. Examples of multi-correlator bank-based algorithms include the multiple tracking loops proposed in [137], the Spoofing Estimating Delay Lock Loop (SEDLL) [136] or the vector tracking loops investigated in [138]. Often, this family of techniques is indicated with the name of *vestigial signal defence*, as it aims at tracking replicas of the correlation peak aside the principal one. Multi-correlators banks suffer from high computational load, linearly proportional to the number of tracking channels (e.g., in a multi-constellation, multi-frequency receiver it may easily reach one hundred or more tracking channels).

3) Multi-Correlator Output With Auto Regressive Modelling (MCAR) [88]: is based on forming multi-correlator outputs and analysing them through an Auto-Regressive (AR) modelling. The assumption is that the variances of the correlator outputs increase with the presence of a jammer. Only continuous wave and narrowband interference were studied with this method in [88] and its applicability to other interference types is yet unknown.

4) C/N_0 Monitoring [140]–[142]: The C/N_0 is an important measure of the performance of a GNSS receiver, as it indicates undesired decreases in GNSS signal power or the increases in noise power per tracking channel. However, the C/N_0 may change due to several other reasons, such as deteriorated satellite visibility, which can easily mislead the detector [64], [76]. A detector based on only C/N_0-monitoring performs rather poor. A jamming signal changes the C/N_0 as it contributes to the noise power, thus this allows to detect jamming. Several approaches were studied in the literature: the difference between C/N_0 and effective C/N_0 was used in [140], the binary hypothesis testing framework was exploited in [141], assuming the C/N_0 normally distributed, and Scaramuzza *et al.* [142] analysed C/N_0 data, in combination with GPS satellite azimuth and elevation angle and as well roll, pitch, and yaw angles. C/N_0 monitoring is also a principal indicator for spoofing detection: a sudden upward jump of the C/N_0 level may indicate the onset of a powerful spoofing attack [64], [74], but also a sudden and concentrated fluctuation of its level may indicate a tracking peak shifting from the authentic to the fake signal [74], [76]. Continuous C/N_0 monitoring can be considered a must-to-have process in an anti-spoofing receiver, although it cannot be the sole means for interference detection.

5) Absolute Power Monitoring [64]: The monitoring of the absolute receiver power of each PRN channel as a method to detect spoofing is discussed in [64], where it is demonstrated with theoretical considerations that such a method can be widely more robust than the C/N_0 monitoring. Although not explicitly indicated in the paper, the TPD detector applied to the post-correlation samples is a candidate method to implement absolute power monitoring. However, the relatively high dynamic range of the GNSS signal strength may limit the achievable performance of the monitoring algorithm.

6) Support Vector Machines (SVM) [143]: The SVM approaches can act both as detectors and as as classifiers and can be applied both in pre-correlation or post correlation stages in a GNSS receiver [143], but they are more common in the post-correlation stage. The studies in [143] focus on narrowband and wideband jammers with JSR between 5 and 25 dB and estimate the training time it takes for the SVM-based classifier to reach 100% monitoring precision (i.e., between 0.75 ms and 60 ms).

7) Signal Quality Monitoring (SQM) Detector [144], [145]: On the upper side of the complexity line, SQM techniques probably offer the highest sensitivity and the smallest vulnerability to spoofers: they are intended to monitor the distortion of the received signal induced by a non-authentic source, by applying metrics often originally developed for detecting multipath conditions. The basis of the SQM approaches is the observation and statistical characterisation of cross-correlation samples between the received signal and local replicas delayed by opportune amounts [113], [146], [147]. The quantification of the deviation of such samples from the nominal correlation function is the test statistic adopted to detect the presence of counterfeit signals. A well-known method belonging to this class is the *ratio test* proposed for spoofing detection in [148]; other approaches belonging to the same class are the *Goodness of Fit (GoF) test* and the *sign test*, used and analysed in [75], [149]–[152]. The SQM detectors also have limitations, in that they may fail in correctly discriminating between natural multipath and counterfeit signal copies, unless some sort of fine tuning is adopted [145].

E. Detection Techniques at Navigation Level

These techniques are carried out in the navigation module. They take into account multi-links (i.e., signal received from all the satellites from the sky) and the signal at pseudorange domain (after the tracking module, (see Fig. 4)). These techniques incorporate additional data to monitor the GNSS receiver. They effectively reveal anomalies of the receiver observables, through cross-checks with other PRNs, data from other frequency bands, receivers or sensors. Various navigation techniques for interference detection are summarized in the next paragraphs.

1) Correlation of Propagation-Dependent Observables [68], [153]–[155]: If the aircraft is moving, the propagation channel affects the received signals with recognisable variations of the power level and Doppler frequency shift, but also with multipath and blockage effects. Since the directions of arrival from the satellites are different, little or no cross-correlations of such metrics are expected in the receiver. On the contrary, in case of different PRN signals coming from the same source of spoofing, they are obviously affected by the same propagation channel effects [68]. Therefore, if a high correlation of such propagation-dependent metrics is observed, then the signals should be flagged as counterfeit with high probability [153]–[155].

2) Consistency Checks With APNT [156]: An APNT system complementary to GNSS has different error mechanisms than GNSS and can therefore be exploited to detect RFI. Detection methods based on APNT systems use respective observables or outcomes of the APNTs system to check the integrity of the GNSS solution. A performance criterion of the APNT- and GNSS observables needs to be found to be used as test statistic and to determine a detection threshold (e.g., the variance of the observables). Broumandan and Lachapelle [157] and Khanafseh *et al.* [158] proposed a method that cross checks the solutions provided by GNSS with the INS/odometer solution. The authors of [156] rely on DME and L-band Digital Aeronautical Communication System (L-DACS) to monitor the integrity of the GNSS solution, either on positioning level or on pseudorange level, and to detect spoofing.

3) AoA Discrimination [68], [69], [159]: A multi-antenna receiving architecture is likely the best candidate to detect the presence of counterfeit signals, under the reasonable hypothesis that they are generated from the same source. The underlying idea is that the post-correlation measurements from different PRNs observed by two or more receiving chains can be manipulated in order to detect signals arriving from the same direction, which are recognised to be non-authentic. The receiving chains can be physically arranged in an antenna array, as for example in [132], [160]–[162], or can be emulated

by the movement of a single antenna to form a synthetic aperture antenna, as for example in [163]. The determination of the AoA of the false signals can open the path toward the localization of the source position [103], [163]. The major obstacle for such approaches is the complexity of practical implementation, because they typically put severe requirements on the geometrical setup (including aircraft motion), on the calibration and synchronization of the receiving chains, etc. [162]–[164].

4) Sum of Squares (SOS) Detector [67], [165], [166]: In order to reduce the complexity of AoA discrimination methods, the authors in [67], [165] developed a dual-antenna spoofing detector which relaxes the constraints. The approach, indicated as Sum of Squares detector, exploits the fact that the receiver-to-receiver phase difference measurements of signals coming from the same direction share a common geometrical term. For spoofed signals, this term cancels out with the computation of the satellite-to-satellite double difference measurements, which then are characterized by noise only, plus a nuisance factor due to the integer carrier phase. On the contrary, for authentic signals the geometrical terms are different and do not fade in the computation of the double differences. Based on this principle, the authors in [67], [165] set a binary hypothesis problem upon on a GLRT statistic, to distinguish between fake and real GNSS signals. The algorithm proved to be successful in a setup made by a dual-antenna system with two independent Commercial Off-The-Shelf (COTS) receivers. The idea was also extended in the Dispersion of Double Differences (D^3) algorithm [166] to more practical situations in the presence of cycle slips and 'mixed tracking', i.e., when only a subset of the signals in tracking is counterfeit.

5) Polarization Discrimination or Dual Polarization Antenna (DPA) [159], [167]–[169]: is based on the ability of an aircraft receiver to receive both right-hand and left-hand circularly polarized signals. Genuine signals coming from the satellites are mainly RHCP, while signals coming from a transmitter located at approximately the same height of the receiver, or even below as in the case of a flying aircraft, thus their RHCP and Left-Hand Circularly Polarized (LHCP) components are equal. Based on this principle, the presence of signals coming from terrestrial sources can be detected [159]. In [169] the polarization received from the genuine satellites is admitted to be elliptic and different for each satellite, because of reflections and antenna non-idealities. On the other hand, the forged signals transmitted from a single source travel the same propagation path and arrive with the same polarization, regardless of which type.

6) Crowd-Sourcing [170], [171]: the idea in Crowd-sourcing shown in [170], [171] is to create some interference maps, based on GNSS observables from Android devices, and interference assessment tools, based on data collectively gathered at multiple locations. The collected observables can be anything from C/N_0 and AGC values to raw I/Q samples from all the satellites in view. Such a solution requires a continuous Internet access and relies on the assumption that the jammers are static or slowly moving. Such a method also raises significant privacy concerns, as planes could be tracked based on their GNSS observables reported to a cloud server. Crowd-sourcing also relies on a high number of participants, which could be difficult to acquire without adequate incentives. In addition, the quality of the collected data can be highly varying, according to the user receiver and the participants' level of trustworthiness. While Crowd-sourcing-based jamming detection is highly impractical today in the context of aviation (due to the above-mentioned drawbacks), with the fast development of cloud-based/crowd-sourcing solutions, this might be an interesting solution worth to be investigated more in the future.

The main interference detection algorithms are summarized and compared in Table V. Empty entries in the table signify that the considered algorithm is not applicable or not available for that particular interference type.

VI. Interference Direction Finding and Localization Mechanisms

Localization of passive RFI sources is typically a two-step process that relies on one or several of the following parameters of the emitted signal: power, time, frequency, or angle of arrival/ phase. In a first step, the target parameters must be extracted or measured. In a second step, multiple measurements, obtained at spatially displaced antennas, at various times, or at various frequencies, are used to estimate the source's position. GNSS interference localization is facilitated when more signal characteristics are known or estimated. Identifying and classifying the interference signal may help in that regard (see also Section VII).

In case of a jammer localization the challenge is to locate a passive source that emits an *unknown* signal. Thus, the absolute values of measurements cannot be used, as the reference times are unknown. Instead, one can use the differences of measurements, namely Angle of Arrival (AoA), Time Difference of Arrival (TDoA), Received Signal Strength Difference (DRSS) and Frequency Difference of Arrival (FDoA), where

- AoA measurements refer to the differences of the signal's phases at different antennas at the receiver and they can be used to infer the direction to the source,
- TDoA measurements refer to the differences of the signal's propagation times at different antennas and they can be used to infer the distance to the source,
- DRSS measurements refer to the differences of the signal powers at different antennas and they can be used similarly to TDoA to infer the distance to the source, and
- FDoA measurements refer to the differences of the signal Doppler shifts at different antennas, caused by the relative motion between source and receivers; they can be also used to infer the angles to the source.

The following paragraphs explain these four main localization methods in more detail. For clarity, we rely on the assumption of an isotropic RFI source that radiates spherical travelling waves, which travel with the speed of light c. If the propagation time can be measured (as in GNSS), one can deduce the distance between interferer and receiver as $r = \tau c$, the product of the wave's propagation time τ and the speed of light,

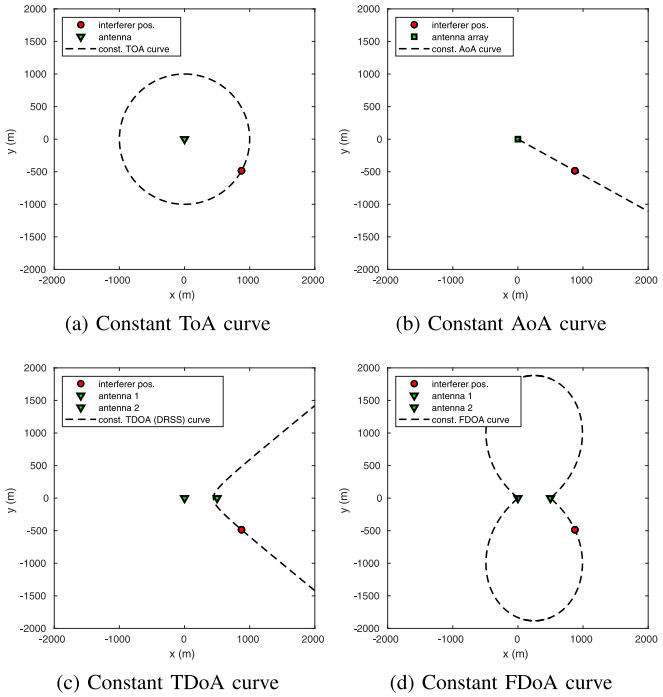
TABLE V
SUMMARY OF INTERFERENCE DETECTION METHODS FROM LITERATURE. COMPLEXITY RANGES FROM LOW (LEFT) TO VERY HIGH (RIGHT) AND PERFORMANCE RANGES FROM POOR (LEFT) TO GOOD (RIGHT). THE COLOUR CODE IN COMPLEXITY AND PERFORMANCE COLUMNS SUPPORTS A QUICK ASSESSMENT, LIGHT-COLOURED REGIONS ARE BETTER THAN DARK-COLORED REGIONS

Domain	Algorithm	Type of Detect			Complexity	Performance	Limitations	References
		Jammer	Spoofer	Others				
Front-End	AGC	✓	✓	✓			HW and temperature-dependent; thresholds need to be adaptive, function of the receiver chipsets, interference type, temperature; as a spoofer detector, it is only valid for high-power spoofers	[108]–[110]
Pre-correlation	Time and frequency power detectors (TPD, FPD, Welch spectrogram)	✓	✓	✓			Sensitive to the observation window used to compute the signal power; TPD and FPD typically better than spectrogram; as a spoofer detector, it is only valid for high-power spoofers	[72], [102], [117]–[123], [172], [173]
	PDF	✓		✓			Working only at high JSR	[110], [112], [113]
	Kurtosis	✓					Working only at high JSR	[117], [124]–[126]
	Adaptive Notch Filter (ANF)	✓					Better suited for chirp jammers than for other interference types	[127]–[130]
	Pulse Blanking Methods	✓					Performance similar with ANF	[130], [174]
	Detection based on multi-antenna arrays	✓	✓	✓			Limited knowledge available in the current literature; impractical in aviation domain as additional antennas increase the interference on-board; as a spoofer detector, it is only valid if the spoofers are transmitted from the same location	[131], [132]
	HRT	✓					Working only at high JSR	[133], [134]
	SVD	✓					It does not work with chirp jammers	[135]
	Wavelet	✓	✓				Sensitive to the choice of the mother wavelet; not well-understood in GNSS context; high complexity	[175]
Post-Correlation	PDM	✓	✓	✓			More suitable for jamming than for spoofing	[120]
	MCAR	✓					Assumes that the variance of the correlator outputs increases with the interference; this assumption is not always valid in practice	[88]
	C/N_0 monitoring	✓	✓				Difficult to distinguish between various causes of a low C/N_0	[140]–[142]
	SVM	✓					Not a real-time solution	[143]
	SQM	✓	✓	✓			It works only for limited times; it can be used as a transient indicator or interference	[144]
Navigation	SoS/D^3	✓	✓				More suitable for spoofing than for jamming	[67], [166]
	Crowd-sourcing	✓	✓	✓			Not a real-time solution; poses security and privacy threats; insufficiently studied in the literature; currently not suitable in aviation	[170], [171]
	Consistency checks with INS/Odometer coupling		✓				Typical delays of 20s or higher in spoofing detection; it does not work for constant-speed receivers	[156]–[158]

Complexity: □ – low, ■ – moderate, ■ – high, ■ – very high
Performance: ■ – poor, ■ – medium, □ – good

and establish a sphere (in 3D) or a circle (in 2D) of possible positions around the receiver at which the source is located, see Figure 9(a).

The point of intersection of three of these spheres, from propagation time measurements at spatially displaced receivers, determines the location of the RF source.



(a) Constant ToA curve (b) Constant AoA curve

(c) Constant TDoA curve (d) Constant FDoA curve

Fig. 9. Line of positions of differential positioning mechanisms.

A. AoA/Direction of Arrival (DoA)

determining AoAs (also called DoA in the interference localization cases) typically equals to estimate the orientation of surfaces of constant phase, or wavefront. The orientation of a wavefront can be inferred from the time-difference, or phase-difference measurements at two or more spatially displaced antennas. A common approximation is the far-field assumption, which simplifies AoA estimation because the spherical wavefront becomes a plane wavefront, when compared to the physical size of the antenna array. The phase difference between two antenna elements, in horizontal plane spaced by d, is related to the AoA through $\Delta\phi_{12} = \frac{2\pi f_{\text{carr}}}{c} d \sin\alpha$, thus the AoA reads

$$\alpha = \arcsin \frac{\Delta\phi_{12}}{d} \frac{c}{2\pi f_{\text{carr}}}, \tag{21}$$

where $\Delta\phi_{12}$ is the phase difference between antennas 1 and 2, f_{carr} is the carrier frequency, and c is the speed of light. A single AoA results in a line of bearing on which the interferer is located, as shown in Figure 9(b). Again, the point of intersection of multiple lines of bearing, from spatially displaced antenna arrays, determines the location of the interferer. See, for example, [15], [59], [102], [161], [167], [168], [176], [177].

B. TDoA

the location of an interference source can also be estimated from differences of signal propagation times that are measured at spatially displaced receivers $\Delta\tau_{12} = \tau_1 - \tau_2$. A single difference of distances

$$r_1 - r_2 = \Delta\tau_{12} c \tag{22}$$

results in a hyperbolic curve on which the RFI source is located; as illustrated in Figure 9(c). If the TDoAs from multiple pairs of receivers can be obtained, the interferer's position is determined by the point of intersection of the corresponding hyperbolic curves. This approach found appliation in, e.g., [15], [83], [96], [178]–[183].

C. DRSS

The power at the aircraft is related to the interferer-aircraft distance through a path loss model. If we assume a log-distance path-loss model, then $P_i = P_0 - 10\gamma \log_{10}(r_i/r_0)$, where γ is the path-loss coefficient, P_i is the received power at r_i distance from the interferer, and P_0 is the power at a known reference distance r_0 from the interferer. The relation of a pair of power measurements at spatially displaced on-board receivers to the differences of distances is then given by

$$r_1 - r_2 = 10^{\frac{\Delta P_{12}}{10\gamma}}, \tag{23}$$

forming as well a hyperbolic curve as that shown in Figure 9(c). Multiple distance differences from further pairs of receivers can be used to infer the source location as in the case of TDoA measurements. The main challenge with this approach is the need to know or estimate the path-loss coefficient γ, which is highly dependent on the environment. In addition, a log-distance path-loss model is not very accurate, especially at large distances as those involved in commercial aircraft in cruise mode. Recent path-loss models in various scenarios, including scenarios for aerial low-altitude vehicles have been developed in [184], [185]. The DRSS techniques have been studied very little so far in the context of the interferer localization. For examples we refer to [15], [140], [186].

