Vulnerabilities, Threats, and Authentication in Satellite-Based Navigation Systems

By MOENESS G. AMIN, *Fellow, IEEE*

PAU CLOSAS, *Senior Member, IEEE*

ALI BROUMANDAN, *Member, IEEE*

JOHN L. VOLAKIS, *Fellow, IEEE*

Ubiquitous use of Global Navigation Satellite Systems (GNSSs) including Global Positioning System (GPS) in civilian, security, and defense applications, and the growing dependence on them within critical infrastructures has highlighted the need for protection against vulnerability due to intentional or unintentional interference sources. GNSS receivers are used in variety of critical infrastructural services, including communications, power grid distribution, finance, emergency services, ground and airborne navigation, active sensing, high precision surveying, and a number of other critical industries. For example, financial institutions rely on GNSS receivers to provide precise timing for high-frequency trading. Wireless networks and cellphone towers use GNSS timing to coordinate signal handshakes and enable connectivity. Bistatic and multistatic radars as well as multiple-input–multiple-output (MIMO) system configurations also rely on GPS for transceiver synchronizations. Of course, accurate signal parameter estimation is crucial for position, navigation, and timing (PNT) for GNSS applications. High level of accuracy is essential for the above operations, implying a necessity to ensure that the GNSS data are immune from interfering sources. Interference mitigation and anti-jam techniques must proceed under the challenging conditions of weak satellite navigation signals with highly negative decibel signal-to-noise-and-interference ratio, and under possible structural similarity of the desired and undesired signals. There are several ways to deliberately compromise positioning, velocity, and timing accuracies. For example, spoofers that mimic GNSS signals can mislead the receivers into false positioning, incorrect timing, and wrong velocity. The challenge to maintain accurate GNSS signals is compounded by the explosion in the number of wireless devices causing nondeliberate interference.

This special issue addresses various jammers and their effect on different processing stages and overall Global Navigation Satellite System (GNSS) receiver performance, and presents countermeasures and solutions to combat interference.

The proliferation of unintentional and intentional interference to GNSS signals has led to a heightened interest in devising effective anti-jamming

Digital Object Identifier: 10.1109/JPROC.2016.2550638

techniques at different levels. The level of protection against interferences is commensurate to anti-jam performance requirements. GNSS interference robustness would clearly increase cost and add to receiver hardware and software complexity.

This special issue addresses the various types of jammers and analyzes their effects on different processing stages and overall GNSS receiver performance. It presents state-of-the-art countermeasures and provides solutions to combat interference and malicious jammers. The 13 overview papers in the issue cover both software processing and hardware components and are written by experts in the field. The primary goal of this issue is to highlight the potential vulnerabilities of GNSSs, delineate effective mitigation approaches, and deliberate on future trends in the field. The papers of this special issue cover the topics of interference classification, detection, and localization; signal authenticity verification; hardware-specific antennas and front-end designs for interference mitigation; and signal and antenna array processing techniques for advanced GNSS receiver designs, including sparse apertures and jammer excision algorithms using time, frequency, or spacial domain as well as joint-variable representations.

ISSUE OVERVIEW

A brief description of the content for each of the 13 overview paper is provided below. These papers were organized in the special issue according to the addressed topics. The issue begins with the introductory paper "Known vulnerabilities of Global Navigation Satellite Systems, status and potential mitigation techniques" by Ioannides *et al.* This paper provides a thorough discussion and classification of GNSS vulnerabilities and their impact on different stages of a GNSS receiver. Two main threats, namely, jamming interferences and spoofing attacks, are analyzed. While the former aims at impeding receiver operation, the goal of the latter is to counterfeit legitimate signals and deceive the receiver yielding erroneous PNT solution. Besides the technical aspects, the paper discusses the political and socioeconomic impact of GNSS vulnerabilities.

