

# Preface

## I

Global Navigation Satellite System (GNSS) generally refers to various global satellite navigation systems, and their augmentation systems. It can provide accurate position, velocity and time (PVT) for any person or object at any place and at any time. GNSS, as an important space information infrastructure, reflects a country's comprehensive national strength. Major countries and organizations all around the world have been vigorously developing satellite navigation systems with various characteristics, such as the Global Positioning System (GPS) of the USA, the GLObal NAVigation Satellite System (GLONASS) of Russia, the Galileo System of Europe (Galileo), the BeiDou Satellite System of China (BeiDou), the Indian Regional Navigational Satellite System (IRNSS) of India, and the Quasi-Zenith Satellite System (QZSS) of Japan. Since 1996, the United States has initiated the "GPS modernization" project. In recent years, we have seen the most extensive GPS satellite launching schedule since 1993, and the first GPS III is scheduled to be launched in 2018. China proposed a "three-step" development plan for the Beidou system. In 2012, the Asia-Pacific Regional Navigation Satellite System was constructed and put into use (making China the third country in the world to put a GNSS system into operation); and since then, China has been making steady progress toward establishing a global system by launching the first global GNSS satellite in July 2017. In the future, all these systems will be integrated into a Global Navigation Satellite System of Systems, to provide more reliable and accurate services for global users.

GNSS applications are almost ubiquitous, and can be applied in almost any imaginable situation, including air, sea, and ground transportation and management, smart grid, telecommunications systems, mobile phone positioning, smart carrier tools, exploration and mapping, criminal tracking, emergency rescue, disease control, fishing operations, oil exploration, precision agriculture, as well as military applications such as precise weapon guidance and targeting. GNSS are embedded in all the above applications as a stealthy technology running in the background. It can also provide support for many critical infrastructures tightly connected to the

operations of a nation and the livelihood of its people, e.g., smart grids (timing service), bank operations (timing service), transportation systems (location and timing services), and communication systems (location and timing services).

GNSS is vulnerable because it is so valuable! Since GNSS satellites are usually positioned 20,000–30,000 kilometers above the earth, their signals are very weak (it can be compared to observing a 50W light bulb from approximately 20,000 kilometers away), and they are usually more than 20 dB below the noise level, meaning that they are very vulnerable to a variety of malicious and unintentional interferences. Unintentional interferences include ionospheric scintillation, solar radio pulse interference, multipath interference, Radio Frequency Interference (RFI), and pulse interference generated by DME (Distance Measuring Equipment) and TACAN (Tactical Air Navigation System) equipment working in the aeronautical radio protection band. Malicious interferences include jamming and spoofing. Jamming can make the receiver out of lock, but the monitoring and suppression of jamming are easier and more established methods are available, as many related techniques can be borrowed from the radar field. Spoofing takes advantage of the open transparency and predictability of GNSS civil signals, and it can create interference signals very similar to authentic GNSS signals. Consequently, spoofing has superior concealment and can result in greater repercussions. Spoofing can generate timing and positioning errors, or even take control of the target receiver, without the user even being aware of its presence. Due to the existence of these interference sources, GNSS cannot provide safe and reliable services.

The robustness and safety of GNSS have led to great concerns around the world for the past dozen years. Below are comments made by some renowned political characters, GNSS experts, and related organizations in the US:

(1) Former U.S. President Barack Obama (February 2013)

“Critical infrastructure must be secure and able to withstand and rapidly recover from all hazards.”

“The nation’s critical infrastructure provides the essential services that underpin American society. Proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure—including assets, networks, and systems....”

(2) Former US President George W. Bush (December 2004)

“...the Global Positioning System has grown into a global utility...integral to the U.S. national security, economic growth, transportation safety, and homeland security, and are an essential element of the worldwide economic infrastructure....”

“The Secretary of Transportation shall...develop, operate, and maintain backup position, navigation, and timing capabilities that can support critical transportation, homeland security, and other critical civil and commercial infrastructure ...in the event of a disruption of the Global Positioning System or the other space-based positioning, navigation, and timing services.”

- (3) US National Positioning, Navigation, and Timing (PNT) Advisory Committee (November 2010)

“The United States is now critically dependent on GPS...cell phone towers, power grid synchronization, new aircraft landing systems, and the future FAA Air Traffic Control System cannot function without it...increasing incidents of deliberate or inadvertent interference that render GPS inoperable for critical infrastructure operations.”