D. FDoA

another signal parameter from which the location of a passive RFI source can be estimated is the Doppler frequency shift, i.e., a shift of the carrier frequency due to the relative motion between the source and the receiver. For flying aircraft, the Doppler shift is significant, compared to the terrestrial receivers which have lower speeds. The Doppler shift at an antenna is determined by the relative radial velocity v_r between the interferer and the aircraft and is given by $\Delta f = -v_r \frac{f_{\text{carr}}}{c}$. The difference of Doppler shifts at a pair of receivers becomes $\Delta f_{12} = \Delta f_1 - \Delta f_2 = \frac{f_{\text{carr}}}{c}(v_{r,1} - v_{r,2})$, where the radial velocity is $v_r = \|v\| \cos(\alpha - \alpha_v)$ with $\|v\|$ being the speed of the relative motion, α being the angle between the antenna baseline and the interferer and α_v the angle of the velocity vector. The difference of Doppler shifts is related to the angles between interferer and the GNSS receivers on-board of the aircraft:

$$\alpha_1 = a_{v,1} + \arccos \frac{-\frac{\Delta f_{12} c}{f_{\text{carr}}} + v_{r,2}}{\|v_1\|}. \tag{24}$$

We remark that the typically unknown carrier frequency f_{carr} of the RFI is contained in Eq. (24). Although, the unknown carrier frequency mostly cancels out when taking the difference of Doppler shifts, the remaining residuals may cause

a degradation in accuracy of the FDoA measurement for frequency modulated signals [187]. In order to reduce the search space, a frequency range in the vicinity of the carrier frequency is required. After multiple Doppler shift difference measurements have been obtained at different pairs of GNSS receivers on-board of the aircraft, the source of the RFI can be estimated. Works particular dealing with RFI have not been found, further general references are for example [187]–[193].

In case of spoofing, the fact that the interfering signal has the same structure and relatively comparable power with respect to the true GNSS signals, means that the incoming signal phase, the Doppler frequency, and time of arrival are available for each satellite signal only at a post-correlation stage. Therefore, the principles described so far for direction finding are in principle applicable to the counterfeit GNSS signals on measurements obtained after local correlation [161], [163]. For example, Dampf *et al.* [163] apply classic digital beamforming algorithms to determine the direction of arrival of spoofing signal and spatially removing them from the receiver solution, using precisely synchronised samples of the early, prompt and late correlators output for each satellite, taken from a synthetic aperture antenna and corrected for the receiver clock drift and jitter. In [161] the DoA of the received signals, determined with a classic DoA estimation method, is compared with ephemeris-predicted one in order to jointly detect the presence of counterfeit signals and estimate the receiver platform attitude.

Differently than the previous approaches, the DPA-based approach developed in [167], [168] is able to extract the azimuth of an incoming signal from the phase relationship between RHCP and LHCP received components. In the hypothesis that the forged signals are linearly polarized instead of RHCP, their azimuth can be determined from the signals processed by the two antenna channels.

The different interference localization algorithms are summarized and compared in Table VI.

VII. Interference Classification Mechanisms

Interference classification is also a two-step process: feature extraction and signal classification. In addition, a preprocessing step is often necessary to represent the data in a uniform way. The actual classification comprises first the extraction of features from the signal. This reduces the data dimensions and it is a crucial step, as the selected feature(s) should be as characteristic for the interference classes as possible. In principle any feature of a signal could be used for classification. Nevertheless, the more distinctive the features, the better the classifier that builds upon these feature. If the signal consists of multiple components of different structure, several features that represent well the structure of the components should be found.

These feature are used in the second step to classify the signal. In order to assign the input signals to the corresponding classes, the classifier obeys a rule, as a function of the selected features, that separates the different classes. The rule is commonly obtained automatically by means of supervised learning, that is, it is established based on a large amount of correctly labelled examples from each class.

If the *a priori* knowledge about the interferer signal is high, e.g., only a certain type of signal is expected, parameters estimated directly from the signal may be good and sufficient features to discriminate the signals [197]. The classification of jamming signals that belong to the pulsed narrowband interference was studied by [198]. For wider classes of interference, such as non-stationary or multi-component signals, the features can be extracted from the joint time-frequency domain [199]–[202] and machine learning methods can be applied for learning and classification [203], [204]. Boashash [205] provides a good introduction to signal classification using time-frequency methods, including a discussion of time-frequency distributions for different types of signals and a list of features based on the statistics and of the image of the time-frequency distribution. However, no extensive studies on interference classification exist for jammer and spoofer in GNSS to the best of the authors' knowledge. Table VII lists studies that address GNSS interference classification or characterisation. As it can be seen, the number of works on this particular topic is rather small. It is the authors' belief that features and methods used in image classification may be applicable to images of the time-frequency distributions too, and thus to the spectrograms of GNSS with interferers. Also, general concepts of supervised and unsupervised learning may be of interest here. Table VII covers jammer signal classification as well as spoofer signal classification. Due to their different focuses, the complexity and performance of the listed methods are not necessarily comparable.

VIII. Interference Mitigation Mechanisms

Mitigation refers to a condition in which the receiver under attack is able to recover its correct positioning capability, neutralizing the effect of the interference. Because of the structural difference between jamming signals and spoofing signals, mitigating the effect of such unwanted transmissions requires completely different approaches, which are reviewed hereafter. As a general notice, jamming is generally tackled by means of front-end and pre-correlation techniques, while spoofing must be dealt with post-correlation or navigation techniques (see Fig. 4). Interference mitigation techniques require typically also the detection of the interference in order to suppress it. Thus, many of the mitigation algorithms act as joint detection and mitigation algorithms and complement the detection methods presented in Section V. The next subsections give an overview of various interference mitigation techniques, grouped according to their placement in the GNSS receiver chain, see Fig. 4.

A. Front-End Mitigation Techniques

Front-end techniques described hereafter have been mostly developed to mitigate jamming attacks and are not effective for spoofing mitigation. Most of them rely on spatial filtering.

1) Switching Frequencies: The main idea of a switching frequency mitigation technique is to use a second frequency band when the primary band is affected by interference [85].

TABLE VI
SUMMARY OF JAMMER LOCALIZATION METHODS FROM LITERATURE. THE COLOUR CODE IN COMPLEXITY AND PERFORMANCE COLUMNS SUPPORTS A QUICK ASSESSMENT, LIGHT-COLOURED REGIONS ARE BETTER THAN DARK-COLORED REGIONS

Domain	Algorithm	Complexity	Performance	Limitations	Refs
Front-End	AoA antenna array (CRPA), static or moving aircraft			Requires phase/gain calibration of antenna array elements; multipath presence or non-LOS situations affect the performance	[15]
Pre-correlation	AoA single antenna, moving aircraft			IMU required to estimate trajectory of antenna, propagation channel assumed stationary during spatial sampling; multipath presence or non-LOS situations affect the performance	[176]
	AoA antenna array, static or moving aircraft			Requires phase/gain calibration of antenna array elements; multipath presence or non-LOS situations affect the performance	[59], [102], [177]
	DRSS, single antenna with moving aircraft or or multiple antennas, both static and moving aircraft			Not suitable for aircraft flying at medium and high altitudes due to high path losses; mostly useful for short distances between the jammer and aircraft	[15], [140], [186]
	TDoA single antenna, a.k.a DTime of Arrival (ToA)/VTDoA, moving aircraft			Propagation channel assumed stationary during spatial sampling; performance highly dependent on the bandwidth of the interferer and the plane trajectory; multipath presence or non-LOS situations affect the performance	[178]
	TDoA multiple antennas, both static and moving aircraft			Precise time synchronization between antennas needed in some of the approaches; large separation between antennas needed; multipath presence or non-LOS situations affect the performance	[83], [15], [179], [180], [181], [96], [182], [183]
	FDoA, multiple antennas, both static and moving aircraft			It needs precise timing and frequency synchronization between antennas; localization with only FDoAs not much addressed in general, nor in jamming, aviation or GNSS context	[188]
	TDoA+FDoA single antenna, aka VFDoA, moving aircraft only			Mostly theoretical works, not studied yet in the context of jamming, aviation, or GNSS	[193]
	TDoA+FDoA, multiple antennas			It combines the drawbacks and advantages of TDoA-only and FDoA-only solutions	[60], [187], [190]–[192], [194]
	AoA+TDoA, multiple antennas, both static and moving aircraft			Precise time synchronization between antennas needed	[96], [187]
	AoA+FDoA, multiple antennas, both static and moving aircraft			Precise time synchronization between antennas needed	[189]
Post-correlation, single-link level	AoA, synthetic aperture antenna, digital beamforming, static receiver			Compensation of satellite motion, receiver clock drift and jitter needed	[163]
	AoA, DPA, dynamic receiver			High quality DPA needed, DoA determination requires several steps (not straightforward), elevation not measurable, azimuth measurable for medium-to-low elevations only	[159], [168]
Post-correlation, multi-link/ navigation level	AoA, antenna array, digital DoA estimation, static and dynamic receiver			Antenna array needed, with precise synchronization of the receiving chains, limited and stable mutual coupling between antenna elements, limited multipath	[161], [195], [196]

Complexity: □ – low, ▒ – moderate, ▓ – high, ■ – very high
Performance: ■ – poor, ▓ – medium, □ – good

This works with multi-frequency GNSS receivers where at least one frequency band is not affected by the interference. A probabilistic analysis done in [85] showed that it is less probable that both L1/E1 and L5/E5 frequencies of GPS/Galileo systems are affected by interference and recommended a hopping between the available frequencies based on

TABLE VII
SUMMARY OF INTERFERENCE CLASSIFICATION METHODS FROM LITERATURE. THE COLOUR CODE IN COMPLEXITY AND PERFORMANCE COLUMNS SUPPORTS A QUICK ASSESSMENT, LIGHT-COLOURED REGIONS ARE BETTER THAN DARK-COLORED REGIONS

Domain	Algorithm	Type of Interference			Complexity	Performance	Limitations	Refs
		Jammer	Spoofer	Other				
Pre-correlation	Different time-frequency representation to characterise chirp signals	✓					Jamming signal characterisation only, actual classifier not presented	[117]
	Characterisation of chirp signals using time-frequency distribution and Rényi entropy	✓					Jamming signal characterisation only, actual classifier not presented	[206]
	Machine learning	✓	✓	✓			Binary classification between intentional harmful events and unintentional interferences; ...	[207]–[209]
	Extraction of different features & SVM to classifier		✓				Spoofing signals are QPSK modulated and simulated with Hammerstein model	[210]
Post-correlation, single-link level	Bias/slope of double difference carrier phase to classify between spoofer and authentic signal		✓				Binary spoofing classifier; poor antenna geometry and small antenna baselines deteriorate the classification performance; requires multiple receivers communicating with central unit	[211]
	Power & correlation distortion monitoring to classify between authentic, spoofing, multi-path and jamming signal	✓	✓	✓			Either high mis-classification between jamming and spoofing, or between multipath and clean data	[120], [212]

Complexity: □ – low, ▒ – moderate, ▓ – high, ■ – very high
Performance: ■ – poor, ▒ – medium, □ – good

the received C/N_0. The main problems with such an approach are that they require dual-band or triple-band GNSS receivers, and that there is no guarantee that the jammer does not jam all GNSS frequency bands at the same time.

2) Switching Antennas: Heddebaut *et al.* [213] studied spatial diversity to mitigate jamming in a on-board train scenario. The robustness of the studied communication systems is improved by choosing the signal/antenna with the highest Signal-to-Jamming-plus-Noise Ratio (SJNR) (or effective C/N_0). The antenna displacement in [213] is up to 300 m. The use of multiple antennas or antenna arrays to be installed on-board of the aircraft and the distance between the antennas limit its suitability for aviation applications, especially for small-sized or non-commercial aircraft.

3) Adaptive Beamforming/CRPA: An adaptive beamformer controls the radiation pattern of the GNSS antenna array to suppress the direction of an interferer and to steer the remaining power towards the GNSS satellites. This concept is now widely used in form CRPAs. The CRPA in [214] puts nulls in the direction of interferers in case that this direction is known or towards the ground if interference direction is unknown, starting from the premises that interferers are on the ground and GNSS satellites are on the sky. Also Dabak *et al.* [215] design a CRPA with such features. A multitude of beamforming algorithms can be used, such as: Capon (MPDR) beamformer [216], null steering of Howells [217] and Applebaum [218], spatial matched filter with Chebyshev windowing, zero forcing beamformer and so forth [219], [220]. Several methods require to estimate the interferers' AoA before it can be mitigated, commonly by putting nulls in their directions. CRPAs are available for airborne systems.

B. Mitigation Techniques at Pre-Correlation Level

Most pre-correlation approaches transform the signal to a different domain with the objective to either estimate certain characteristics of the interference signal, or separate better the GNSS and the interference signals and to extract the transform domain components that represent the interferer. The estimated parameters are often used to filter out the interferer. The extracted components of some transform are frequently used synthesize/reconstruct the interferer and to subtract from the incoming signal mix.

1) NF: Notch Filters (NFs), also proposed for interference detection, as shown in Section V, are band-stop filters characterized by a narrow stop band. NFs for interference mitigation are typically designed as Adaptive Notch Filters (ANFs). Saulnier and Das [127], for example, presented a Least Mean Squares (LMS) filter [221] to suppress narrowband jamming in spread spectrum receivers. In [127] AM tone jammer mitigation was investigated, but only at JSRs equal to 10 dB. The method from [127] is unlikely to work with

chirp-like jammers, as it was fine-tuned for AM tone jammers and is also highly sensitive to noise. An IIR adaptive notch filter for jamming mitigation was studied in [129]. This method showed about 1 dB C/N_0 improvement compared with Digital Excision Filter (DEF)-based mitigation and about 1–2 dB C/N_0 improvement compared with other notch filters proposed in the literature. Chien [129] tested only CW jammers at JSRs above 30 dB. An adaptive IIR NF was also studied in [128], [130], [222], and [223]. The method proposed in [130] is inferior than Pulse Blanking Methods (PBMs) for pulsed narrowband interference (chirp signals were not studied). Another adaptive notch filter was studied in [128]. It achieved a C/N_0 improvement of up to 5 dB in the presence of chirp jammers.

2) DEF: The frequency excision filters are an extension of the frequency-zeroing concept. A DEF is a generic term referring to various filtering or processing approaches in frequency domain. Chien *et al.* [224] proposed a DEF called Consecutive Mean Excision (CME). They showed more than 90 % signal acquisition probability after the DEF algorithm in the presence of one or two jammers and for JSR below 40 dB, but their algorithm was tested only with multi-tone AM jammers. A DEF to suppress narrowband interference in Direct Sequence Spread Spectrum (DSSS) was presented in [119]. A complex modulated filter bank is used to divide the signal into several sub-bands. A TPD detector processes each sub-band and the sub-bands in which interference was detected are removed. After the analysis of the sub-bands, the bands are synthesized to reconstruct the original signal. An improvement in terms of bit-error-rate was shown for JSRs between 0 dB and 60 dB. An excision filter based on Radon Wigner distribution was studied in [225] for chirp jamming mitigation in generic DSSS systems. The DEF performance in the context of jammers for GNSS remains unclear and many excision filters have been designed for specific and particular interference types and cannot be applied broadly.

3) Pulse Blanking: PBMs are among the simplest time-domain interference suppression techniques [226] and have been studied extensively [227]–[230]. Several of these studies focus on unintentional interference from DME/TACAN. The principle idea is to reject or set to zero the signal in the periods its power exceeds a certain threshold. Borio [174] compares PBM with NF and shows that PBM performance is similar to ANF for low and moderate wideband jammers and much better than ANF for strong jammers (JNR $>$ 70 dB).

4) Wavelet-Based Mitigation: The wavelet transform decomposes the signal into a so-called mother wavelet and its derivative wavelet functions. It is able to capture highly variable signal characteristics in time and frequency domains. The key idea is to identify and isolate the interference signal in wavelet domain by extracting its wavelet coefficients in order to synthetically reconstruct the interference signal [175], [227]. This synthesized interference signal is then subtracted from the original received signal to mitigate the effect of interference without suppressing too much of the useful GNSS signal. The algorithm performs well for multiple pulse and narrowband interference [175], [227]. The drawbacks of wavelet-based interference mitigation method are its high complexity, as the complexity of the wavelet-based approaches increases exponentially with the number of wavelet decomposition stages, the need to adequately choose the mother wavelet, the thresholds to isolate the coefficients of interference signal. The convergence time can also be high.

5) Hilbert-Huang Transform (HHT): is an adaptive time-frequency method whose capabilities for jammer suppression was studied in [117]. The HHT has been introduced to deal with non-stationary and non-linear signals which cannot be described well enough with classical Fourier analysis. To detect and mitigate interference, the HHT decomposes the signal into the so-called intrinsic-mode functions. Then a pattern matching algorithm is used to estimate whether or not a jamming signal is present in the components of the intrinsic-mode functions. The main drawback of such a method is its very high computational complexity. According to [117], the HHT outperforms the wavelet transform-based mitigation method, particularly for high-power jammers with JSR above 100 dB.

6) Short Time Fourier Transform (STFT): is a time-frequency method, obtained via the Fourier transform of small, typically overlapping time segments of the signal. The computation over small time segments allows to follow the changes of the frequency content in time. If the spectral information of the jammer can be isolated, it can be used to remove the jammer component of the signal. The STFT can be used both as a detection and as a mitigation technique. Rezaei *et al.* [231] and Amin *et al.* [232] use a STFT to characterize and monitor the received GNSS signals. The method presented in [231] uses the STFT and also the Modified Short Time Fourier Transform (MSTFT), to search and track the peak of the jammer, and employs an infinite impulse-response notch filter to remove the jamming signal. The MSTFT uses an adaptive windowing process and estimates the time-frequency representation more accurate. Rezaei *et al.* [231] could therefore choose the excision filter narrower, which in turn reduces distortions of the GNSS signal. This benefit comes at the expense of a higher complexity. This method was tested and proved to work with linear frequency-modulated chirp jammer with JSR up to 60 dB [231].

7) Karhunen-Loève Transform (KLT): The KLT decomposes a signal in linear combinations of stochastic coefficients and basis functions, where the coefficients are orthogonal in the probability space, while the basis functions are orthogonal in the time domain. KLT projects the signal on the eigenfunctions domain where deterministic and stochastic signal components can be well separated and, thus, the jammer can be isolated from the signal part. The KLT as interference mitigation technique was studied for example in [233]. The KLT decomposition relies on the Toeplitz autocorrelation matrix of the received signal and on its eigenvalues. When interference is present only few eigenvalues have very large magnitudes – these correspond to the interference – while in the interference-free case the magnitudes of the eigenvalues are smaller and much less distinct – these correspond to the noise and GNSS signal. This fact is used to detect interference, and also to remove the interfering signal: by applying the inverse KLT only with the eigenfunctions that represent the noise and

GNSS signal. Due to eigenvalue decomposition, KLT is very sensitive to noise and may not work for low JSR.

8) Spatial-temporal Adaptive Processing (STAP): refers to two-dimensional filtering in space and time domain. It requires a steerable antenna array, i.e., a 1D spatial Finite Impulse Response (FIR) filter, in combination with 1D temporal FIR filter, where each antenna element is followed by a temporal FIR filter. The objective is typically to find the two-dimensional spatio-temporal filter weights that maximize the SJNR. STAP for GNSS interference suppression was studied in [234], [235]. In [234] only a limited set of results were provided, with no clear conclusions on the ability of narrowband interference suppression. In [235] the STAP method was compared with Minimum Powerless Distortion-less Response (MPDR) and showed to have better performance for an AM-tone jammer of Jammer-to-Noise Ratio (JNR) of 90 dB. The method was not tested for chirp jammers.

9) Interference Mitigation Using Robust Statistics [236], [237]: This method was derived from the theory of robust statistics from [238]. Two linear transforms are applied to the received signal samples. The first transform is used to project the jamming component into a domain where it admits a sparse representation. For example, a low-pass filter can be used to make the jamming component appear as a sequence of time pulses [236], [237]. After detecting the presence of jammer, a second linear transform inverts the previous transform and brings back the signal to time domain. Borio *et al.* [236] processed both CW and chirp signals for JSRs between -20 and 30 dB. The mitigation was effective even against powerful jammers (up to 30 dB of JSR), especially for CW signals [236].