The first group of papers in the issue considers the use of antenna array technology to counteract the aforementioned vulnerabilities. This type of solution is of paramount importance in many high-grade applications requiring protection under a wide range of scenarios. The paper "Desired features of adaptive antenna arrays for GNSS receivers" by Gupta *et al.* highlights that future GNSS receiver antenna arrays will be inevitably smaller in size and must provide accuracy and signal integrity in contested environments. The paper presents state-of-the-art array signal processing techniques to meet these requirements for small GNSS antenna arrays. Drawbacks of current GNSS antenna signal processing techniques are discussed and directions for further research are presented. Particular emphasis is given to smaller array sizes employing more sophisticated signal processing techniques to mitigate interference. It is noted that knowledge of the individual antenna array response and interelement coupling is required for reliable GNSS signal reception. The paper "Robust GNSS receivers by array signal processing: Theory and implementation" by Fernàndez-Prades *et al.* is aimed at exploring multiantenna receiver architectures and techniques that are specifically designed considering the particularities of GNSS signals. An updated bibliographical review is given, including the formulae and critical discussions on the various research directions. Particularly, the paper discusses adaptive nullers, adaptive beamformers, and snapshot-based approaches. Notably, the paper provides insights into practical implementation issues of this technology, including simulated and experimental results on a prototype software-defined receiver. The third paper "Small and adaptive antennas and arrays for GNSS applications" by Volakis *et al.* reviews design aspects of antenna arrays for GNSS. The focus is on miniaturized and lightweight adaptive arrays with interference rejection capabilities. Such miniaturization is crucial to enable GNSS in markets where size and weight are key constraints. The paper includes several GNSS antenna array examples of large bandwidth.

The second group of articles discusses jamming types and spoofing attacks, their impact at different stages of a GNSS receiver, and potential countermeasures. "Impact and detection of GNSS jammers on consumer grade satellite navigation receivers" by Borio *et al.* describes different types of GNSS jammers and reviews their impact on commercial receivers. A survey of state-of-the-art methods for jamming detection is also provided. Different detection approaches are investigated which can be implemented at different receiver processing stages. It is shown that jamming can practically impact all receiver stages, from the front-end to the navigation solution. Specific emphasis is given to intermediate power jamming attacks when jamming signals are sufficiently powerful to significantly degrade receiver performance without interrupting receiver operations. The article "Overview of spatial processing approaches for GNSS structural interference detection and mitigation" by Broumandan *et al.* provides an overview of recent research work on GNSS signal authentication utilizing spatial processing methods, categorized into three different groups. The first group considers the antenna array jammer and spoofing mitigation methods, being the most effective countermeasure against interference signals. The second group considers antenna motion to detect spoofing attacks. In this case, the spatial samples are taken over an observation window that can be implemented at

the tracking or navigation level of a receiver. Finally, a cloud-based spoofing countermeasure method applicable to the emerging technologies such as driverless car and autonomous vehicle applications was proposed. This method consists of spatially distributed receivers operating in a nearby region. The benefits and shortcoming of each group are discussed in the paper. Special receiver processing methods can be implemented to provide defenses against spoofing attacks, as discussed in "GNSS spoofing and detection" by Psiaki and Humphreys. The development of appropriate spoofing defenses requires an understanding of the possible attack modes of a spoofer and their properties that can be exploited for defense in detail. The paper discusses several practical defense strategies ranging from signal processing methods to investigate telltale signal anomalies within a traditional GNSS receiver to employing advanced encryption-based techniques that rely on carrier-phase measurements and interferometric methods. The methods are sensitive to differences between signal of arrival directions for spoofed and nonspoofed situations. In "Coding aspects of secure GNSS receivers" by Curran *et al.*, decoding operation of a GNSS receiver under jamming is analyzed. Navigation message signal decoding has been typically overlooked in the literature, mainly due to large coding gains of spreading sequences. However, with the increasing threat of jamming and spoofing, this functionality can be compromised, as shown in this paper. The paper provides an introduction to the various coding schemes employed by current GNSS signals, discussing their performance in the presence of malicious interferences. Additionally, the benefits of soft-decoding schemes for navigation message are highlighted, requiring estimation of the noise plus interference power and yielding enhanced decoding performances under severe jamming conditions. In addition, cryptographic schemes as a means of providing anti-spoofing for geosecurity location-based services and their potential vulnerability are discussed. Finally, "Concepts, development, and validation of multiantenna GNSS receivers for resilient navigation" by Cuntz *et al.* focuses on the development and validation of antenna arrays for robust GNSS navigation. Some examples of radio-frequency interference mitigation and spoofing detection approaches are also provided. Several signal processing techniques are discussed to improve robustness for weak signal conditions, jamming, and counterfeit GNSS signals. Processing for interference mitigation includes prewhitening and postcorrelation enhancements of the satellite signal, along with beamforming and robust positioning using vector tracking for addressing short-term outages due to interference. Experimental results from field tests, carried out at the German Galileo Test and Development Environment (GATE), are provided. As in the Gupta *et al.* paper, the authors conclude that adequate hardware design (from the antenna array to the analog-to-digital conversion components) is necessary to ensure robust interference mitigation.