“We strongly recommend that the previously announced decision (to deploy eLoran as the primary Alternate PNT) should be reconfirmed and quickly implemented.”

- (4) The “Father of GPS,” Prof. Brad Parkinson at Stanford University (2013)

“Reliance on satellite navigation and timing systems has become a single point of failure for much of America and is our largest, unaddressed critical infrastructure problem.”

“Positioning, Navigation and Time (PNT) service has become a worldwide utility-thanks to GPS. In fact, PNT service is now worth billions of dollars a year, yet taken for granted. On the other hand this service is potentially threatened by jamming and related threats. I subscribe to PTA-Protect, Toughen and Augment this valuable asset. Particularly appealing is the use of eLoran to Augment or as a standalone service. In this role, eLoran would be a powerful deterrent to malicious interference.”

- (5) Renowned GNSS interference mitigation expert, Prof. Todd Humphreys at University of Texas at Austin (2013)

“The next few decades will see pervasive autonomous control systems become critical to the world economy-from autonomous cars and aircraft to smart homes, smart cities, and vast energy, communication, and financial networks controlled at multiple scales. Protecting these systems from malicious navigation and timing attacks is a matter of urgent societal interest.”

“The greatest upcoming challenge in PNT security will be providing proof of location or time to a skeptical second party.”

In the present day, there are many types of jamming equipment in the market, including the Personal Privacy Device (PPD), which can be purchased cheaply online. In November 2011, in an event that shocked the whole world, an Unmanned Aerial Vehicle (UAV) owned by the US Central Intelligence Agency (CIA) was captured by Iran with only minor damage to the landing gear, which was estimated to be caused by the landing. Until today, the exact reason has not been released. Engineers from the Iranian side claimed that they had interfered with the communication link between US UAV operators and the UAV, causing the UAV to switch to an autopilot mode. Then the UAV was guided to a base in Afghanistan relying solely on the GPS equipment on the UAV. When the UAV was in this working mode, Iranian engineers claimed that they had tricked the UAV to fly to Iran using spoofing. Some US experts questioned the claims made by Iranian

engineers because the CIA UAV usually uses a military code, so it should have been very difficult to use spoofing against it. Instead, the experts envisaged the following scenario: The Iranians used jamming and spoofing simultaneously to interfere with GPS military and civil signals respectively, and the UAV was set in a mode in which the civil signals were used when the military signals were jammed. Regardless of which explanation is correct, the evidences imply that the UAV was experiencing malicious interferences of jamming and spoofing simultaneously.

In 2001, the US Department of Transportation evaluated the impacts on transportation facilities by vulnerabilities of GPS, and expressed concerns on the threats posed by spoofing. In 2008, researchers created low-cost spoofing devices that could be made based on software radio technology and components from general stores, and showed that spoofing signals can be successfully generated using this low-cost approach. In June 2012, Prof. Todd E. Humphreys, the head of radio navigation lab of the University of Texas at Austin, was invited by the US Department of Homeland Security to perform two public test studies in order to evaluate the impacts of spoofing and jamming on civil UAVs (which will be merged into the national airspace system) and smart grid. The results showed that these systems were easily affected by spoofing. In July 2013, in an actual field demo, the same lab successfully tricked a ship into deviating from its original route using spoofing.

The above events show that the robustness and safety of GNSS face very big challenges. The Science and Technology Directorate (S&T) is a branch within the United States Department of Homeland Security. Part of the S&T's mission is to evaluate the impacts of jamming and spoofing, study interference mitigation measures, and provide better practical means to protect critical infrastructures. In June 2014, former US Defense secretary Ashton Carter expressed concerns about the lack of robust PNT. One of the senior US officers even proclaimed that "GPS is much too vulnerable, we must replace it with new inertials and chip scale atomic clocks." It is reported that the US has been evaluating various possibilities on alternative PNT schemes that can complement GPS. The goal is to improve GPS robustness and safety through integration.

Interference monitoring and suppression for GNSS have drawn great attentions around the world. In 2011, the International Committee on GNSS promoted the establishment of a special workshop on Interference Detection and Mitigation (IDM). In 2012, the first workshop session was held at the Vienna International Convention Center in Austria with the main topics being compatible interoperability among different GNSS systems, and interference monitoring and suppression. The workshop has been held for five consecutive sessions. In addition, at the GNSS academic annual meeting hosted by ION (Institute of Navigation), IDM has always been a hot topic and focus for discussion.