10) Maximum Likelihood Estimator (MLE)-Based Direct Positioning Technique [239]: This method employs the Direct Position Estimation (DPE) approach [240], an approach which directly obtains the PVT solution without the intermediate steps of estimating observables. Wang *et al.* [239] designed a method for spoofer detection and mitigation that monitors MLE cost function of the DPE method. Based on the MLE PVT parameters, a composite signal that represent the authentic signals is reconstructed and then subtracted from the original signal. The residual signal is used for interference detection in a GLRT. The method proposed in [239] can detect and mitigate attacks even when all of the channels of the victim receiver are affected by interference. It was tested for a variety of spoofing attacks and detection probabilities up to 97% have been reported, at $P_{\mathrm{fa}} = 10^{-6}$, when seven satellite signals or more are available.

C. Mitigation Techniques at Post-Correlation or Link Level

Most of the post-correlation techniques proposed in the literature are meant for spoofing mitigation rather than for jamming mitigation. Indeed, spoofing mitigation is possible only if the true signals can be recognized and separated from the counterfeit ones. As a consequence, in a condition in which the authentic signals are cancelled by the spoofing, such as the 'coherent spoofing' described in [65], mitigation is unfeasible; nonetheless, such a kind of attack is quite complex to implement, especially for receivers in movement and relatively far from the attacker. In the other cases, the authentic signals can be discriminated using advanced processing techniques such as the mentioned vestigial signal tracking based on multi-correlator banks (see Section V). The underlying idea of such techniques, besides the specific implementation flavors, is to track all the different replicas of a satellite signals, discriminate between genuine and counterfeit, and employ for navigation only those that are recognized as genuine.

1) SuCcessive spoofing Cancellation (SCC) Method: The SCC described in [155] follows a detection and classification stage, in which the tracked signals are classified as counterfeit or authentic. Then, the SCC module receives as input the raw intermediate frequency samples, the list of forged signals and the corresponding tracked signal parameters, including code delay, Doppler frequency, carrier phase, and signal amplitude. These parameters are used to reconstruct the counterfeit signals and to remove them by subtraction from the raw samples of the received signal ensemble – in order to provide a spoofing-free sample stream. The SCC successively re-runs the signal acquisition on the spoofing-free samples to identify and then track the PRN code copies previously hidden by the counterfeit transmission. The iterations on detection/classification/cancellation end when all the signal channels in tracking are recognized as authentic and can be safely used for navigation. The performance of the method is promising for all the cases tested in [155]; nonetheless, the complexity of its practical implementation to achieve accurate results is high.

2) Subspace Projection Method: The accurate estimation of all the received signal parameters required for spoofing cancellation can be cumbersome and somehow fragile. To avoid that problem, the authors in [99] propose a subspace projection method that reduces the required input information to code delays and Doppler frequencies estimated by the tracking loops. The idea developed in [99] is that of constructing the signal subspace of the counterfeit signals, based on the quasi-orthogonality of their PRN codes. Then, the orthogonal projection of the received signal onto this subspace separates the false signals, which are subtracted from the whole ensemble so as to enable the acquisition and tracking of the genuine ones. The approach is robust in that it does not require the estimation of signal amplitudes, carrier phases, or data bits. However, its separation capability is limited to code delay differences between false and authentic signals greater than one chip period, meaning that a nearby spoofer cannot be detected with this method.

3) Integration INS/GNSS: A hybrid jamming mitigation algorithm relies on combining GNSS signals with other available signals, such as INS, cellular systems, etc. [241].

D. Mitigation Techniques at Navigation Level

Navigation-level techniques have the great advantage of exploiting the observables normally made available at the output of most receivers tracking stages; in this way, they do not need *ad-hoc* designs of the receiver correlation stage and therefore they can be applied to commercial and type-approved receivers. Since at the navigation stage the mitigation is only

possible by discarding the signals detected as forged, a consequent drawback is the possible reduction of navigation solution availability and continuity.

1) RAIM-Based Defences: Legacy RAIM techniques are able to detect the presence of corrupted pseudoranges that bias the computed PVT solution above a certain minimum threshold. However, as explicitly declared in [69], "RAIM defence is too weak against modern spoofers to justify a description".

2) Spatial Filtering: A special case is represented by *multi-antenna arrangements* [67], [68]. A receiver equipped with an antenna array, i.e., a set of antennas separated by (about) half a wavelength, could perform spatial filtering to shape its antenna beam pattern and cut down the reception gain in the direction of the non-authentic signals. Such type of "smart" antennas is commonly known as CRPA. Whereas as few as two antennas are normally enough for the detection of undesired signals, mitigation via beam shaping requires at least four antennas; typical arrangements use four to seven [159]. The major limitation of the multi-antenna approach is the equipment complexity, size, and cost; although it has been demonstrated that *antenna motion* can replace physical multi-antenna arrangement for spatial processing, the complexity of such implementations remains high [163]. The test setup presented in [163] clearly demonstrates the feasibility and effectiveness of multi-antenna processing for spoofing mitigation; however, in that case the employed synthetic aperture antenna was equivalent to a 250-elements antenna array, which is unfeasible in aviation domain.

Table VIII summarizes and compares the different interference mitigation methods existing in the literature.

IX. Performance Metrics and Examples of Comparative Performance

A. Performance Metrics

In order to be able to compare the different counter-interference methods and determine which is more accurate, we need to define some comparison metrics. In the vast literature dedicated to GNSS interference, there are no unified metrics to analyse the impact of interference or the interference countermeasures.

The performance assessment of interference detection algorithms is basically intended as the quantification of the capability to determine, to a targeted confidence level, whether counterfeit signals are present or not in the received signal ensemble [159]. For safety-of-life applications, such as those used in the civil aviation field, the reliability of the employed methods is fundamental, which is commonly expressed through requirements on [159].

Probability of false alarm: the probability of *raising* an interference alarm when *no interferer* is active, which must be kept below a target limit to guarantee system availability above a minimum level of quality of service (P_{fa}, e.g., used in [139], [249]–[251], see Eq. (16));

Probability of detection: the probability of *raising* an interference alarm when interference is *active* (P_{d}, e.g., used in [117], [239], [249], [250], see Eq. (16));

Probability of miss-detection: the probability of *not raising* an interference alarm when an interferer is *active*, which must be kept low enough not to exceed the safety level of the system ($P_{\mathrm{md}} = 1 - P_{\mathrm{d}}$) [159].

Probabilistic approaches relying on P_{fa}, P_{d} and/or P_{md} are very attractive for three main reasons: 1) it allows to set system requirements first (the probabilities) and from them to derive decision thresholds for the algorithms; 2) a vast knowledge in the field of the detection theory is available and applicable [72], [73], [219]; 3) it allows to consistently compare performance of extremely different algorithms, because the evaluation is done in the system domain instead of the signal domain. The drawback is that this approach is based on a precise statistical characterisation of the detection metrics, which sometimes is not easy or is even impossible to express and to manage in closed form.

In addition to probability-based metrics, the following metrics are often encountered when dealing with the interference management solutions:

Mean, variance, Root Mean Square Error (RMSE), or Cumulative Distribution Function (CDF): a descriptive statistic of the estimation error, where the error can refer to the position error or to the angle error (i.e., azimuth and elevation) in estimating the position/direction of the interferer (e.g., used in [77], [83], [140], [181], [182], [182], [252]);

Spectral Separation Coefficient (SSC): a measure of how much the frequencies of the GNSS signal and of the interferer signal intersect; this is a purely theoretical metric which assumes known signal and interference spectra [253], [254];

Effective C/N_0: the C/N_0 measured in the presence of the interference signal [128], [140], [253], [254], which can be significantly smaller than the C/N_0 measured in the absence of interference, especially in the cases of jamming-type of interference. The effective C/N_0 is typically derived theoretically as a function of SSC, when the interference spectrum is assumed known.

Another approach to compare the performance of jamming and spoofing detection algorithms is the so-called *vulnerability region* [64]. Given a distinguishing parameter of the interference (e.g., power, interference-to-noise ratio, interference-to-signal ratio) on the *x*-axis and the detection metric used by the algorithm on the *y*-axis, the applied detection threshold cuts the quadrant in two regions. The region that includes feasible values of the *x*-axis for which the detection metric is below the detection threshold indicates conditions for which the algorithm is expected to fail in detecting the interference (vulnerability). The smaller the vulnerability region, the more robust the algorithm with respect to the parameter indicated on the *x*-axis. In this case the performance metric is defined in the signal domain and the consistency of the detection metrics for different algorithms must be carefully verified.

Finally, the induced variations on all the observable data produced by a receiver exposed to a spoofing attack can be used to evaluate the residual receiver vulnerability to the attack. An example of comprehensive analysis of all the observables for three receivers under tests and several spoofing test cases is contained in [76].

TABLE VIII
SUMMARY OF INTERFERENCE MITIGATION METHODS FROM LITERATURE. THE COLOUR CODE IN COMPLEXITY AND PERFORMANCE COLUMNS SUPPORTS A QUICK ASSESSMENT, LIGHT-COLOURED REGIONS ARE BETTER THAN DARK-COLORED REGIONS

Domain	Algorithm	Type of Interference			Complexity	Performance	Limitations	References
		Jammer	Spoofer	Others				
Front-End	Switching frequencies	✓	✓	✓			It requires a prior interference detector and it assumes that at least one GNSS frequency is not affected by interference (typically untrue); it also requires multi-GNSS receivers	[85]
	CRPA; adaptive beamforming; MPDR	✓	✓	✓			It requires multi GNSS-antennas on-board of the aircraft, which is a huge limiting factor, also antennas need to be closely spaced (below $\lambda/2$), which would create cross-interference to other on-board antennas	[214], [215], [242]–[244]
	Switching antennas	✓	✓	✓			Large spacing between antennas needed (e.g., tens of m), for significant difference in JSRs from the antennas; not feasible on-board of the aircraft	[213]
Pre-correlation	NF; ANF	✓					Poor for multiple concurrent jammers; adaptive NF works better than non-adaptive NF, but its parameter need to be adjusted for each jammer type (i.e., a priori jammer classification required)	[127]–[130], [222]
	DEF	✓					Not working well for chirp jammers	[224], [225]
	PBM and frequency-zeroing	✓					Threshold choice is jammer-dependent; it also requires a prior jammer classification algorithm; it does not work well for chirp jammers	[130]
	Wavelet-based mitigation	✓	✓	✓			Not studied much in the GNSS context; working only at high JSR; not working for high-frequency jammers	[90], [175], [245]
	HHT	✓					Not studied much in the GNSS context; working only at high JSR	[117]
	STFT; MSTFT	✓		✓			Studied only for chirp jammers; accuracy of MSTFT is slightly better than the accuracy of STFT at a slight increase in complexity	[231], [232], [246]
	KLT	✓					Not studied for chirp jammers	[233]
	STAP	✓					It requires multi-antenna arrays on-board of the aircraft; not studied for chirp jammers	[99], [234], [235]
	Interference mitigation using robust statistics	✓					Studied only with AM jammer; the performance is highly sensitive to the Huber threshold to be fine-tuned according to the JSR	[236], [247]
	MLE		✓				It does not work when both the number of spoofing signals and number of legitimate GNSS signals is smaller than 4; it also works poorly at low C/N_0	[239]
Post-correlation, single-link level	SCC		✓				The necessary accurate estimation of all the signal parameters used for cancellation may result in a fragile approach	[155]
	Subspace projection		✓				It works for delay misalignment between counterfeit and genuine signals greater than one chip	[99]
Post-correlation, multi-link/ navigation level	Integration INS/GNSS	✓	✓	✓			Additional hardware/sensors needed; GNSS signal quality may be very poor if the interferer was not additionally mitigated up to the post-correlation domain	[241], [248]

Complexity: ■ – low, ■ – moderate, ■ – high, ■ – very high
Performance: ■ – poor, ■ – medium, ■ – good

In Table IX we summarise the most relevant metrics found in literature and which can be used to compare various countermeasures for GNSS interference. Most of the metrics can be used for any type of interference and for any of the four stages identified in Section III to manage the interference (detection, localization, classification, mitigation). Some metrics, such as

TABLE IX
COMPARATIVE PERFORMANCE METRICS IN ADDRESSING THE INTERFERENCE IN GNSS

Metric	Where Applicable	Challenges	References
SSC and effective C/N_0	Interference detection and mitigation	Rather theoretical concepts, not giving a very accurate image of the detection and mitigation capabilities of an algorithm	[253]
Measured CNR	Interference detection and mitigation	Not very accurate	[140]
Signal-to-Noise Ratio (SNR) degradation	Interference detection and mitigation	It requires the knowledge of the nominal SNR, in the absence of interference	[108]
Detection, miss-detection and false alarm probabilities (P_{d},P_{md},P_{fa})	Interference detection	Good detection thresholds are difficult to be found and they depend on each algorithm	[117], [249], [250]
Spectrogram inspection	Interference detection, mitigation and classification	It typically requires manual inspection and it does not provide a comprehensive performance evaluation	[202], [255]
Detection and miss-classification probabilities	Interference classification	Good classification thresholds are difficult to be found and they depend on each algorithm	[250]
Angle errors (mean, standard deviation, RMSE, CDF)	Interference mitigation and direction finding	Large angle errors may not be useful in dealing with interference	[252]
Position errors (mean, standard deviation, RMSE, CDF)	Interference localization	RMSE and CDF are typically more comprehensive than mean and standard deviation figures	[77], [140], [182]
GNSS signal acquisition probability	Interference detection and mitigation	it requires access to the GNSS acquisition outputs	[224]
Pseudorange double difference	Spoofing detection and mitigation	It requires carrier phase measurements, applicable only to spoofing	[68]
Vulnerability region	Interference detection	It requires precise statistical characterisation of the detection metrics	[64]

pseudorange double differences, are only relevant for some particular contexts (e.g., spoofing detection and mitigation techniques).

B. Comparative Detection Performance for Jammer Detection

This section shows a comparison between different detection algorithms against three different jammer types, selected as the most representative between the various jammer types, as they are the ones most encountered in literature studies: CW, chirp and DME-like. The results shown in this sub-section are based on MATLAB simulations. For the simulations parameters we used 10^5 independent Monte-Carlo iterations. The considered satellite signal was an GPS C/A L1 signal with a C/N_0 of 45 dB-Hz. The channel used was a fading channel model with a single path for the GNSS signal and a multipath model composed of 5 paths for the jammer signal. The jammer ground-to-air channel and the GNSS satellite-to-air channels were modeled as uncorrelated channels.

Fig. 10, Fig. 11 and Fig. 12 show the probability of detection for a CW jammer, a chirp jammer, and a DME-like jammer, respectively.

We remarked that the best detection performance against the different jammer types are generally yielded by the power based detectors, such as AGC, TPD, FPD, Welch and Periodogram. In the case of CW and chirp signal, the jammer can be reliably detected even at JSRs below 0 dB. Especially the FPD detector offers the best performance at any JSR

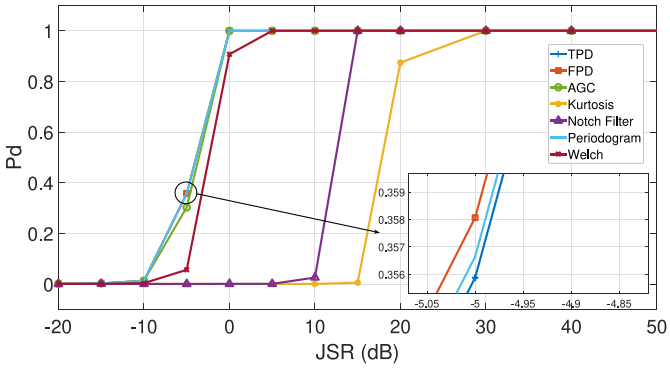


Fig. 10. Probability of detection of an CW jammer for different jamming powers.

among the considered detectors, except for the DME-like jamming signal, although the differences in performance between the top three methods are rather small (below 1 dB of difference of JSR to obtain the same amount of P_{d}). Further comparison of Fig. 10, Fig. 11 and Fig. 12 shows that the detection methods behave similar for AM and chirp signals. The detection probability start to be non-zero at JSR higher than -15 dB. The main difference between the analyzed detection algorithms occurs with the notch filter, which requires up to 15 dB more jamming power to detect the jammer compared with the rest of methods. In the three considered cases (i.e., CW, chirp-jamming and DME-like/pulse), in order to achieve $P_{\mathrm{d}} = 1$ with any of the methods, we need a jammer transmitting with a JSR of at least 0 dB. The detectors that offer the worst performance among the considered ones are the Notch

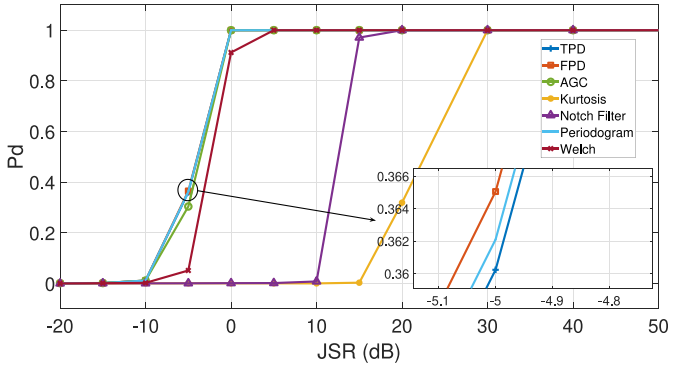


Fig. 11. Probability of detection of a chirp jammer for different jamming powers.

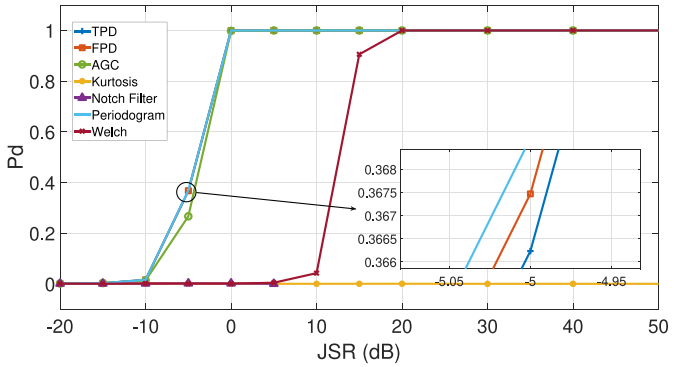


Fig. 12. Probability of detection of a DME-like jammer for different jamming powers.

Filter and the detector based on the Kurtosis. In addition, as it is shown in Fig. 12, the Kurtosis detector does not work at all with DME-like/pulse jammers; in this case, the jammer signal stays virtually undetected. The reason is that the pulses of the considered signal are too short and are not repeated constantly, which makes it undetectable with the considered detectors.

C. Comparative Detection Performance for Spoofing Detection

An example of spoofing detection analysis based on Monte Carlo evaluation of the false alarm rate is shown in Fig. 13. The algorithm under test is the D^3 [166], mentioned in Section V. The false alarm rate, defined as the number of false spoofing identifications over the total number of decisions along a Monte Carlo simulation test, is used as an estimator of the probability of false alarm P_{fa}. It is evaluated in nominal signal conditions (no spoofing active) as a function of the C/N_0 ratio of the authentic signals. The simulation length for each point of the plot was 300 seconds $\times$ 9 satellites. The parameters of the D^3 configurations compared in the figure are the detection window length, t_{det}, and the distance between the two antennas, l_{b}. The figure shows that, with the parameters under test, the false alarm rate is below 3% for any C/N_0 level with a detection window of 3 s, and below 1% for any C/N_0 level with a detection window of 1 s. The antenna distance has quite limited impact on the performance.