An important aspect in the context of GNSS anti-jamming is the possibility to locate the jamming sources and take corresponding measures to cease its emission. The special issue contains two articles dealing with localization and direction-of-arrival (DOA) estimation. "Sparse arrays and sampling for interference mitigation and DOA estimation in GNSS" by Amin *et al.* establishes the role of sparse arrays and sparse sampling in anti-jam GNSS. Extended aperture of the receiver sparse arrays is used to angularly localize a number of jammers which exceeds the physical number of GNSS receiver antennas. The finite number of jammers in the field of view and the highly concentrated jammer power in the time-frequency domain motivate the development of a sparsity-based perspective to jammer's DOA and waveform estimation and mitigation. The paper "Interference localization for satellite navigation systems" by Dempster and Cetin provides a survey and analysis of interference localization techniques that include received signal strength, angle of arrival, time difference of arrival, and frequency difference of arrival approaches. The performance of these techniques is considered when applied individually and in combination, both using fixed and mobile platforms. The paper features real systems and architectures of interference geolocalization.

The capabilities of GNSS can be augmented when used in combination to other sensors. The last group of articles in this issue is precisely dealing with such hybridization and complementarity with external sensors. Particularly, in "Protecting GNSS receivers from jamming and interference" by Gao *et al.*, the authors provide an overview of various approaches for protecting GNSS receivers against interference. Namely, external aiding using inertial systems, spatial filtering via antenna array beamforming, signal conditioning and filtering in the time-frequency domain, and vector tracking instead of traditional scalar tracking are discussed. Using inertial aiding and vector tracking, the minimum required signal-to-noise ratio is lowered for reliable signal acquisition and tracking. The authors also discuss how spatial and time-frequency filtering approaches can be used to suppress interfering signals before feeding the receiver. These approaches can be combined for more robust anti-jamming protection of a GNSS receiver. The last paper is "Multisensor navigation systems: A remedy for GNSS vulnerabilities?" by Grejner-Brzezinska *et al.* This paper offers a review of the technological advances that have taken place in space-based PNT over the last two decades. These advances are already available in handheld PDAs, making their hybridization viable for realizing multisensory

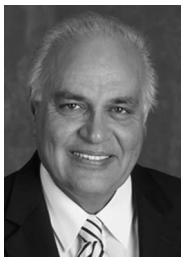
systems. Specifically, the authors review advances in image-based PNT, IMUs, magnetic and RF-based systems, and note that the combination of these approaches along with high processing speeds offer effective alternatives for robust GNSS. The authors conclude that a hybridization of different PNT solutions offer more reliable continuous, accurate, and robust PNT.