A similar Mont Carlo approach is used in Fig. 14 to compare the performance of the D^3 detector with that of the Sum of

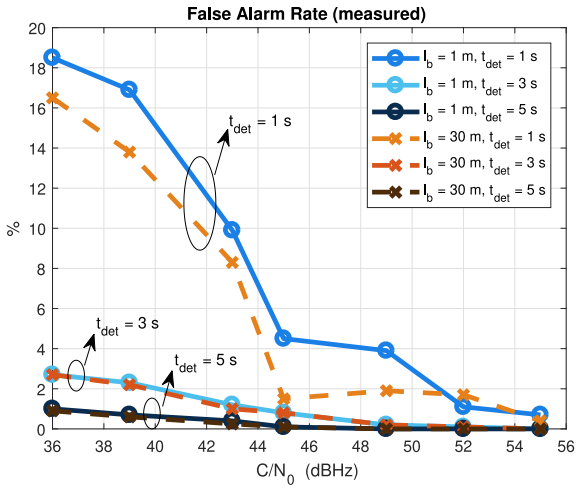


Fig. 13. Comparison of false alarm rates from Monte Carlo simulations for the D^3 dual-antenna spoofing detector, as a function of the C/N_0 ratio of the genuine signal and for different choices of parameters of the D^3 algorithm.

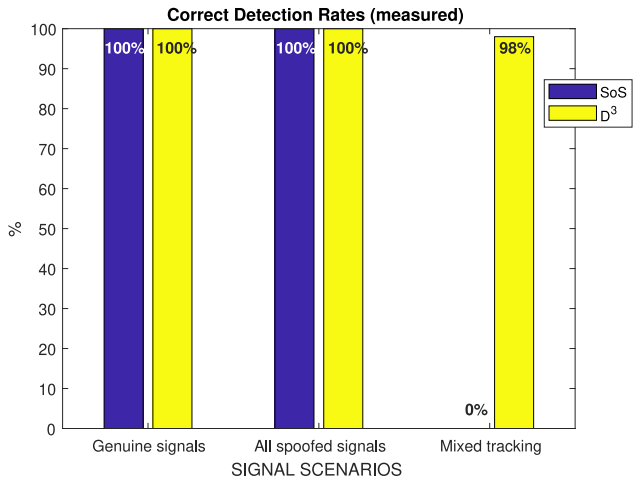


Fig. 14. Correct detection rates from Monte Carlo simulations for the SoS and D^3 dual-antenna spoofing detectors, in different signal conditions.

Squares (SoS) [67]. In this case, the correct detection rates were computed in three different scenarios: a case of genuine signal ensemble (without spoofing), to estimated the correct detection probability $(1 - P_{\mathrm{fa}})$, and two cases of spoofed signals, where in the latter the receiver experiences a 'mixed tracking'; these cases give an estimate of the probability of detection P_{d}. The purpose of the comparison is to show that the D^3 detector is as reliable as the SoS in the first two scenarios, and is also able to cope with a 'mixed tracking' scenario with very high reliability, where instead the SoS totally fails [166].

D. Examples of Direction Finding and Positioning of an RFI Source

This section compares two approaches to infer the location of an RFI source jamming the GPS L1 band. In addition to the interferer, we simulate GNSS signals and a noisy fading channels for an en-route scenario. The first approach is based on a small antenna array as part of a on-board system. The channels in that case consist of uncorrelated single fading paths

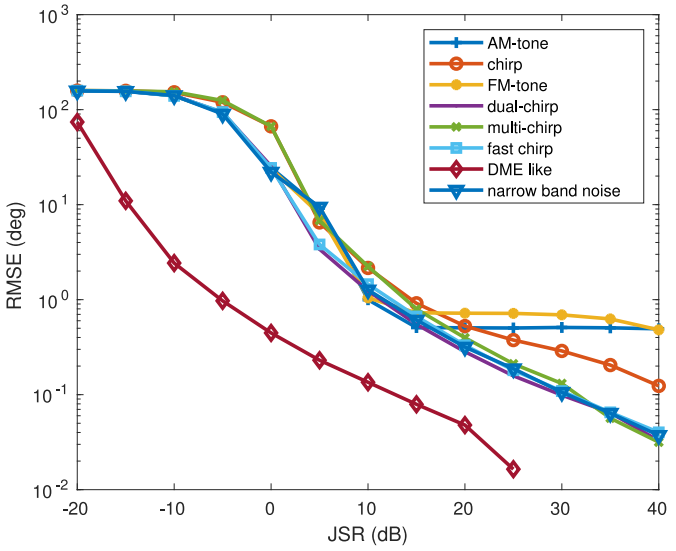


Fig. 15. AoA estimation (azimuth) with three-element antenna array in a triangular configuration with about 1 m inter-element distance.

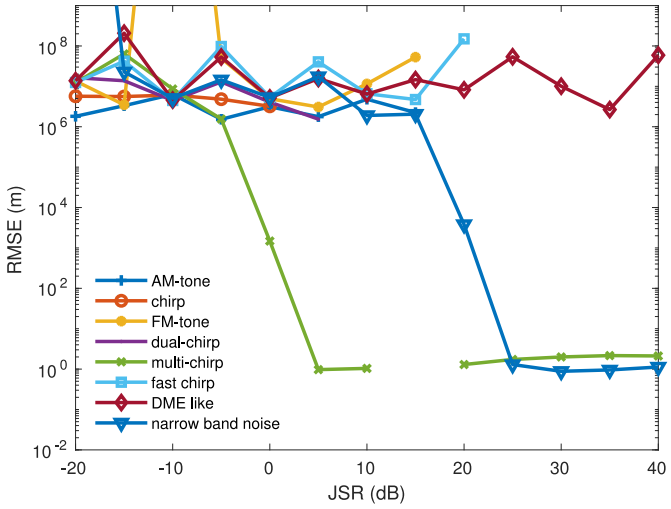


Fig. 16. Position estimation (two-dimensional) based on TDoA estimates with three antennas in a triangular configuration with baselines about 10 km.

for both the jamming signal and the GNSS signals. The second approach uses a large antenna configuration as it could be used to cover the surrounding area of an airport. For this case we assume multi-path propagation for the jamming signal, and single LOS path for each of the GNSS signals. For each approach we show the performance for different jamming signals, see Table III and Fig. 7.

For the on-board approach we simulated a RFI source at a distance of 1 km from the aircraft. The antenna array consists of three elements placed on the vertices of a triangle in a distance of about 1 m. The spatial spectrum and the AoA were estimated using the MPDR method [219]. Fig. 15 shows the AoA for different jamming signals.

At a JSR of about 15 dB the accuracy is about 1°. The DME like jammer concentrates its energy in a relatively small time-frequency section and its AoA can be estimated accurately already at 0 dB. Harder to localize is a narrow band noise jammer.

The second case is the jammer localization with TDoA measurements from ground stations. The antennas are placed in a triangle and the baseline between the three antennas is about 10 km. The TDoAs are estimated by cross-correlating the outputs of two different antennas and the position solution is computed using iterative, linearized Least Squares (LS) algorithm. Fig. 16 shows the positioning accuracy for this scenario.

Large outliers are observable in low JSR regimes for the FM-tone and narrowband noise signal. Moreover, the algorithm did not converge in all cases, which explains the interrupted graphs and missing data points.

X. Design Recommendations for Dealing With Interferences in SatNav for Aviation

Our literature survey and own investigations based on theoretical analysis, simulations, and experimental work as shown in previous sections, point out towards the following main findings regarding the interference management in GNSS:

- In order to detect both jamming-type and spoofing/meaconing-type of interferences, there is the need to incorporate two interference detection blocks in the SatNav receiver: one in the pre-correlation domain for the jammer detection and another in the navigation domain for the spoofer detection. Unlike the jammer detectors which can be implemented with a relative low cost, the anti-spoofing post-correlation detectors would require profound modifications to the HW/firmware of the receiver and therefore have been ranked as less suitable for acceptance in aviation domain.
- It is recognized that a single technique able to deal with all the possible interference conditions – either jamming or spoofing – does not exist and a combination of techniques is the most promising approach in terms of safety. Nonetheless, in the vast panorama brought to light in this paper, it is possible to identify some especially effective techniques. The most suitable methods for interference detection in a SatNav receiver used in aviation were identified to be the AGC and time and frequency power detectors (TPD, FPD) for the jammer detection and the SoS/D^3 dual-antenna detector for the spoofing detection.
- The algorithms giving the best tradeoffs between complexity and performance for the interference localization/direction finding were identified to be the AoA algorithms for both jamming and spoofing. To reduce the additional complexity and extra interference due to placing additional antennas on board of the aircraft, maximum three GNSS on-board antennas are recommended for the AoA-based interference localization. Nevertheless, one antenna suffices for jamming detection and only two antennas are required for spoofing detection with SoS or D^3.
- In terms of interference mitigation approaches for aviation, when the number of GNSS antennas must be kept to a minimum, the most promising ones for jammer mitigation are the pre-correlation approaches, such as ANF or PBM, if an a priori interference classifier block is used or MSTFT if no a priori classifier is used. The spoofing mitigation is effective only in the post-correlation/navigation domain.

- Last but not least, the current literature on interference classification in GNSS is rather scarce and no conclusive algorithms could be found to work for all types of interferences. Machine learning classifier seem promising, but their performance or complexity as classifiers of GNSS interferences has yet to be studied.

In addition to the challenges related to GNSS-based navigation in aviation, there are of course challenges related to communication aspects, which fall outside the focus of this paper. Good surveys on communication challenges and solutions in future aviation can be found for example in [256] (future aeronautical communication systems), [257] (air traffic security solutions), [258] (medium access control protocols for UAV) and [259] (aeronautical channel models).

XI. Challenges, Future Trends in Navigation for Aircraft and Open Research Directions

The future of SatNav on-board of aircraft is expected to follow some evolutionary trends that also will open new research challenges and will shape future research directions [2], [12], [260]–[263]. The main trend in GNSS is certainly the development towards dual/multi-frequency and multi-constellation receivers in order to improve accuracy, availability, continuity, and resilience to atmospheric effects, multipath and interference. Today's high-precision and mass-market receivers already offer Dual-Frequency Multi-Constellation (DFMC) support. Although moving at sensibly slower pace for reasons of regulation, safety and certification, the GNSS receivers segment for civil aviation is evolving in the same direction of DFMC. ICAO and European Organisation for Civil Aviation Equipment (EUROCAE) are working at the definition of the next generation standards for DFMC GNSS, targeting Minimum Operational Performance Standards (MOPS) for GPS and Galileo on L1/E1 and L5/E5a frequency bands. The ICAO concept of operations for DFMC GNSS dates from April 2018.

Following the above-mentioned DFMC evolution, in the near future SBAS is expected to support DFMC capabilities in order to take advantage of GNSSs other than GPS and of dual-frequency operations. The next generation of EGNOS (EGNOSv3) will provide its corrections and integrity services for DFMC. According to European GNSS Agency (GSA)'s notes available at the time of writing, EGNOSv3 operational target date is foreseen around 2022, while its Safety-of-Life service is foreseen to become operational around 2024. Before that date, the new generation of user terminals needs to have been industrialised and certified, so that aviation users can be equipped with new receivers. A similar evolution must be pursued by the GBASs.

The main development trends in the navigation domain for aviation can be summarized as follows.

a) *Advanced coping with RFI:* The vulnerabilities of GNSSs are a well-known risk since longtime; however, with the evolution of the GNSS role they have become more and more of an issue, as also emphasized in our survey. Coping with RFI in the future is also likely to follow the above-mentioned DFMC trends, posing new challenges for researchers to deal with interferences in dual/multi-frequency bands and multi-constellation receivers while preserving an affordably low complexity.

As RFI mitigation is now known to be a challenge in aviation, ICAO released a "GNSS RFI Mitigation Plan" in 2017, in order to give a strong push towards the investigation and adoption of interference countermeasures. Also Radio Technical Commission for Aeronautics (RTCA) and EUROCAE are working in the same direction. The introduction of DFMC is seen as strongly beneficial, however it is expected that receivers and antennas could need to include superior technologies and algorithms to improve their resilience to RFI. Ensuring the integrity of more complex on-board GNSS receiver and computing protection levels, etc. is a progressing challenge as significantly more information from different sources/methods needs to be combined compared with existing solutions.

b) *Facing the spoofing risk in aviation:* The risk of a spoofing attack purposely directed to a civil aircraft has been seen as relatively unlikely so far, because of the very high technical complexity of its implementation when the aircraft is in flight (on the contrary, the airport areas should be constantly monitored by terrestrial stations); also "collateral" spoofing, in which the aircraft is affected though not being the intended victim of the attack, is not labelled with high probability of success. Nevertheless, in the panorama traced above where GNSS is increasing its role in navigation operations, this risk should not be relegated as negligible, but should be managed with appropriate measures. The GATEMAN project promoted by the Single European Sky Air traffic management Research (SESAR) Joint Undertaking is an example of research targeted to future RFI and spoofing management procedures [264], [265].

c) *The role of GNSS authentication:* The GNSS authentication mechanisms foreseen for Galileo [266] and, in a farther future, for GPS [267] add an intrinsic anti-spoofing barrier in the Signal-In-Space. Nonetheless, the suitability and effectiveness of such mechanisms in civil aviation has not been proved so far, because they should be compared against the strict availability, continuity and time-to-alert requirements posed by the aviation standards. Also the presence of key management protocols has to be verified for acceptance in the civil aviation safety framework. In general, this topic still leaves wide spaces for technical research and strategic discussions.

d) *Advanced Receiver Autonomous Integrity Monitoring (ARAIM):* According to this evolutionary trend, the ARAIM-Milestone 3 released by the ARAIM working group in February 2016 has included the concept evolution towards DFMC. The complementarity and coexistence of ARAIM with SBAS in the future evolutions have been reinforced. ARAIM challenges in civil aviation have recently been addressed in [268].

e) *Evolution of the GNSS role:* The solid improvement of performance expected from DFMC operations, including SBAS and ARAIM, fosters a fundamental change in the role of GNSS in the civil aviation domain: from a supplemental means of navigation, GNSS is rushing to become the primary one, while legacy terrestrial aids, such as ILS, VOR, DME,

seem destined to cover more and more a backup role in case of GNSS outage.

f) *The concept of Free Route Airspace (FRA):* In this evolved panorama, a new concept is emerging, enabled by the new trust on GNSS. Free Route Airspace (FRA) is a novel approach for the management of the airspace, in which aircraft will be allowed to select the most economical route between two points. The introduction of this concept changes the perception of GNSS from simple sensor to a component of the traffic management system and, as such, necessitates the involvement of many different stakeholders, e.g., air traffic controllers, pilots, carriers, etc. The FRA concept and its associated challenges is detailed for example in [269].

Further research trends can be recognized in:

g) *5G mobile communication network:* 5G has the potential to provide positioning services with a more precise accuracy (below 10 cm) than GNSS using the existing infrastructure [28], [270]. The position provided by 5G has to be accurate (centimeter-level), reliable, and with a low latency (few ms). The main drawback for aviation is that currently the cellular antennas are not pointing to the sky, so the communication range is reduced. In addition, 5G mm-wave signals will suffer high path losses compared to cm-wave signals and will be unlikely to be received at medium and high-altitude, thus such solutions are likely to be limited to drones and other low-altitude aircraft and in the vicinity of the airports. An open research challenge remains to design the future 5G systems also with antenna up-tilting, in order to better serve also the aerial users and vehicles, and the reliability required in aviation.

h) *Airbone Separation Assurance System (ASAS):* ASAS [271] provides pilots assistance to maintain the required separation between aircraft, while information about the surrounding traffic is also provided. ASAS enables the possibility of the flexible use of airspace ('free-flight'). With ASAS, the airspace capacity may increase, as well as the congestion might be reduced since aircraft may fly closer to each other. In addition, ASAS does not depend on ground-to-air communication.

i) *N-D trajectory management:* This concept, used on Eurocontrol and SESAR pages [272], [273] relies on adding additional dimensions ($N \geq 4$) to the traditional 3-D navigation parameters (latitude, longitude, altitude), including information such as the wind speeds, temperature modelling, fog, and mist estimation, etc. N-D trajectory management can thus offer additional protection against interference, as channel/environmental effects are likely to be very different on the interferer-aircraft channel compared to the satellite-aircraft channel. However further research is needed to fully understand the capabilities of N-D trajectory management to deal with wireless interference.

j) *Cloud-based GNSS:* Cloud GNSS receivers [274]–[277] make easier the implementation of sophisticated signal processing techniques, since the actual processing of the GNSS samples is not done in the aircraft. The processing is done remotely in cloud terrestrial servers, and this can be more powerful and accurate than the in-built/on-board GNSS receivers. In addition, upgrades such as adding new signals or new constellations are easier to implement in cloud, since the only needed modifications are to be applied at the cloud side [274]. Cloud GNSS receivers operation is really simple: the user terminal only needs to collect the RF samples and to transmit them to the cloud infrastructure, where the GNSS signal processing takes place. Some of the main challenges in cloud-based GNSS will be to achieve low latency in the navigation solution and to provide authentication and security of the navigation solution.

k) *Machine learning in GNSS:* An increased use of machine learning techniques in GNSS is expected also in aviation domain. Machine learning techniques might be useful for aiding the navigation estimation by using the vehicle dynamic model [278], for detecting ionospheric scintillations [279] or for detecting the multipaths [280]. Machine learning algorithms may also find their applicability to detect and classify jamming and spoofing [143], [210] and further research is needed in order to explore the vast possibilities of the machine learning techniques in the aviation domain.

XII. Conclusion

This paper has provided a comprehensive survey of interference types in GNSS systems as well as of interference management solutions, namely interference detection, localization, classification, and mitigation methods existing in the specialized literature on SatNav systems from the last four decades. Because the intentional interference, such as jamming and spoofing, are the most threatening and increasingly occurring in SatNav systems, the focus here has been on these intentional interferences. However, the surveyed methods apply as well to unintentional interferences, as most of them can be also modeled via the jammer or spoofer models given in Section IV. In addition, our focus has been on SatNav in aviation.

The counter-interference solutions in aviation domain need to fulfil additional constraints compared to other counter-interference solutions in GNSS in general. Examples of such constraints are: to keep the number of additionally needed antennas on-board of an aircraft to a minimum, to not create additional interference with other on-board wireless receivers, to take into account that the on-board antenna placement is limited by the surface of the fuselage due to vibrations of less rigid parts of an aircraft, etc. After surveying different methods in detecting, mitigating, localizing, and classifying the interferers in GNSS, our Section X summarized the main findings in the context of aviation, in order to convey significant take-away points to a possible designer.

We have shown that the research areas of interference detection, mitigation, and localization have been widely covered by the research community so far, while the research area of interference classification is still lagging behind and there are still not many methods investigated in the context of GNSS interference classification. We have also provided unified and comprehensive mathematical models of jammers, spoofers, and meaconers in GNSS and we analyzed how different interference countermeasures are applicable to each interference type. We pointed out that one cannot generally use the same receiver algorithm to deal with all types of interferences, as most algorithms work only with a particular

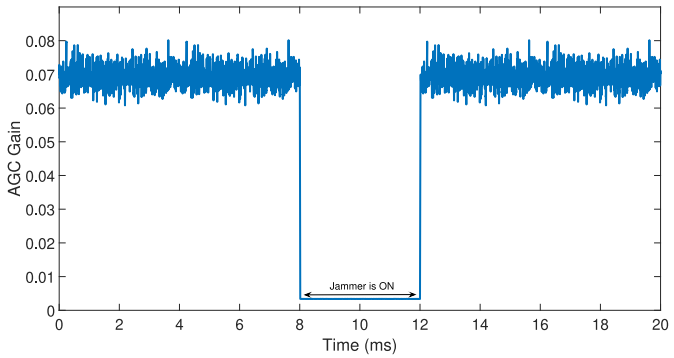


Fig. 17. Example of test statistic of AGC detector for a double-tone AM jamming signal. JSR and C/N_0 are 40 dB and 50 dBHz, respectively.

interference type. Also, as a general rule, the pre-correlation-level methods proved to be more effective than other methods in the context of jamming-type of interference; while to combat spoofing, the methods at navigation-level tend to outperform the methods at other receiver stages, if a trade-off between complexity and performance is set up. We have also shown that AoA-based localization methods are the ones with the best performance-complexity trade-off for localizing interferers.

Future trends and open challenges were also discussed in Section XI. Future possible directions in the aviation area are to complement the existing on-board navigation solutions with alternative solutions, while ensuring the reliability required in aviation; for example, with those based on DFMC GNSS, on cloud GNSS, or on the upcoming 5G signals. Expanding the existing algorithms with machine learning solutions and N-D trajectory management are an other timely research directions in this field.

APPENDIX
EXAMPLES OF INTERFERENCE DETECTORS

This Appendix gives some numerical examples of various interference detectors, based on the discussions in Section V. These examples can shed more light for the interested readers into the details of various interference detection algorithms.

An example of an AGC detector for a two-tone AM jamming signal is shown in Fig. 17, for the situation when the jammer is disabled during the first 8 ms, enabled for the next 4 ms, and then off again. A clear drop in the AGC gain is observed when the jammer is on (less gain is required since the signal at the input is stronger), so this can be a good indicator about the jammer presence.

Figure 18 exemplifies a PDF detector for a 'clean' GPS signal (no interference) and two types of jammers (single-tone AM and single-chirp jammer). The samples are clearly not normally distributed in the presence of jammers.

Fig. 19 illustrates how the test statistic of an TPD detector can evolve over a time period while the jammer is absent and present.

The signal power increases considerably after 7 ms, which is the time instant the jammer is switched on. At this moment the estimated input power starts increasing, until it reaches a maximum, where the window of samples to compute the TPD takes into account only the time instants where the jammer is

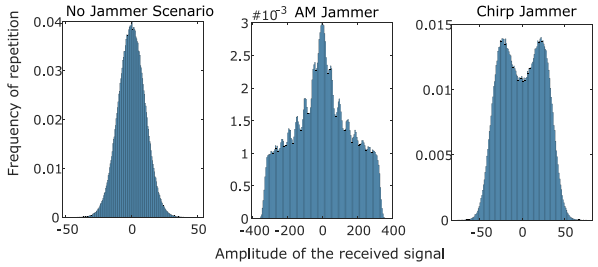


Fig. 18. Example of PDF detector's test statistic for AM and chirp jamming signals. JSR and C/N_0 are 40 dB and 50 dBHz, respectively.

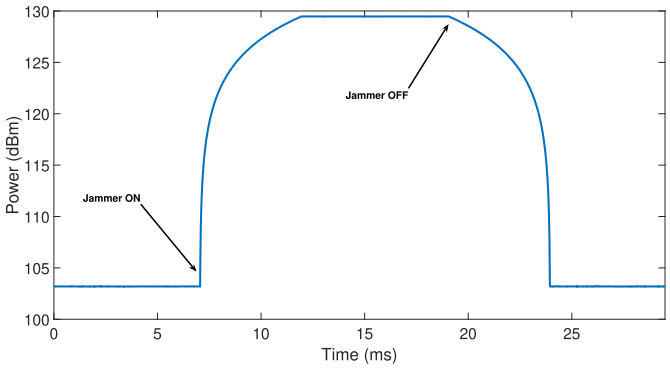
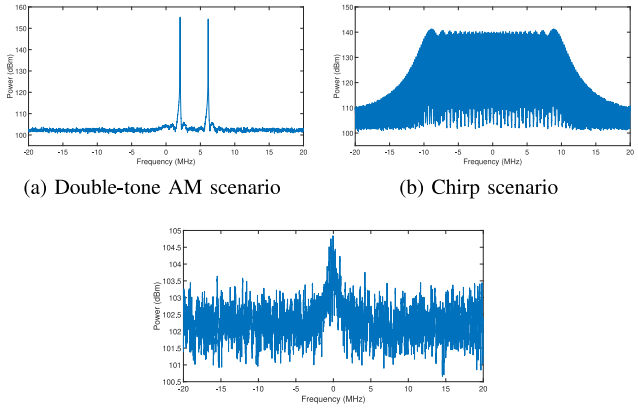


Fig. 19. Example of test statistic of TPD detector for double-tone AM jamming signal. JSR and C/N_0 are 40 dB and 50 dBHz, respectively. The window time used by the detector algorithm is 5 ms.



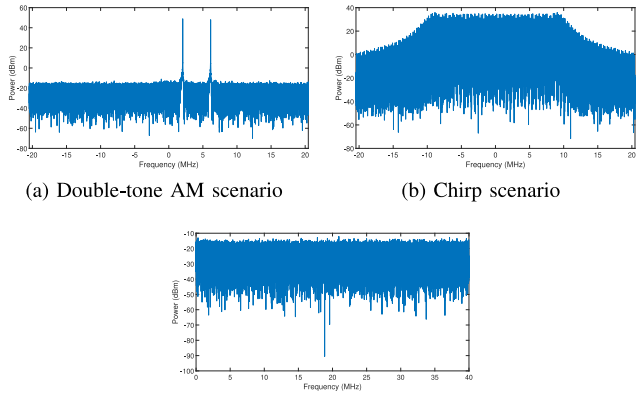
(a) Double-tone AM scenario (b) Chirp scenario

(c) No jammer scenario

Fig. 20. Example test statistic of FPD detector for double-tone AM and chirp jammers. The no-jammer case is also shown as a reference. The time window used by the detection algorithm was 5 μs.

on. At about 20 ms the jammer is switched off, and then the detected power returns to the nominal level before the jammer was enabled.

An example of an FPD detector is shown in Fig. 20. Sub-plot Fig. 20(c) shows the FPD's test statistic when the jammer absent. In the sub-plot Fig. 20(a), the case of a two-tone AM jammer is shown. The power of the AM tone jammer is about 50 dBm above the rest of the signal on the frequencies of both AM tones. In this case, the test statistic shows the tone's frequencies, knowledge that might be exploited for jamming mitigation. Figure 20(b) shows a chirp jammer with a power 35 dBm higher than the GNSS signal, over the whole sweep



(a) Double-tone AM scenario (b) Chirp scenario

(c) No jammer scenario

Fig. 21. Example test statistic of periodogram detector for double-tone AM and chirp jammers. The no-jammer case is also shown as a reference. The length of the used window was 5 μs.

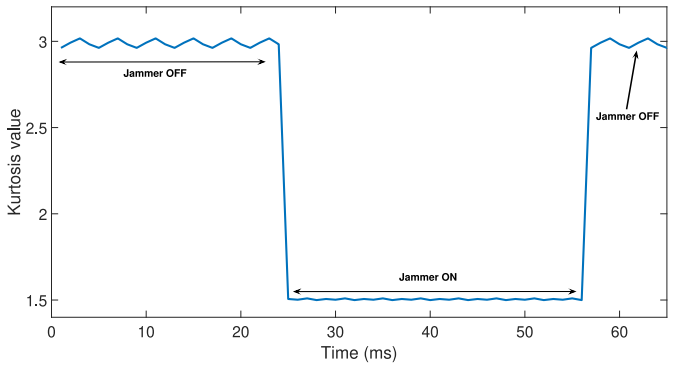


Fig. 22. Example test statistic of Kurtosis detector for AM jammer. JSR=40 dB and CNR=50 dBHz. The window time for the detector algorithm was 1 ms.

range. For the chirp jammer, the instantaneous frequency can not be determined easily.

Fig. 21 shows the Welch periodogram as the test statistic in the presence of a double-tone AM jammer (Fig. 21(a)), a chirp jammer (Fig. 21(b)), and a GNSS signal without any jammer (Fig. 21(c)). The jammers here were assumed to be 20 dBm stronger than the GNSS signal.

Fig. 22 shows an example of a Kurtosis detector for an AM jammer.

We can see from Fig. 22 that as long as the jammer is off, the Kurtosis is approximately 3. Otherwise the value of the kurtosis drops significantly (e.g., it is halved in this example), signaling the presence of a jammer.

ACKNOWLEDGMENT

The opinions expressed herein reflect the authors' views only. Under no circumstances shall the SESAR Joint Undertaking be responsible for any use that may be made of the information contained herein.

REFERENCES

[1] "Unmanned aerial vehicle (UAV) market by application, class, system (UAV platforms, UAV payloads, UAV GCS, UAV data links, UAV launch and recovery systems), UAV type, mode of operation, range, point of sale, MTOW, and regionÚGlobal forecast to 2025," Res. Markets, Dublin, Ireland, Rep. AS-2802, Oct. 2019.

[2] GSA. *GSA Market Report 2017*. Accessed: Sep. 2, 2018. [Online]. Available: https://www.gsa.europa.eu/newsroom/news/european-gnss-agency-gsa-launches-2017-gnss-market-report

[3] L. Gupta, R. Jain, and G. Vaszkun, "Survey of important issues in UAV communication networks," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1123–1152, 2nd Quart., 2016.

[4] P. Enge, "Satellite navigation: Present and future," *URSI Radio Sci. Bull.* no. 341, pp. 5–9, Jun. 2012.

[5] ICAO. *Aeronautical Telecommunications: Volume IV—Surveillance Radar and Collision Avoidance Systems. Annex 10 to the Convention on International Civil Aviation*. Accessed: Jan. 31, 2019. [Online]. Available: https://cfapp.icao.int/tools/ATMiKIT/story_content/external_files/story_content/external_files/Annex10_Volume

[6] IATA. *Safety Report 2017*. Accessed: Aug. 28, 2018. [Online]. Available: https://aviation-safety.net/airlinesafety/industry/reports/IATA-safety-report-2017.pdf

[7] Eurocontrol. *Eurocontrol Voluntary ATM Incident Reporting (EVAIR) Bulletin No 19. 2012–2016*. Accessed: Sep. 6, 2018. [Online]. Available: https://eurocontrol.int/sites/default/files/publication/files/evair-bulletin-19.pdf

[8] G. Buesnel. (Apr. 2018). *Expect Your GPS to Be Trashed, GPS & ADS-B Problems at Manila Airport, RNT Foundation*. [Online]. Available: https://rntfnd.org/2018/04/10/expect-yourgps-to-be-trashed-gps-ads-b-problems-at-manila-airport/

[9] RNT Foundation, Ed. (Oct. 2017). *Russian Exercise Jams Aircraft GPS in North Norway for a Week—NRK Translated From Norwegian, RNT Foundation*. [Online]. Available: https://rntfnd.org/2017/10/05/russian-exercise-jams-aircraft-gps-in-northnorway-for-a-week-nrk/

[10] Yle Uutiset. (Nov. 2018). *Russia Suspected of GPS Jamming During Nato Exercises, Yleisradio Oy*, [Online]. Available: https://yle.fi/uutiset/osasto/news/russia_suspected_of_gps_jamming_during_nato_exercises/10500210

[11] M. Hagstroem and A. Lennartsson, *Aircraft Navigation*, Amer. Cancer Soc., Atlanta, GA, USA, 2010.

[12] J. Blanch, T. Walter, and P. Enge, "Satellite navigation for aviation in 2025," *Proc. IEEE* vol. 100, pp. 1821–1830, May 2012.

[13] J. Rife and S. Pullen, *Aviation Applications*. Norwood, MA, USA: Artech House, 2009, ch. 10.

[14] S. Pullen and J. Rife, *Differential GNSS: Accuracy and Integrity*. Norwood, MA, USA: Artech House, 2009, ch. 4.

[15] A. Brown, D. Reynolds, D. Roberts, and S. Serie, "Jammer and interference location system," in *Proc. ION GPS*, 1999, pp. 137–142.

[16] M. Koifman and I. Y. Bar-Itzhack, "Inertial navigation system aided by aircraft dynamics," *IEEE Trans. Control Syst. Technol.*, vol. 7, no. 4, pp. 487–493, Jul. 1999.

[17] RTCA. *Operational Impacts of Intentional GPS Interference. A Report of the Tactical Operations Committee in Response to Tasking From the Federal Aviation Administration*. Accessed: Mar. 2018. [Online]. Available: https://www.rtca.org/sites/default/files/intentional_gps_interference_approved.pdf

[18] C. Williams, "A survey of continuous-wave short-distance navigation and landing aids for aircraft," *J. Inst. Elect. Eng. I Gen.*, vol. 94, no. 82, pp. 491–492, Oct. 1947.

[19] R. G. Hart, "A historical survey of radio and radar aids to aircraft navigation," *J. Brit. Inst. Radio Eng.* vol. 20, no. 6, pp. 409–415, Jun. 1960.

[20] W. B. Hawthorne and L. C. Daugherty, "VOR/DME/TACAN frequency technology," *IEEE Trans. Aerosp. Navig. Electron.* vol. ANE-12, no. 1, pp. 11–15, Mar. 1965.

[21] G. Casserly and D. Richardson, "Operation of current navigation aids and future prospects," *IEEE Trans. Commun.*, vol. COM-21, no. 5, pp. 427–435. May 1973.

[22] D. J. Biezad, "Synthesis and test issues for future aircraft inertial systems integration," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 3, no. 9, pp. 19–23, Sep. 1988.

[23] H. O. Shirer, "The U.S. federal radionavigation plan," in *Proc. IEEE PLANS 92 Position Location Navig. Symp. Rec.*, Mar. 1992, pp. 68–73.

[24] J. Meyer-Hilberg and T. Jacob, "High accuracy navigation and landing system using GPS/IMU system integration," in *Proc. PLANS*, vol. 9, Apr. 1994, pp. 11–17.

[25] Y. Wang, X. Li, and Y. Huang, "Navigation system of pilotless aircraft via GPS," *IEEE Aerosp. Electron. Syst. Mag.* vol. 11, no. 8, pp. 16–20, Aug. 1996.

[26] S. Han, Z. Gong, W. Meng, C. Li, and X. Gu, "Future alternative positioning, navigation, and timing techniques: A survey," *IEEE Wireless Commun.* vol. 23, no. 6, pp. 154–160, Dec. 2016.

[27] R. Kapoor, S. Ramasamy, A. Gardi, and R. Sabatini, "UAV navigation using signals of opportunity in urban environments: A review," *Energy Procedia*, vol. 110, pp. 377–383, Mar. 2017.

[28] H. Wymeersch, G. Seco-Granados, G. Destino, D. Dardari, and F. Tufvesson, "5G mmWave positioning for vehicular networks," *IEEE Wireless Commun.*, vol. 24, no. 6, pp. 80–86, Dec. 2017.

[29] J. A. del Peral-Rosado, G. Seco-Granados, S. Kim, and J. A. Ló, "Network design for accurate vehicle localization," *IEEE Trans. Veh. Technol.*, vol. 68, no. 5, pp. 4316–4327, May 2019.

[30] DeckFinder. *Local Positioning System for Precise and Reliable Navigation*. Accessed: Sep. 2019. [Online]. Available: http://deckfinder.net/webneu/

[31] L. L. Hanzo, L. Yang, E. Kuan, and K. Yen, "CDMA overview," in *Single and Multi-Carrier DS-CDMA: Multi-User Detection, Space- Time Spreading, Synchronisation, Networking, and Standards*. Chichester, U.K.: Wiley, 2004.

[32] E. D. Kaplan and C. J. Hegarty, Eds., *Understanding GPS: Principles and Applications*, 2nd ed. Norwood, MA, USA: Artech House, 2005.

[33] P. Misra and P. Enge, *Global Positioning System: Signals, Measurements, and Performance*, 2nd ed. Lincoln, MA, USA: Ganga-Jamuna Press, 2011.

[34] E. S. Lohan and K. Borre, "Accuracy limits in multi-GNSS," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 52, no. 5, pp. 2477–2494, Oct. 2016.

[35] I. J. Gupta, I. M. Weiss, and A. W. Morrison, "Desired features of adaptive antenna arrays for GNSS receivers," *Proc. IEEE*, vol. 104, no. 6, pp. 1195–1206, Jun. 2016.

[36] S.-H. Kong, "High sensitivity and fast acquisition signal processing techniques for GNSS receivers: From fundamentals to state-of-the-art GNSS acquisition technologies," *IEEE Signal Process. Mag.*, vol. 34, no. 5, pp. 59–71, Sep. 2017.

[37] E. S. Lohan, D. A. de Diego, J. A. Lopez-Salcedo, G. Seco-Granados, P. Boto, and P. Fernandes, "Unambiguous techniques modernized GNSS signals: Surveying the solutions," *IEEE Signal Process. Mag.*, vol. 34, no. 5, pp. 38–52, Sep. 2017.

[38] S. U. Qaisar and C. R. Benson, "Processing cost of Doppler search in GNSS signal acquisition: Measuring Doppler shift in navigation satellite signals," *IEEE Signal Process. Mag.*, vol. 34, no. 5, pp. 53–58, Sep. 2017.

[39] K. Wyatt and M. Gruber, *Radio Frequency Interference Pocket Guide—RFI Characterization, Location Techniques, Tools and Remediation Methods, With Key Equations and Data*, Inst. Eng. Technol., London, U.K., 2015.

[40] F. Dovis, Ed., *GNSS Interference Threats and Countermeasures*. Norwood, MA, USA: Artech House, 2015.

[41] B. R. Elbert, *Radio Frequency Interference in Communications Systems*, (Artech House Space Technology and Applications Series). Norwood, MA, USA: Artech House, 2016.

[42] P. Stavroulakis, *Interference Analysis and Reduction for Wireless Systems*, (Mobile Communications Series). Norwood, MA, USA: Artech House, 2003.

[43] M. Sahmoudi and M. G. Amin, "Fast iterative maximum-likelihood algorithm (FIMLA) for multipath mitigation in the next generation of GNSS receivers," *IEEE Trans. Wireless Commun.*, vol. 7, no. 11, pp. 4362–4374, Nov. 2008.

[44] S. Daneshmand, A. Broumandan, N. Sokhandan, and G. Lachapelle, "GNSS multipath mitigation with a moving antenna array," *IEEE Trans. Aerosp. Electron. Syst.* vol. 49, no. 1, pp. 693–698, Jan. 2013.

[45] J. Seo and T. Walter, "Future dual-frequency GPS navigation system for intelligent air transportation under strong ionospheric scintillation," *IEEE Trans. Intell. Transp. Syst.*, vol. 15, no. 5, pp. 2224–2236, Oct. 2014.

[46] L. Chen *et al.*, "Robustness, security and privacy in location-based services for future IoT: A survey," *IEEE Access*, vol. 5, pp. 8956–8977, 2017.

[47] T. Kraus, R. Bauernfeind, and B. Eissfeller, "Survey of in-car jammers—Analysis and modeling of the RF signals and IF samples (suitable for active signal cancelation)," in *Proc. 24th Int. Tech. Meeting Satellite Div. Inst. Navig. (ION GNSS)*, pp. 430–435, 2017.