SUMMARY AND CONCLUSION

The main goal of this issue is to highlight the importance of GNSS technology in our life and reflect on its ubiquitous use in service infrastructures. Due to its widespread adaptation, compromising GNSS receivers can have direct consequences on operation integrity and service deliverables. GNSS receivers must therefore be protected against interference in all of its kinds. The papers in this issue provide a broad and comprehensive discussion on receiver vulnerabilities, along with pertinent and effective countermeasure solutions to maintain high system performance in presence of malicious jammers. We hope that the reader finds the topics covered in this issue useful, informative, and representative of future trends in this important area of research and development.

We wish to thank all the contributors for their outstanding papers which, individually and in combination, addressed the status of GNSS research and technology. The anonymous reviewers are herein acknowledged for their insightful reviews that increased the quality of this issue. Finally, we are gratefully to Vaishali Damle, the Managing Editor and Jo Sun, the Senior Publication Editor of the PROCEEDINGS OF THE IEEE, who strongly supported the development of this issue. ■

ABOUT THE GUEST EDITORS



Moeness G. Amin (Fellow, IEEE) received the Ph.D. degree from the University of Colorado, Boulder, CO, USA, in 1984.

He joined Villanova University, Villanova, PA, USA, in 1985, where he is now the Director of the Center for Advanced Communications. He has over 700 journal and conference publications in signal processing theory and applications. He coauthored 20 book chapters and is the editor of the three books *Through the Wall Radar Imaging*, *Compressive Sensing for Urban Radar*, and *Radar for Indoor Monitoring* (Boca Raton, FL, USA: CRC Press, 2011, 2014, and 2017, respectively).

Dr. Amin is a Fellow of the International Society of Optical Engineering, the Institute of Engineering and Technology, and the European Association for Signal Processing. He is a Recipient of the 2016 Alexander von Humboldt Research Award, the 2014 IEEE Signal Processing Society Technical Achievement Award, the 2009 Individual Technical Achievement Award from the European Association for Signal Processing, the IEEE Warren D White Award for Excellence in Radar Engineering, the IEEE Third Millennium Medal, the 2010 NATO Scientific Achievement Award, the 2010 Chief of Naval Research Challenge Award, the Villanova University Outstanding Faculty Research Award in 1997, and the IEEE Philadelphia Section Award in 1997. He was a Distinguished Lecturer of the IEEE Signal Processing Society (2003–2004), and is currently the Chair of the Electrical Cluster of the Franklin Institute Committee on Science and the Arts.

Pau Closas (Senior Member, IEEE) received the M.Sc. and Ph.D. degrees in electrical engineering and the M.Sc. degree in advanced mathematics and mathematical engineering from the Universitat Politécnica de Catalunya (UPC), Barcelona, Spain, in 2003, 2009, and 2014, respectively.

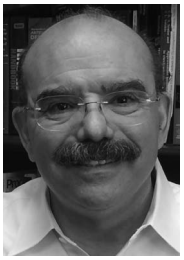
In 2003, he joined the Department of Signal Theory and Communications, UPC, as a Research Assistant and during 2008 he was a Research Visitor at the Stony Brook University (SBU), Stony Brook, NY, USA. In September 2009, he joined the Centre Tecnològic de Telecomunicacions de Catalunya (CTTC), Barcelona, Spain, where he currently holds a position as a Senior Researcher and Head of the Statistical Inference for Communications and Positioning Department. He has many years of experience in projects funded by the European Commission, Spanish and Catalan Governments, as well as the European Space Agency in both technical and managerial duties. His primary areas of interest include statistical and array signal processing, estimation and detection theory, Bayesian filtering, robustness analysis, and game theory, with applications to positioning systems, wireless communications, and mathematical biology.

Dr. Closas is a Senior Member of ION and EURASIP. He was involved in the organizing committees of EUSIPCO'11, IEEE IMWS'11, IEEE RFID-TA'11, European Wireless'14, IEEE SSP'16, and IEEE ICASSP'20 conferences. He is the recipient of the EURASIP Best PhD Thesis Award 2014 and the 9th Duran Farell Award for Technology Research, both in recognition to his contributions to the field of signal processing for GNSS.