[48] D. Borio, F. Dovis, H. Kuusniemi, and L. L. Presti, "Impact and detection of GNSS jammers on consumer grade satellite navigation receivers," *Proc. IEEE*, vol. 104, no. 6, pp. 1233–1245, Jun. 2016.

[49] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 4, pp. 42–56, 4th Quart., 2009.

[50] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, "Denial of service attacks in wireless networks: The case of jammers," *IEEE Commun. Surveys Tuts.* vol. 13, no. 2, pp. 245–257, 2nd Quart., 2011.

[51] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: Attack and defense strategies," *IEEE Netw.*, vol. 20, no. 3, pp. 41–47, May/Jun. 2006.

[52] K. Grover, A. Lim, and Q. Yang, "Jamming and anti-jamming techniques in wireless networks: A survey," *Int. J. Ad Hoc Ubiquitous Comput.*, vol. 17, no. 4, pp. 197–215, Dec. 2014.

[53] X. Wei, Q. Wang, T. Wang, and J. Fan, "Jammer localization in multi-hop wireless network: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 765–799, 2nd Quart., 2017.

[54] C. Shahriar *et al.*, "PHY-layer resiliency in OFDM communications: A tutorial," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 1, pp. 292–314, 1st Quart., 2015.

[55] M. Lichtman, R. P. Jover, M. Labib, R. Rao, V. Marojevic, and J. H. Reed, "LTE/LTE-A jamming, spoofing, and sniffing: Threat assessment and mitigation," vol. 54, no. 4, pp. 54–61, Apr. 2016.

[56] H. Al-Mefleh and O. Al-Kofahi, "Taking advantage of jamming in wireless networks: A survey," *Comput. Netw.*, vol. 99, pp. 99–124, Apr. 2016.

[57] G. X. Gao, M. Sgammini, M. Lu, and N. Kubo, "Protecting GNSS receivers from jamming and interference," *Proc. IEEE*, vol. 104, no. 6, pp. 1327–1338, Jun. 2016.

[58] C. Fernández-Prades, J. Arribas, and P. Closas, "Robust GNSS receivers by array signal processing: Theory and implementation," *Proc. IEEE*, vol. 104, no. 6, pp. 1207–1220, Jun. 2016.

[59] M. G. Amin, X. Wang, Y. D. Zhang, F. Ahmad, and E. Aboutanios, "Sparse arrays and sampling for interference mitigation and DOA estimation in GNSS," *Proc. IEEE*, vol. 104, no. 6, pp. 1302–1317, Jun. 2016.

[60] A. G. Dempster and E. Cetin, "Interference localization for satellite navigation systems," *Proc. IEEE*, vol. 104, no. 6, pp. 1318–1326, Jun. 2016.

[61] "Vulnerability assessment for the transportation infrastructure relying on the global positioning system," John A. Volpe Nat. Transp. Syst. Center, Cambridge, MA, USA, Rep., 2001.

[62] L. Scott, "Anti-spoofing and authenticated signal architectures for civil navigation systems," in *Proc. 16th Int. Techn. Meeting Satellite Div. Inst. Navig. (ION GPS)*, 2003, pp. 1543–1552.

[63] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner, Jr., "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in *Proc. ION GNSS*, 2008, pp. 2314–2325.

[64] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS vulnerability to spoofing threats and a review of antispoofing techniques," *Int. J. Navig. Observation*, vol. 2012, May 2012, Art. no. 127072, doi: 10.1155/2012/127072.

[65] C. Günther, "A survey of spoofing and counter-measures," *J. Inst. Navig.* vol. 61, no. 3, pp. 159–177, 2014.

[66] D. Margaria and M. Pini, *GNSS Interference Threats and Countermeasures* (GNSS Technology and Applications), F. Dovis, Ed. Norwood, MA, USA: Artech House, 2015.

[67] D. Borio and C. Gioia, "A sum-of-squares approach to GNSS spoofing detection," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 52, no. 4, pp. 1756–1768, Aug. 2016.

[68] A. Broumandan, A. Jafarnia-Jahromi, S. Daneshmand, and G. Lachapelle, "Overview of spatial processing approaches for GNSS structural interference detection and mitigation," *Proc. IEEE*, vol. 104, no. 6, pp. 1246–1257, Jun. 2016.

[69] M. L. Psiaki and T. E. Humphreys, "GNSS spoofing and detection," *Proc. IEEE*, vol. 104, no. 6, pp. 1258–1270, Jun. 2016.

[70] R. T. Ioannides, T. Pany, and G. Gibbons, "Known vulnerabilities of global navigation satellite systems, status, and potential mitigation techniques," *Proc. IEEE*, vol. 104, no. 6, pp. 1174–1194, Jun. 2016.

[71] D. Margaria, B. Motella, M. Anghileri, J.-J. Floch, I. Fernandez-Hernandez, and M. Paonni, "Signal structure-based authentication for civil GNSSs: Recent solutions and perspectives," *IEEE Signal Process. Mag.*, vol. 34, no. 5, pp. 27–37, Sep. 2017.

[72] S. Kay, *Fundamentals of Statistical Signal Processing*, vol. 2. Princeton, NJ, USA: Prentice-Hall, 1998.

[73] H. L. Van Trees, K. L. Bell, and Z. Tian, *Detection Estimation and Modulation Theory, Part I: Detection, Estimation, and Filtering Theory*, 2nd ed. Hoboken, NJ, USA: Wiley, 2013.

[74] T. Humphreys, J. Bhatti, D. Shepard, and K. Wesson, "The Texas spoofing test battery: Toward a standard for evaluating GPS signal authentication techniques," in *Proc. 25th Int. Tech. Meeting Satellite Div. Inst. Navig. (ION GNSS)*, 2012, pp. 3569–3583.

[75] M. T. Gamba, D. M. Truong, B. Motella, E. Falletti, and T. H. Ta, "Hypothesis testing methods to detect spoofing attacks: A test against the TEXBAT datasets," *GPS Solutions*, vol. 21, no. 2, pp. 577–589, 2017.

[76] E. Falletti, D. Margaria, G. Marucco, B. Motella, M. Nicola, and M. Pini, "Synchronization of critical infrastructures dependent upon GNSS: Current vulnerabilities and protection provided by new signals," *IEEE Syst. J.*, vol. 13, no. 3, pp. 2118–2129, Sep. 2019.

[77] L. H. Wegner, "On the accuracy analysis of airborne techniques for passively locating electromagnetic emitters," RAND Corporat., Santa Monica, CA, USA, Rep R-722-PR. Accessed: Nov. 28, 2018. [Online]. Available: https://www.rand.org/pubs/reports/R0722.html

[78] F. Amoroso, "Adaptive A/D converter to suppress CW interference in DSPN spread-spectrum communications," *IEEE Trans. Commun.*, vol. COM-31, no. 10, pp. 1117–1123, Oct. 1983.

[79] G. L. Falen, "Analysis and simulation of narowband GPS jamming using digital excision temporal filtering," Ph.D. dissertation, Dept. Air Force, Air Univ., Air Force Inst. Technol., Wright-Patterson AFB, OH, USA, 1995.

[80] R. P. Crow, "Federal radionavigation plan-pie in the sky for civil aviation?" *IEEE Aerosp. Electron. Syst. Mag.*, vol. 13, no. 10, pp. 9–16, Oct. 1998.

[81] R. L. Fante and J. J. Vaccaro, "Wideband cancellation of interference in a GPS receive array," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 36, no. 2, pp. 549–564, Apr. 2000.

[82] K. G. Gromov, "GIDL: Generalized interference detection and localization system," Ph.D. dissertation, Dept. Aeronaut. Astronaut., Stanford Univ., Stanford, CA, USA, 2002.

[83] K. Gromov, D. Akos, S. Pullen, P. Enge, and B. Parkinson, "GIDL: Generalized interference detection and localization system," in *Proc. 13th Int. Tech. Meeting Satellite Div. Inst. Navig. (ION GPS)*, 2000, pp. 447–457.

[84] J. R. Clynch, A. A. Parker, R. W. Adler, W. R. Vincent, P. McGill, and G. Badger. *The Hunt for RFI: Unjamming a Coast Harbor*. Accessed: Sep. 7, 2018. [Online]. Available: http://gpsworld.com/the-hunt-rfi/

[85] J.-L. Issler, L. Ries, J.-M. Bourgeade, L. Lestarquit, and C. Macabiau, "Probabilistic approach of frequency diversity as interference mitigation means," in *Proc. 17th Int. Tech. Meeting Satellite Div. Inst. Navig.*, 2004, pp. 2136–2145.

[86] M. G. Amin and W. Sun, "A novel interference suppression scheme for global navigation satellite systems using antenna array," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 5, pp. 999–1012, May 2005.

[87] S. Pullen and G. Gao, *GNSS Jamming in the Name of Privacy*, Inside GNSS, Mar./Apr. 2012, pp. 34–43.

[88] C. Ouzeau, C. Macabiau, B. Roturier, and M. Mabilleau, "Performance assessment of multi correlators interference detection and repair algorithms for civil aviation," in *Proc. Eur. Navig. Conf.*, 2008.

[89] M. Raimondi, C. Macabiau, and O. Julien, "Frequency domain adaptive filtering against pulsed interference: Performance analysis over Europe," in *Proc. Nat. Tech. Meeting Inst. Navig.*, 2008, pp. 164–176.

[90] M. R. Mosavi, M. Pashaian, M. J. Rezaei, and K. Mohammadi, "Jamming mitigation in global positioning system receivers using wavelet packet coefficients thresholding," *IET Signal Process.*, vol. 9, no. 5, pp. 457–464, Jul. 2015.

[91] A. Steingass, T. Thiasiriphet, and J. Samson, "Modeling distance measurement equipment (DME) signals interfering an airborne GNSS receiver," *Navigation*, vol. 65, no. 2, pp. 221–230, 2018.

[92] J.-C. Juang, "Analysis of global navigation satellite system position deviation under spoofing," *IET Radar Sonar Navig.*, vol. 3, no. 1, pp. 1–7, Feb. 2009.

[93] M. Wildemeersch, A. Rabbachin, E. Cano, and J. Fortuny, "Interference assessment of DVB-T within the GPS L1 and Galileo E1 band," in *Proc. 5th ESA Workshop Satellite Navig. Technol. Eur. Workshop GNSS Signals Signal Process. (NAVITEC)*, 2010, pp. 1–8.

[94] R. H. Mitch *et al.*, "Signal characteristics of civil GPS jammers," in *Proc. 24th Int. Techn. Meeting Satellite Div. Inst. Navig. (ION GNSS)*, 2011, pp. 20–23.

[95] Z. Hu, R. Susitaival, Z. Chen, I. Fu, P. Dayal, and S. K. Baghel, "Interference avoidance for in-device coexistence in 3GPP LTE-advanced: Challenges and solutions," *IEEE Commun. Mag.*, vol. 50, no. 11, pp. 60–67, Nov. 2012.

[96] M. Trinkle, E. Cetin, R. J. R. Thompson, and A. G. Dempster, "Interference localisation within the GNSS environmental monitoring system (GEMS)—Initial field test results," in *Proc. Int. Techn. Meeting Satellite Div. Inst. Navig. (ION GNSS)*, 2012, pp. 2930–2939.

[97] P. Wang, E. Cetin, A. G. Dempster, Y. Wang, and S. Wu, "Time frequency and statistical inference based interference detection technique for GNSS receivers," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 53, no. 6, pp. 2865–2876, Dec. 2017.

[98] D. Fontanella, R. Bauernfeind, and B. Eissfeller, *In-Car GNSS Jammer Localization With a Vehicular Ad-Hoc Network*, Inside GNSS, May/Jun. 2013, pp. 70–80.

[99] S. Han, L. Chen, W. Meng, and C. Li, "Improve the security of GNSS receivers through spoofing mitigation," *IEEE Access*, vol. 5, pp. 21057–21069, 2017.

[100] J. Tu, X. Zhan, X. Zhang, Z. Zhang, and S. Jing, "Low-complexity GNSS anti-spoofing technique based on Doppler frequency difference monitoring," *IET Radar Sonar Navig.*, vol. 12, no. 9, pp. 1058–1065, Sep. 2018.

[101] W. D. Wilde, G. Cuypers, J.-M. Sleewaegen, R. Deurloo, and B. Bougard, "GNSS interference in unmanned aerial systems," in *Proc. 29th Int. Tech. Meeting Satellite Div. Inst. Navig. (ION GNSS+)*, 2016, pp. 1465–1476.

[102] X. Wang, M. Amin, F. Ahmad, and E. Aboutanios, "Interference DOA estimation and suppression for GNSS receivers using fully augmentable arrays," *IET Radar Sonar Navig.*, vol. 11, no. 3, pp. 474–480, Mar. 2017.

[103] L. Canzian *et al.*, *Interference Localization From Space: Theoretical Background*, Inside GNSS, Nov./Dec. 2016, pp. 59–68.

[104] W. F. Young *et al.*, "LTE impacts on GPS: Final test report," Nat. Inst. Stand. Technol., Gaithersburg, MA, USA, Rep. 1952, 2017.

[105] Q. Guo, L. Qi, J. Xiang, and G. Ruan, "Multiple interferences suppression method based on adaptive signal data regrouping for GNSS receivers," *IET Radar Sonar Navig.*, vol. 12, no. 6, pp. 641–648, Jun. 2018.

[106] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner, "Assessing the spoofing threat," in *Proc. 21st Int. Tech. Meeting Satellite Div. Inst. Navig.*, vol. 20, 2019, pp. 28–38.

[107] P. Closas, J. Arribas, and C. Fernandez-Prades, "Spoofing detection by a reduced acquisition process," in *Proc. ION Int. Techn. Meeting*, 2016, pp. 726–731.

[108] F. Bastide, D. Akos, C. Macabiau, and B. Roturier, "Automatic gain control (AGC) as an interference assessment tool," in *Proc. 16th Int. Tech. Meeting Satellite Div. Inst. Navig. (ION GPS/GNSS)*, 2003, pp. 2042–2053.

[109] A. Balaei, B. Motella, and A. G. Dempster, "GPS interference detected in Sydney, Australia," in *Proc. IGNSS Conf.*, 2017, pp. 1–11.

[110] M. Z. H. Bhuiyan, H. Kuusniemi, S. Söderholm, and E. Airos, "The impact of interference on GNSS receiver observables—A running digital sum based simple jammer detector," *Radioengineering*, vol. 23, no. 3, pp. 898–906, 2014.

[111] D. M. Akos, "Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC)," *J. Inst. Navig.*, vol. 59, no. 4, pp. 281–290, 2012.

[112] E. Conte, A. De Maio, and C. Galdi, "Signal detection in compound-Gaussian noise: Neyman–Pearson and CFAR detectors," *IEEE Trans. Signal Process.*, vol. 48, no. 2, pp. 419–428, Feb. 2000.

[113] M. Pini, B. Motella, and M. T. Gamba, "Detection of correlation distortions through application of statistical methods," in *Proc. 26th Int. Tech. Meeting Satellite Div. Inst. Navig. (ION GNSS+)*, 2013, pp. 3279–3289.

[114] R. L. Edgeman, "Assessing the inverse Gaussian distribution assumption," *IEEE Trans. Rel.*, vol. 39, no. 3, pp. 352–355, Aug. 1990.

[115] D. Bradley and J. M. Morris, "On the performance of negentropy approximations as test statistics for detecting sinusoidal RFI in microwave radiometers," *IEEE Trans. Geosci. Remote Sens.*, vol. 51, no. 10, pp. 4945–4951, Oct. 2013.

[116] G. A. P. Cirrone *et al.*, "A goodness-of-fit statistical toolkit," *IEEE Trans. Nucl. Sci.*, vol. 51, no. 5, pp. 2056–2063, Oct. 2004.

[117] N. Fadaei, "Detection, characterization and mitigation of GNSS jamming interference using pre-correlation methods," M.S. thesis, Faculty Grad. Stud., Univ. Calgary, Calgary, AB, Canada, 2016.

[118] J. Lehtomäki, "Analysis of energy based signal detection," Ph.D. dissertation, Dept. Elect. Inf. Eng., Univ. Oulu, Oulu, Finland, 2005.

[119] T. H. Stitz and M. Renfors, "Filter-bank-based narrowband interference detection and suppression in spread spectrum systems," *EURASIP J. Adv. Signal Process.*, vol. 2004, no. 8, pp. 1163–1176, Jul. 2004.

[120] K. D. Wesson, J. N. Gross, T. E. Humphreys, and B. L. Evans, "GNSS signal authentication via power and distortion monitoring," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 54, no. 2, pp. 739–754, Apr. 2018.

[121] W. Li, Z. Jiaqi, L. Yan, and P. Shusheng, "Detection of radiometer radio frequency interference with power-law detector," in *Proc. Int. Appl. Comput. Electromagn. Soc. Symp. (ACES)*, 2017, pp. 1–2.

[122] J. T. Johnson and L. C. Potter, "Performance study of algorithms for detecting pulsed sinusoidal interference in microwave radiometry," *IEEE Trans. Geosci. Remote Sens.*, vol. 47, no. 2, pp. 628–636, Feb. 2009.

[123] F. M. Ahmed, K. A. Elbarbary, and A. R. H. Elbardawiny, "Detection of sinusoidal signals in frequency domain," in *Proc. CIE Int. Conf. Radar*, 2006, pp. 1–5.

[124] F. D. Nunes and F. M. G. Sousa, "GNSS blind interference detection based on fourth-order autocumulants," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 52, no. 5, pp. 25740–25786, Oct. 2016.

[125] A. J. Schoenwald, D. C. Bradley, P. N. Mohammed, J. R. Piepmeier, and M. Wong, "Performance analysis of a hardware implemented complex signal kurtosis radio-frequency interference detector," in *Proc. 14th Spec. Meeting Microw. Radiometry Remote Sens. Environ. (MicroRad)*, 2016, pp. 71–75.

[126] R. D. De Roo, S. Misra, and C. S. Ruf, "Sensitivity of the kurtosis statistic as a detector of pulsed sinusoidal RFI," *IEEE Trans. Geosci. Remote Sens.*, vol. 45, no. 7, pp. 1938–1946, Jul. 2007.

[127] G. J. Saulnier and P. Das, "Antijam spread spectrum receiver using LMS adaptive filtering techniques," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, vol. 3, 1984, pp. 482–487.

[128] D. Borio, C. O'Driscoll, and J. Fortuny, *Fast and Flexible Tracking and Mitigating a Jamming Signal With an Adaptive Notch Filter*, vol. 9, Gibbons Media, 2014, pp. 67–73.

[129] Y.-R. Chien, "Design of GPS anti-jamming systems using adaptive notch filters," *IEEE Syst. J.*, vol. 9, no. 2, pp. 451–460, Jun. 2015.

[130] D. Alonso, "Narrowband interference rejection studies for Galileo signals via simulink," M.S. thesis, Dept. Electron. Commun. Eng., Tampere Univ. Technol., Tampere, Finland, 2015.

[131] J. Querol, R. Onrubia, D. Pascual, H. Park, and A. Camps, "A radio-frequency interference detector for GNSS navigation and GNSS-reflectometry applications," in *Proc. IEEE Int. Geosci. Remote Sens. Symp. (IGARSS)*, 2017, pp. 1266–1269.

[132] J. Magiera and R. Katulski, "Detection and mitigation of GPS spoofing based on antenna array processing," *J. Appl. Res. Technol.*, vol. 13, no. 1, pp. 45–57, Feb. 2015.

[133] S. Thayilchira and S. Krishnan, "Detection of linear chirp and non-linear chirp interferences in a spread spectrum signal by using hough-radon transform," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process.*, vol. 4, 2002, p. 4181.

[134] S. Erkucuk, S. Krishnan, and M. Zeytinoglu, "A robust audio watermark representation based on linear chirps," *IEEE Trans. Multimedia*, vol. 8, no. 5, pp. 925–936, Oct. 2006.

[135] M. Sgammini, F. Antreich, and M. Meurer, "SVD-based RF interference detection and mitigation for GNSS," in *Proc. 27th Int. Tech. Meeting Satellite Div. Inst. Navig.*, 2014, pp. 3475–3483.

[136] S. Fantinato *et al.*, "The spoofing estimating delay lock loop," in *Proc. 7th ESA Workshop Satellite Navig. Technol. (NAVITEC)*, 2014.

[137] G. B. Moon, S.-H. Im, and G.-I. Jee, "A civil GPS anti-spoofing and recovering method using multiple tracking loops and an adaptive filter technique," in *Proc. 26th Int. Tech. Meeting Satellite Div. Inst. Navig. (ION GNSS+)*, 2013, pp. 2916–2920.

[138] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "Detection and mitigation of spoofing attack on a vector based tracking GPS receiver," in *Proc. Int. Tech. Meeting Inst. Navig.*, 2012, pp. 790–800.

[139] Z. Zhang, X. Zhan, S. Feng, and W. Y. Ochieng, "Sensitivity analysis of the vestigial signal defence-based civil GNSS spoofing detection method," *IET Radar Sonar Navig.*, vol. 11, no. 5, pp. 861–872, May 2017.

[140] S. Bartl, P. Berglez, and B. Hofmann-Wellenhof, "GNSS interference detection, classification and localization using software-defined radio," in *Proc. Eur. Navig. Conf. (ENC)*, 2017, pp. 159–169.

[141] R. Calcagno, S. Fazio, S. Savasta, and F. Dovis, "An interference detection algorithm for COTS GNSS receivers," in *Proc. 5th ESA Workshop Satellite Navig. Technol. Eur. Workshop GNSS Signals Signal Process. (NAVITEC)*, 2010, pp. 1–8.

[142] M. Scaramuzza, H. Wipf, M. Troller, H. Leibundgut, S. Rämi, and R. Wittwer, "GNSS RFI detection: Finding the needle in the haystack," in *Proc. 28th Int. Tech. Meeting Satellite Div. Inst. Navig.*, 2015, pp. 1617–1624.

[143] W. Li, Z. Huang, R. Lang, H. Qin, K. Zhou, and Y. Cao, "A real-time interference monitoring technique for GNSS based on a twin support vector machine method," *Sensors*, vol. 16, no. 3, p. 329, 2016.

[144] E. G. Manfredini, D. M. Akos, Y.-H. Chen, S. Lo, T. Walter, and P. Enge, "Effective GPS spoofing detection utilizing metrics from commercial receivers," in *Proc. Int. Tech. Meeting Inst. Navig.*, 2018, pp. 672–689.

[145] E. G. Manfredini, B. Motella, and F. Dovis, "Signal quality monitoring for discrimination between spoofing and environmental effects, based on multidimensional ratio metric tests," in *Proc. 28th Int. Tech. Meeting Satellite Div. Inst. Navig. (ION GNSS+)*, 2015, pp. 3100–3106.

[146] K. D. Wesson, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "An evaluation of the vestigial signal defense for civil GPS anti-spoofing," in *Proc. 24th Int. Tech. Meeting Satellite Div. Inst. Navig. (ION GNSS+)*, 2011, pp. 2646–2656.

[147] M. H. Jin, Y. S. Choi, H. H. Choi, S. J. Lee, and C. Park, "A multiple lock detector for the signal abnormality detection in the GPS receiver," in *Proc. 26th Int. Tech. Meeting Satellite Div. Inst. Navig. (ION GNSS+)*, 2013, pp. 1577–1582.

[148] B. M. Ledvina, W. J. Bencze, B. Galusha, and I. Miller, "An in-line anti-spoofing device for legacy civil GPS receivers," in *Proc. Int. Tech. Meeting Inst. Navig. (ITM)*, 2010, pp. 698–712.

[149] M. T. Gamba, B. Motella, and M. Pini, "Statistical test applied to detect distortions of GNSS signals," in *Proc. Int. Conf. Localization GNSS*, 2013, pp. 1–6.

[150] E. G. Manfredini, F. Dovis, and B. Motella, "Validation of a signal quality monitoring technique over a set of spoofed scenarios," in *Proc. 7th ESA Workshop Satellite Navig. Technol. Eur. Workshop GNSS Signals Signa Process. (NAVITEC)*, pp. 1–7, 2014.

[151] K. Ali, E. G. Manfredini, and F. Dovis, "Vestigial signal defense through signal quality monitoring techniques based on joint use of two metrics," in *Proc. IEEE/ION Position Location Navig. Symp. (PLANS)*, 2014, pp. 1240–1247.

[152] M. Pini, B. Motella, and L. L. Presti, "Comparison between AGC control and statistical based methods for low power interference detection," in *Proc. 29th Int. Tech. Meeting Satellite Div. Inst. Navig. (ION GNSS+)*, 2016, pp. 265–274.

[153] A. Broumandan, A. Jafarnia-Jahromi, V. Dehghanian, J. Nielsen, and G. Lachapelle, "GNSS spoofing detection in handheld receivers based on signal spatial correlation," in *Proc. IEEE/ION Position Location Navig. Symp.*, 2012, pp. 479–487.

[154] J. Nielsen, A. Broumandan, and G. LaChapelle, "GNSS spoofing detection for single antenna handheld receivers," *J. Inst. Navig.*, vol. 58, no. 4, pp. 335–344, 2012.

[155] A. Broumandan, A. Jafarnia-Jaromi, and G. Lachapelle, "Spoofing detection, classification and cancellation (SDCC) receiver architecture for a moving GNSS receiver," *GPS Solutions*, vol. 19, no. 3, pp. 475–487, 2015.

[156] O. Osechas, S. Perea, B. Belabbas, and M. Meurer, "Use of APNT to protect GNSS-based RNP services from international and unintentional RF interference," in *Proc. Int. Tech. Meeting Inst. Navig.*, 2017, pp. 681–692.

[157] A. Broumandan and G. Lachapelle, "Spoofing detection using GNSS/INS/odometer coupling for vehicular navigation," *Sensors*, vol. 18, no. 5, 2018, Art. no. E1305.

[158] S. Khanafseh, N. Roshan, S. Langel, F. Chan, M. Joerger, and B. Pervan, "GPS spoofing detection using RAIM with INS coupling," in *Proc. IEEE/ION Position Location Navig. Symp. (PLANS)*, 2014, pp. 1232–1239.

[159] S. Lo, Y. H. Chen, H. Jain, and P. Enge, "Robust GNSS spoof detection using direction of arrival: Methods and practice," in *Proc. 31st Int. Tech. Meeting Satellite Div. Inst. Navig. (ION GNSS+)*, 2018, pp. 2891–2906.

[160] P. Y. Montgomery, T. E. Humphreys, and B. M. Ledvina, "Autonomous spoofing detection: Experimental results of a multiantenna receiver defense against a portable civil GPS spoofer," in *Proc. Int. Tech. Meeting Inst. Navig. (ITM)*, 2009, pp. 124–130.

[161] M. Meurer, A. Konovaltsev, M. Cunz, and C. Haettich, "Robust joint multi-antenna spoofing detection and attitude estimation using direction assisted multipole hypotheses RAIM," in *Proc. 25th Int. Tech. Meeting Satellite Div. Inst. Navig. (ION GNSS)*, 2012, pp. 3007–3016.

[162] M. L. Psiaki *et al.*, "GNSS spoofing detection using two-antenna differential carrier phase," in *Proc. 27th Int. Tech. Meeting Satellite Div. Inst. Navig. (ION GNSS+)*, 2014, pp. 2776–2800.

[163] J. Dampf *et al.*, *Real World Spoofing Trials and Mitigation via Direction of Arrival Discrimination*, Inside GNSS, May/Jun. 2017, pp. 55–65.

[164] S. Daneshmand, N. Sokhandan, M. Zaeri-Amirani, and G. Lachapelle, "Precise calibration of a GNSS antenna array for adaptive beamforming applications," *Sensors*, vol. 14, no. 6, pp. 9669–9691, 2014.

[165] D. Borio and C. Gioia, "A dual-antenna spoofing detection system using GNSS commercial receivers," in *Proc. 28th Int. Tech. Meeting Satellite Div. Inst. Navig. (ION GNSS+)*, 2015, pp. 325–330.

[166] V. H. Nguyen, G. Falco, E. Falletti, and M. Nicola, "A dual antenna GNSS spoofing detector based on the dispersion of double difference measurements," in *Proc. 9th ESA Workshop Satellite Navig. Technol. Eur. Workshop GNSS Signals Signal Process. (NAVITEC)*, 2018, pp. 1–8.

[167] E. McMilin, "Single antenna null steering for GPS and GNSS aerial applications," Ph.D. dissertation, Stanford Univ., Stanford, CA, USA, Mar. 2016.

[168] Y.-H. Chen, F. Rothmaier, D. Akos, S. Lo, and P. Enge, "Demonstrating single element null steering antenna direction finding for interference detection," in *Proc. Inst. Navig. Int. Tech. Meeting*, 2018, pp. 240–259.

[169] W. De Wilde *et al.*, "Authentication by polarization: A powerful anti-spoofing method," in *Proc. 31st Int. Tech. Meeting Satellite Div. Inst. Navig. (ION GNSS+)*, 2018, pp. 3643–3658.

[170] L. Strizic, D. M. Akos, and S. Lo, "Crowdsourcing GNSS jammer detection and localization," in *Proc. Int. Tech. Meeting Inst. Navig.*, 2018, pp. 626–641.

[171] H. L. Nguyen, M. T. Gamba, E. Falletti, and T. H. Ta, "Situational awareness: Mapping interference sources in real-time using a smartphone app," *Sensors*, vol. 18, no. 12, p. 4130, 2018.

[172] G. Q. Liu, X. Zhang, and Q. B. Lv, "The realization of smoothed pseudo Wigner–Ville distribution based on LabVIEW," in *Measurement Technology and Its Application* (Applied Mechanics and Materials), vol. 239. Zürich, Switzerland: Trans Tech Pub., Jan. 2012, pp. 1493–1496.

[173] Y. S. Shin and J.-J. Jeon, "Pseudo Wigner–Ville time-frequency distribution and its application to machinery condition monitoring," *Shock Vib.*, vol. 1, no. 1, pp. 65–67, 2013.

[174] D. Borio, "Swept GNSS jamming mitigation through pulse blanking," in *Proc. Eur. Navig. Conf. (ENC)*, 2016, pp. 1–8.

[175] L. Musumeci and F. Dovis, "Use of the wavelet transform for interference detection and mitigation in global navigation satellite systems," *Int. J. Navig. Observation*, vol. 2014, Feb. 2014, Art. no. 262186.

[176] A. Broumandan, T. Lin, A. Moghaddam, D. Lu, J. Nielsen, and G. Lachapelle, "Direction of arrival estimation of GNSS signals based on synthetic antenna array," in *Proc. 20th Int. Tech. Meeting Satellite Div. Inst. Navig.*, 2007, pp. 728–738.

[177] M. Sahmoudi and M. G. Amin, "Optimal robust beamforming for interference and multipath mitigation in GNSS arrays," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP)*, vol. 3, 2007, pp. 693–696.

[178] B. Hao, J. Zhu, Z. Li, S. Xiao, and L. Tong, "Passive radar source localization based on PSAAA using single small size aircraft," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, 2015, pp. 1–6.

[179] O. Isoz and D. Akos, "Development of a deployable low cost interference detection and localization system for the GNSS L1/E1 band," in *Proc. 5th ESA Workshop Satellite Navig. Technol. Eur. Workshop GNSS Signals Signal Process. (NAVITEC)*, 2010, pp. 1–4.

[180] J. Poncelet and D. M. Akos, "A low-cost monitoring station for detection amp; localization of interference in GPS L1 band," in *Proc. 6th ESA Workshop Satellite Navig. Technol. (Navitec) Eur. Workshop GNSS Signals Signal Process.*, 2012.

[181] J. A. Bhatti, T. E. Humphreys, and B. M. Ledvina, "Development and demonstration of a TDOA-based GNSS interference signal localization system," in *Proc. IEEE/ION Position Location Navig. Symp. (PLANS)*, 2012, pp. 455–469.

[182] E. Cetin, R. J. R. Thompson, and A. G. Dempster, "Passive interference localization within the GNSS environmental monitoring system (GEMS): TDOA aspects," *GPS Solutions*, vol. 18, no. 4, pp. 483–495, 2014.

[183] H. W. Kang, D. W. Lim, and M. B. Heo, "Design of an enhanced TDOA method for swept CW interferences," *J. Position. Navig. Timing*, vol. 1, no. 1, pp. 23–27, Oct. 2012, doi: 10.11003/JKGS.2012.1.1.023.

[184] "Technical specification group radio access network: Study on channel model for frequencies from 0.5 to 100 GHz, v14.3.0," 3GPP, Sophia Antipolis, France, Rep. TR 38.901. [Online]. Available: http://www.3gpp.org/DynaReport/38-series.htm

[185] "Technical specification group radio access network: Study on enhanced LTE support for aerial vehicles (release 15), v15.0.0," 3GPP, Sophia Antipolis, France, Rep. TR 36.777. Accessed: Jan. 3, 2018. [Online]. Available: http://www.3gpp.org/DynaReport/36-series.htm

[186] R. J. R. Thompson, E. Cetin, and A. G. Dempster, "Unknown source localization using RSS in open areas in the presence of ground reflections," in *Proc. IEEE/ION Position Location Navig. Symp.*, 2012, pp. 1018–1027.

[187] P. C. Chestnut, "Emitter location accuracy using TDOA and differential Doppler," *IEEE Trans. Aerosp. Electron. Syst.*, vol. AES-18, no. 2, pp. 214–218, Mar. 1982.

[188] E. Weinstein, "Measurement of the differential Doppler shift," *IEEE Trans. Acoust., Speech, Signal Process.* vol. ASSP-30, no. 1, pp. 112–117, Feb. 1982.

[189] K. Becker, "An efficient method of passive emitter location," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 28, no. 4, pp. 1091–1104, Oct. 1992.

[190] K. C. Ho and Y. T. Chan, "Geolocation of a known altitude object from TDOA and FDOA measurements," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 33, no. 3, pp. 770–783, Jul. 1997.

[191] K. C. Ho, X. Lu, and L. Kovavisaruch, "Source localization using TDOA and FDOA measurements in the presence of receiver location errors: Analysis and solution," *IEEE Trans. Signal Process.*, vol. 55, no. 2, pp. 684–696, Feb. 2007.

[192] D. Musicki and W. Koch, "Geolocation using TDOA and FDOA measurements," in *Proc. Inf. Fusion*, 2008, pp. 1–8.

[193] D. Musicki, R. Kaune, and W. Koch, "Mobile emitter geolocation and tracking using TDOA and FDOA measurements," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1863–1874, Mar. 2010.

[194] J. A. Garcia-Molina and M. Crisci, "Snapshot localisation of multiple jammers based on receivers of opportunity," in *Proc. 8th ESA Workshop Satellite Navig. Technol. Eur. Workshop GNSS Signals Signal Process. (NAVITEC)*, 2016, pp. 1–6.

[195] A. Konovaltsev, M. Cuntz, C. Haettich, and M. Meurer, "Performance analysis of joint multi-antenna spoofing detection and attitude estimation," in *Proc. Int. Tech. Meeting Inst. Navig.*, 2013, pp. 864–872.

[196] R. Sun, K. O'Keefe, J. Guo, and E. Gill, "Precise and fast GNSS signal direction of arrival estimation," *J. Navig.*, vol. 67, no. 1, pp. 17–35, 2014.

[197] S. Peleg and B. Porat, "Estimation and classification of polynomial-phase signals," *IEEE Trans. Inf. Theory*, vol. 37, no. 2, pp. 422–430, Mar. 1991.

[198] M. Greco, F. Gini, and A. Farina, "Radar detection and classification of jamming signals belonging to a cone class," *IEEE Trans. Signal Process.*, vol. 56, no. 5, pp. 1984–1993, May 2008.

[199] S. Abrahamsson, B. Brusmark, H. C. Strifors, and G. C. Gaunaurd, "Extraction of target signature features in the combined time-frequency domain by means of impulse radar," in *Automatic Object Recognition II*, vol. 1700, F. A. Sadjadi, Ed. Orlando, FL, USA: SPIE, Sep. 1992, pp. 102–113, doi: 10.1117/12.138260.

[200] B. W. Gillespie and L. E. Atlas, "Optimization of time and frequency resolution for radar transmitter identification," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process.*, vol. 3, 1999, pp. 1341–1344.

[201] Y. Xingyu, R. Huailin, and F. Haoran, "A recognition algorithm of deception jamming based on image of time-frequency distribution," in *Proc. 7th IEEE Int. Conf. Electron. Inf. Emerg. Commun.*, 2017, pp. 275–278.

[202] L. Zhang, J. Ren, and T. Li, "Time-varying jamming modeling and classification," *IEEE Trans. Signal Process.*, vol. 60, no. 7, pp. 3902–3907, Jul. 2012.

[203] M. Davy, C. Doncarli, and J.-Y. Tourneret, "Classification of chirp signals using hierarchical Bayesian learning and MCMC methods," *IEEE Trans. Signal Process.*, vol. 50, no. 2, pp. 377–388, Feb. 2002.

[204] N. Nazmi, M. A. A. Rahman, S.-I. Yamamoto, S. A. Ahmad, H. Zamzuri, and S. A. Mazlan, "A review of classification techniques of EMG signals during isotonic and isometric contractions," *Sensors*, vol. 16, no. 8, 2016, Art. no. E1304.

[205] B. Boashash, "Detection, classification, and estimation in the (t, f) domain," in *Time-Frequency Signal Analysis and Processing: A Comprehensive Reference*. London, U.K.: Elsevier, 2016, pp. 693–743.

[206] P. Wang, E. Cetin, A. G. Dempster, Y. Wang, and S. Wu, "Improved characterization of GNSS jammers using short-term time-frequency Rényi entropy," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 54, no. 4, pp. 1918–1930, Aug. 2018.

[207] W. D. Wilde and J.-M. Sleewaegen, "Effective jammer detection and classification using GNSS receivers on a highway overhead structure," in *Proc. 31st Int. Tech. Meeting Satellite Div. Inst. Navig.*, 2018, pp. 1299–1323.

[208] X. Liu, R. Li, C. Zhao, and P. Wang, "Robust signal recognition algorithm based on machine learning in heterogeneous networks," *J. Syst. Eng. Electron.*, vol. 27, no. 2, pp. 333–342, Apr. 2016.

[209] B. Guermah, H. E. Ghazi, T. Sadiki, and H. Guermah, "A robust GNSS LOS/multipath signal classifier based on the fusion of information and machine learning for intelligent transportation systems," in *Proc. IEEE Int. Conf. Technol. Manag. Oper. Decis. (ICTMOD)*, 2018, pp. 94–100.