Ali Broumandan (Member, IEEE) received the B.Sc. and M.Sc. degrees from the Electrical Engineering Department and the Ph.D. degree from the Geomatics Engineering Department.

From 2009 to 2012, has was a Senior Research Associate in Position, Location And Navigation (PLAN) group of the University of Calgary, Calgary, AB, Canada, where his research focused on signal processing aspects of GNSS receiver. From May 2012 to October 2013, he was involved in GNSS industry as a Senior GNSS Specialist where his work focused on different signal processing aspects of high-precision GNSS receivers. Since November 2013, he has been with the PLAN group, University of Calgary, as a Senior Research Associate, where his research focuses on GNSS interference mitigation utilizing antenna array processing. He has been involved in several industrial research projects focusing on spatial/temporal characterization of GNSS channels in dense multipath environments and synthetic antenna array processing.

Dr. Broumandan won the Parkinson award for graduate student excellence in Global Navigation Satellite Systems in his thesis in 2010.



John L. Volakis (Fellow, IEEE) was born in Chios, Greece, in 1956, and immigrated to the United States in 1973. He received the B.E. degree (*summa cum laude*) from Youngstown State University, Youngstown, OH, USA, in 1978 and the M.Sc. and Ph.D. degrees from The Ohio State University, Columbus, OH, USA, in 1979 and 1982, respectively, all in electrical engineering.

He started his career with Rockwell International, now Boeing, in Columbus, OH, USA, and Lakewood, CA, USA, from 1982 to 1984. In 1984, he was appointed Assistant Professor with The University of Michigan, Ann Arbor, MI, USA, becoming a Full Professor in 1994. He also served as the Director of the Radiation Laboratory from 1998 to 2000. Since January 2003, he has been the Roy and Lois Chope Chair Professor of Engineering with The Ohio State University and also serves as the Director of the ElectroScience Laboratory. His publications include eight books, 375 journal papers, nearly 700 conference papers, 25 book chapters, and 14 patents/patent disclosures. Among his coauthored books are *Approximate Boundary Conditions in Electromagnetics* (London, U.K.: IET, 1995), *Finite Element Methods for Electromagnetics* (New York, NY, USA: IEEE Press, 1998), *Antenna Engineering Handbook* (New York, NY, USA: McGraw-Hill, 2007, 4th ed.), *Small Antennas* (New York, NY, USA: McGraw-Hill, 2010), and *Integral Equation Methods for Electromagnetics* (London, U.K.: SciTech, 2011). He has graduated/mentored over 80 doctoral students/postdoctoral researchers, with 32 of them receiving best paper awards at conferences. Over the years, he carried out research in antennas, wireless communications and propagation, computational methods, electromagnetic compatibility and interference, design optimization, RF materials, multiphysics engineering, millimeter waves, terahertz, and medical sensing.

Prof. Volakis is a Fellow of ACES. His service to professional societies includes the following: 2004 President of the IEEE Antennas and Propagation Society, Chair of USNC/URSI Commission B (2015–2017), twice the general Chair of the IEEE Antennas and Propagation Symposium, IEEE APS Distinguished Lecturer, IEEE APS Fellows Committee Chair, IEEE-wide Fellows committee member, and an Associate Editor of several journals. He was listed by ISI among the top 250 most referenced authors in 2004. Among his awards are the following: The University of Michigan College of Engineering Research Excellence Award in 1993, the Scott Award from The Ohio State University College of Engineering for Outstanding Academic Achievement in 2011, the IEEE AP Society C.-T. Tai Teaching Excellence Award in 2011, the IEEE Henning Mentoring Award in 2013, the IEEE Antennas and Propagation Distinguished Achievement Award in 2014, and The Ohio State Univ. Distinguished Scholar Award in 2016.