[210] P. Gao, S. Sun, Z. Zeng, and C. Wang, "GNSS spoofing jamming recognition based on machine learning," in *Signal and Information Processing, Networking and Computers*. Singapore: Springer, 2018, pp. 221–228. [Online]. Available: https://link.springer.com/chapter/10.1007/978-981-10-7521-6_27

[211] A. Broumandan, A. Jafarnia-Jahromi, S. Daneshmand, and G. Lachapelle, "A network-based GNSS structural interference detection, classification and source localization," in *Proc. 28th Int. Tech. Meeting Satellite Div. Inst. Navig.*, 2015, pp. 3358–3369.

[212] J. N. Gross and T. E. Humphreys, "GNSS spoofing, jamming, and multipath interference classification using a maximum-likelihood multi-tap multipath estimator," in *Proc. Int. Tech. Meeting Inst. Navig.*, 2017, pp. 662–670.

[213] M. Heddebaut, V. Deniau, J. Rioult, and C. Gransart, "Mitigation techniques to reduce the vulnerability of railway signaling to radiated intentional EMI emitted from a train," *IEEE Trans. Electromagn. Compat.*, vol. 59, no. 3, pp. 845–852, Jun. 2017.

[214] J. A. Maloney, D.-H. Kwon, R. Janaswamy, and S. D. Keller, "Comparison of radiation pattern modeling methods for GPS controlled reception pattern array," in *Proc. IEEE Int. Symp. Antennas Propag. USNC/URSI Nat. Radio Sci. Meeting*, 2017, pp. 1897–1898.

[215] O. C. Dabak, F. Erdem, T. Sönmez, L. Alatan, and S. S. Koç, "Interference suppression in a GPS receiver with 4 element array design and implementation of beamforming algorithms," in *Proc. IEEE/ION Position Location Navig. Symp. (PLANS)*, 2016, pp. 645–652.

[216] J. Capon, "High-resolution frequency-wavenumber spectrum analysis," *Proc. IEEE*, vol. 57, no. 8, pp. 1408–1418, Aug. 1969.

[217] P. W. Howells, "Intermediate frequency side-lobe canceller," U.S. Patent 32 029 90a, 1959.

[218] S. Applebaum, "Adaptive arrays," *IEEE Trans. Antennas Propag.*, vol. 24, no. 5, pp. 585–598, Sep. 1976.

[219] H. L. Van Trees, *Optimum Array Processing: Part IV of Detection, Estimation, and Modulation Theory*. New York, NY, USA: Wiley, 2002.

[220] H. Krim and M. Viberg, "Two decades of array signal processing research: The parametric approach," *IEEE Signal Process. Mag.*, vol. 13, no. 4, pp. 67–94, Jul. 1996.

[221] B. Farhang-Boroujeny, *Adaptive Filters: Theory and Applications*. New York, NY, USA: Wiley, 2013.

[222] Y.-R. Chien, Y.-C. Huang, D.-N. Yang, and H.-W. Tsao, "A novel continuous wave interference detectable adaptive notch filter for GPS receivers," in *Proc. IEEE Glob. Telecommun. Conf. (GLOBECOM)*, 2010, pp. 1–6.

[223] M. T. Gamba and E. Falletti, "Performance analysis of FLL schemes to track swept jammers in an adaptive notch filter," in *Proc. 9th ESA Workshop Satellite Navig. Technol. Eur. Workshop GNSS Signals Signal Process. (NAVITEC)*, 2018, pp. 1–8.

[224] Y.-R. Chien, C.-H. Chen, P.-Y. Chen, and H.-W. Tsao, "Impact of jamming excisor on the tracking loops for GPS receivers," in *Proc. SICE Annu. Conf. (SICE)*, 2014, pp. 383–388.

[225] Y. Yuan, W.-B. Mei, and Y.-Q. Li, "Chirp-like jammer excision in DSSS communication systems using EMD based radon Wigner distribution," in *Proc. 5th Int. Conf. Wireless Commun. Netw. Mobile Comput.*, pp. 230–234, 2009.

[226] C. Hegarty, A. J. Van Dierendonck, D. Bobyn, M. Tran, and J. Grabowski, "Suppression of pulsed interference through blanking," in *Proc. IAIN World Congr. 56th Annu. Meeting Inst. Navig.*, 2000, pp. 399–408.

[227] E. Anyaegbu, G. Brodin, J. Cooper, E. Aguado, and S. Boussakta, "An integrated pulsed interference mitigation for GNSS receivers," *J. Navig.*, vol. 61, no. 2, pp. 239–255, 2008.

[228] D. Borio and E. Cano, "Optimal global navigation satellite system pulse blanking in the presence of signal quantisation," *IET Signal Process.*, vol. 7, no. 5, pp. 400–410, Jul. 2013.

[229] L. Musumeci, F. Dovis, and J. Samson, "Performance assessment of pulse blanking mitigation in presence of multiple distance measuring equipment/tactical air navigation interference on global navigation satellite systems signals," *IET Radar Sonar Navig.*, vol. 8, no. 6, pp. 647–657, Jul. 2014.

[230] R. J. Erlandson, T. Kim, C. Hegarty, and A. J. V. Dierendonck, "Pulsed RFI effects on aviation operations using GPS L5," in *Proc. Nat. Tech. Meeting Inst. Navig.*, 2004, pp. 1063–1076.

[231] M. J. Rezaei, M. Abedi, and M. R. Mosavi, "New GPS anti-jamming system based on multiple short-time Fourier transform," *IET Radar Sonar Navig.*, vol. 10, no. 4, pp. 807–815, Apr. 2016.

[232] M. G. Amin, D. Borio, Y. D. Zhang, and L. Galleani, "Time-frequency analysis for GNSSs: From interference mitigation to system monitoring," *IEEE Signal Process. Mag.*, vol. 34, no. 5, pp. 85–95, Sep. 2017.

[233] F. Dovis and L. Musumeci, "Use of the Karhunen–Loève transform for interference detection and mitigation in GNSS," *ICT Exp.*, vol. 2, no. 1, pp. 33–36, 2016.

[234] L. Zhao, Y. Mao, and J. Ding, "A STAP interference suppression technology based on subspace projection for Beidou signal," in *Proc. IEEE Int. Conf. Inf. Autom. (ICIA)*, 2016, pp. 534–538.

[235] S. Daneshmand, A. J. Jahromi, A. Broumandan, and G. Lachapelle, "GNSS space-time interference mitigation and attitude determination in the presence of interference signals," *Sensors*, vol. 15, no. 6, pp. 12180–12204, 2015.

[236] D. Borio, H. Li, and P. Closas, "Huber's non-linearity for GNSS interference mitigation," *Sensors*, vol. 18, no. 7, p. 2217, 2018.

[237] D. Borio, "Robust signal processing for GNSS," in *Proc. Eur. Navig. Conf. (ENC)*, 2017, pp. 150–158.

[238] P. J. Huber and E. M. Ronchetti, *Robust Statistics*. Hoboken, NJ, USA: Wiley, 2009.

[239] F. Wang, H. Li, and M. Lu, "GNSS spoofing detection and mitigation based on maximum likelihood estimation," *Sensors*, vol. 17, no. 7, 2017, Art. no. E1532.

[240] P. Closas and A. Gusi-Amigo, "Direct position estimation of GNSS receivers: Analyzing main results, architectures, enhancements, and challenges," *IEEE Signal Process. Mag.*, vol. 34, no. 5, pp. 72–84, Sep. 2017.

[241] F. Faurie and A. Giremus, "Bayesian detection of interference in satellite navigation systems," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP)*, 2011, pp. 4348–4351.

[242] C. E. McDowell, "GPS spoofer and repeater mitigation system using digital spatial nulling," U.S. Patent 725 090 3b1, 2006.

[243] A. Konovaltsev, S. Caizzone, M. Cuntz, and M. Meurer, "Autonomous spoofing detection and mitigation with a miniaturized adaptive antenna array," in *Proc. 27th Int. Tech. Meeting Satellite Div. Inst. Navig. (ION GNSS+)*, 2014, pp. 2853–2861.

[244] N. Vagle, A. Broumandan, and G. Lachapelle, "Analysis of multi-antenna GNSS receiver performance under jamming attacks," *Sensors*, vol. 16, no. 11, 2016, Art. no. E1937.

[245] Y.-E. Chen, Y.-R. Chien, and H.-W. Tsao, "Chirp-like jamming mitigation for GPS receivers using wavelet-packet-transform-assisted adaptive filters," in *Proc. Int. Comput. Symp. (ICS)*, 2016, pp. 458–461.

[246] A. D. Fonzo, M. Leonardi, G. Galati, P. Madonna, and L. Sfarzo, "Software-defined-radio techniques against jammers for in car GNSS navigation," in *Proc. IEEE Metrol. Aerosp. (MetroAeroSpace)*, 2014, pp. 320–325.

[247] D. Borio and P. Closas, "A fresh look at GNSS anti-jamming," *Inside GNSS*, vol. 15, no. 6, pp. 54–61, 2017.

[248] Y. Liu, S. Li, Q. Fu, and Z. Liu, "Impact assessment of GNSS spoofing attacks on INS/GNSS integrated navigation system," *Sensors*, vol. 18, no. 5, p. 1433, 2018.

[249] R. Lang, Z. Su, K. Zhou, and S. Mou, "A robust signal driven method for GNSS signals interference detection," *Chin. J. Electron.*, vol. 27, no. 2, pp. 422–427, Mar. 2018.

[250] A. J. Jahromi, A. Broumandan, and G. Lachapelle, "GNSS signal authenticity verification using carrier phase measurements with multiple receivers," in *Proc. 8th ESA Workshop Satellite Navig. Technol. Eur. Workshop GNSS Signals Signal Process. (NAVITEC)*, 2016, p. 11.

[251] F. A. Milaat and H. Liu, "Decentralized detection of GPS spoofing in vehicular ad hoc networks," *IEEE Commun. Lett.*, vol. 22, no. 6, pp. 1256–1259, Jun. 2018.

[252] L. Zhang, X. Xue, Q. Yang, and L. Wang, "The application of high-order cumulantin GNSS interference bearings measurement," in *Proc. Int. Conf. Inf. Autom.*, 2013, pp. 946–949.

[253] D. Borio, L. L. Presti, and P. Mulassano, "Spectral separation coefficients for digital GNSS receivers," in *Proc. Eur. Signal Process. Conf. (EUSIPCO)*, 2006, pp. 1–5.

[254] F. D. Nunes, R. F. D. Nunes, and F. M. G. Sousa, "Performance evaluation in AltBOC receivers affected by interference," in *Proc. IEEE Int. Conf. Localization GNSS (ICL-GNSS)*, 2016, pp. 1–6.

[255] E. Cardellach, S. Oliveras, and A. Rius, "GNSS signal interference classified by means of a supervised learning method applied in the time-frequency domain," in *Proc. 2nd Int. Congr. Image Signal Process.*, 2009, pp. 1–5.

[256] N. Neji, R. de Lacerda, A. Azoulay, T. Letertre, and O. Outtier, "Survey on the future aeronautical communication system and its development for continental communications," *IEEE Trans. Veh. Technol.*, vol. 62, no. 1, pp. 182–191, Jan. 2013.

[257] M. Strohmeier, M. Schäfer, R. Pinheiro, V. Lenders, and I. Martinovic, "On perception and reality in wireless air traffic communication security," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 6, pp. 1338–1357, Jun. 2017.
[258] S. Poudel and S. Moh, "Medium access control protocols for unmanned aerial vehicle-aided wireless sensor networks: A survey," *IEEE Access*, vol. 7, pp. 65728–65744, 2019.
[259] J. Zhang *et al.*, "Aeronautical *ad hoc* networking for the Internet-above-the-clouds," *Proc. IEEE*, vol. 107, no. 5, pp. 868–911, May 2019.
[260] "GNSS user technology report, version 2," Eur. GNSS Agency, GSA, Washington, DC, USA, Rep. TS-AD-18-001-EN-N, 2018.
[261] G. Berz, *GNSS Spoofing and Aviation: An Evolving Relationship*, Inside GNSS, Sep./Oct. 2018.
[262] "Report on aviation user needs and requirements, version 3.2," Eur. GNSS Agency, GSA, Washington, DC, USA, Rep. GSA-MKD-AV-UREQ-230069, 2018.
[263] I. Fernández-Hernández *et al.*, "Increasing international civil aviation resilience: A proposal for nomenclature, categorization and treatment of new interference threats," in *Proc. Int. Tech. Meeting Inst. Navig.*, 2019, pp. 389–407.
[264] E. S. Lohan, R. M. Ferre, P. Richter, E. Falletti, G. Falco, and A. De La Fuente, "Innovative concept of operation for GNSS navigation on-board of aircraft within the GATEMAN project," in *Proc. Eur. Aeronautics Days (AERODays)*, pp. 111–125, 2019.
[265] G. Falco, M. Nicola, E. Falletti, and M. Pini, "An algorithm for finding the direction of arrival of counterfeit GNSS signals on a civil aircraft," in *Proc. 32nd Int. Meeting Satellite Div. Inst. Navig. (ION GNSS+)*, 2019, pp. 3185–3196.
[266] *Galileo Navigation Message Authentication Specification for Signal-in-Space Testing*, Eur. Commission, Brussels, Belgium, 2016.
[267] *Chips Message Robust Authentication (Chimera) Enhancement for the L1C Signal: Space Segment/User Segment Interface*, document IS-AGT-100, Space Veh. Directorate Adv. GPS Technol., Air Force Res. Lab., Wright-Patterson AFB, OH, USA. Accessed: Sep. 2019. [Online]. Available: http://www.gpsexpert.net/chimera-specification
[268] Y. Zhai, X. Zhan, M. Joerger, and B. Pervan, "Impact quantification of satellite outages on air navigation continuity," *IET Radar Sonar Navig.*, vol. 13, no. 3, pp. 376–383, Mar. 2019.
[269] C. Nava-Gaxiola, C. Barrado, and P. Royo, "Study of a full implementation of free route in the European airspace," in *Proc. IEEE/AIAA 37th Digit. Avion. Syst. Conf. (DASC)*, 2018, pp. 1–7.
[270] M. Koivisto *et al.*, "Joint device positioning and clock synchronization in 5G ultra-dense networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 5, pp. 2866–2881, May 2017.
[271] SkyBrary, *Airborne Separation Assurance Systems (ASAS)*, EUROCONTROL, Brussels, Belgium, 2015. [Online]. Available: https://www.skybrary.aero/index.php/Airborne_Separation_Assurance_Systems_(ASAS)
[272] Skybrary, *4D Trajectory Concept*, EUROCONTROL, Brussels, Belgium. [Online]. Available: https://www.skybrary.aero/index.php/4D_Trajectory_Concept
[273] G. Enea and M. Porretta, "A comparison of 4D-trajectory operations envisioned for NextGen and SESAR, some preliminary findings," in *Proc. 28th Int. Congr. Aeronautical Sci. (ICAS)*, 2015, pp. 1–14.
[274] V. Lucas-Sabola, G. Seco-Granados, J. A. López-Salcedo, J. A. García-Molina, and M. Crisci, "Cloud GNSS receivers: New advanced applications made possible," in *Proc. Int. Conf. Localization GNSS (ICL-GNSS)*, 2016, pp. 1–6.
[275] V. Lucas-Sabola, G. Seco-Granados, J. A. Lopez-Salcedo, J. A. García-Molina, and M. Crisci, "Computational performance of a cloud GNSS receiver using multi-thread parallelization," in *Proc. 8th ESA Workshop Satellite Navig. Technol. Eur. Workshop GNSS Signals Signal Process. (NAVITEC)*, 2016, pp. 1–8.
[276] J. Liu *et al.*, "CO-GPS: Energy efficient GPS sensing with cloud offloading," *IEEE Trans. Mobile Comput.*, vol. 15, no. 6, pp. 1348–1361, Jun. 2016.
[277] L. Romero-Holguin, V. Lucas-Sabola, J. A. del Peral-Rosado, G. Seco-Granados, J. A. Lopez-Salcedo, and J. A. Garcia-Molina, "Prototype of IoT GNSS sensor for cloud GNSS signal processing," in *Proc. 6th Int. Colloquium Sci. Fundam. Aspects GNSS/Galileo*, 2017, pp. 1–6.
[278] S. Zahran, A. Moussa, N. El-Sheimy, and A. Sesay, "Hybrid machine learning VDM for UAVs in GNSS-denied environment," *J. Inst. Navig.*, vol. 65, no. 3, pp. 477–492, 2018.
[279] N. Linty, A. Farasin, A. Favenza, and F. Dovis, "Detection of GNSS ionospheric scintillations based on machine learning decision tree," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 55, no. 1, pp. 303–317, Feb. 2019.
[280] L.-T. Hsu, "GNSS multipath detection using a machine learning approach," in *Proc. IEEE 20th Int. Conf. Intell. Transport. Syst. (ITSC)*, 2017, pp. 1–6.

Ruben Morales-Ferre received the B.Sc. and M.Sc. degrees in telecommunication engineering from the Universitat Autònoma de Barcelona (UAB) in 2016 and 2018, respectively. He is currently pursuing the double Ph.D. degree in information and electrical engineering with Tampere University and UAB. His research interests include GNSS security and integrity, signal processing with applications to communications and navigation, positioning with GNSS and 4G LTE/5G systems, and array signal processing.

Philipp Richter received the Dipl.Ing. degree in electrical engineering from Technische Universität Darmstadt, Germany, in 2008, and the Dr.Eng. degree from the Universidad Autónoma de Querétaro, Mexico, in 2016. From 2009 to 2012, he was a Research Associate with Fraunhofer IIS, Nuremberg, Germany. He is currently a Post-Doctoral Researcher with the Faculty of Information Technology and Communication Sciences, Tampere University, Finland. His current research interests lie in the design and analysis of robust signal processing, Bayesian inference, and machine learning algorithms and their application in positioning within wireless communication networks.

Emanuela Falletti received the M.Sc. and Ph.D. degrees in telecommunications engineering from the Politecnico di Torino, Turin, Italy. She is the Leader of the Systems Analysis and Simulation Research Team, Space and Navigation Technologies Area, LINKS Foundation, a newborn not-for-profit scientific research foundation that has incorporated the former Istituto Superiore Mario Boella, Turin. She has over ten years' experience on software radio and digital signal processing techniques and algorithms for advanced GNSS software receivers, in particular for interference detection and mitigation, multipath mitigation and signal simulation. She has authored of several scientific papers on journals and international conferences, and acts as a peer reviewer for various scientific publications. Her research has covered array signal processing, multiantenna systems, and wireless propagation channel modeling.

Alberto de la Fuente received the master's degree in telecommunications engineering. He was with GMV for over 10 years. During this period, his activity has been focused on GNSS applied to aviation in the CNS domains: navigation (GPS, Galileo, RAIM, EGNOS, and GBAS), surveillance (ADS-B), and communications (ATN/IPS, CPDLC). His technical background includes threats to GNSS: interference (jamming and spoofing) and ionosphere.

Elena Simona Lohan (S'00–M'06–SM'13) received the M.Sc. degree in electrical engineering from the Polytechnics University of Bucharest, Romania, in 1997, the D.E.A. degree in econometrics from École Polytechnique, Paris, France, in 1998, and the Ph.D. degree in telecommunications from the Tampere University of Technology, Finland, in 2003. She is currently an Associate Professor with the Electrical Engineering Unit, Tampere University. She has co-edited 2 books on positioning and has coauthored over 185 international peer-reviewed publications and 6 patents and inventions. She is also the Coordinator of a MSCA European Joint Doctorate Network. Her current research interests include wireless location techniques, GNSS for aviation, wearables, and privacy-aware positioning solutions.