## II

I studied in the Northwestern Polytechnic University's first accelerated Bachelor's/Master's pilot program from 1985 to 1991. When I was studying for my master's degree, I participated in research works on super-resolution array signal

processing. From 1991 to 1994, I worked on my Ph.D. degree in the field of radar signal processing at Xidian University. During this period, I participated in the research on Airborne Early Warning Radar Space-Time Adaptive Processing (STAP) led by Prof. Zheng Bao, who is the academician of the Chinese Academy of Sciences. This was the earliest group to start systematic STAP research in China. Since then, this research group has achieved advanced research results on par with the findings of other leading international scholars in the field. For example, Dr. Richard Klemm, the author of the first STAP monograph, stated the following in the foreword section of his book “There are activities all over the world, especially in the USA and China.” Between 1997 and 2002, as a postdoctoral fellow and a visiting professor, I worked in the Spectrum Analysis Lab at the University of Florida, USA. During that period, I collaborated with Prof. Jian Li, who is an IEEE fellow and a winner of the American Presidential Young Investigator (PYI) award, in studying spectral estimation based on decoupled parameter estimation theory and robust Capon beamforming. In 2004, I participated in research on anti-jamming technology for the Galileo system in the Imperial College of London as part of the China’s first group of distinguished research scholars. In summary, my research interests have always been focused on sensor array signal processing (super-resolution direction of arrival estimation, adaptive beamforming, and space-time adaptive processing), modern spectrum analyses and their applications.

In the summer 2002, I was invited to be a visiting professor at the Spectrum Analysis Lab at the University of Florida. My main research focus there was to study robust Capon beamforming and its applications. During that tenure, I read the introduction on GNSS robust beamforming written by Professir Sayed’s research group at Stanford University. Another paper brought to my attention was titled “Wideband cancellation of interference in a GPS receiver array,” written by Dr. Ronald L. Fante from the MITRE corporation and published in IEEE Transactions on Aerospace and Electronic Systems, in which the author expanded the STAP technology used for airborne early warning radar to GNSS applications, and used the technology to suppress wideband interference and dispersive multipath interference. Similarly to me, Dr. Fante was originally engaged in airborne radar signal processing works. These two papers have cultivated my strong interest in GNSS interference mitigation technology.

### III

This book is the first most comprehensive monograph on the subject of GNSS adaptive interference mitigation. The book covers the topics of jamming (including high dynamic jamming), spoofing, multipath interference, and pulse interference suppressions. We have mainly studied the above methods based on array signal processing, including spatial domain, and spatial-temporal domain adaptive filtering. These methods take full advantage of the characteristics of GNSS signals, e.g., small power, periodic repetition, and known spread spectrum code. Only autonomous systems are considered, i.e., no other sensors are used (e.g., inertia navigation) to provide supplementary information. The focus of this book is on the robust adaptive filtering method that is not sensitive to array calibration errors.

Direction of Arrival (DOA) estimation and multipath time delay estimation can both take advantage of the methods based on decoupled parameter estimation theory. By using this approach, an estimation problem of multiple overlapping signal parameters can be converted into a series of estimation problems on a single signal parameter using a cyclic optimization algorithm with a special structure (the key is to assure the accuracy and computation efficiency of these single signal parameter estimations). This approach has the benefits of simple and effective computation, good convergence, and robustness to model errors.

#### IV

The research works and achievements listed in the book have been sponsored by the Chinese National Outstanding Youth Fund (60325102) and National Natural Science Foundation of China (61179064, 61172112, 61471363, 61271404). And thanks to the sustained support of the National Natural Science Foundation of China, these research works have lasted 12 years.

First of all my grateful thanks go to my Ph.D. advisor, Academician Zheng Bao at Xidian University. I have benefited throughout my whole life from my research experiences on STAP under his guidance. His attitudes and methods toward academic research have made profound impacts on my life and career. My thanks also go to Prof. Jian Li at the University of Florida USA. During my three working tenures in her lab, we have co-authored and published more than 20 articles in IEEE and IET/IEE journals, which have greatly improved my academic prowess. These papers were mainly focused on using the decoupled parameter estimation theory and method in various applications. Many of the achievements of this book would not have been possible without the guidance from my two mentors. My appreciations are also extended to my lab mates in the former STAP group at Xidian University (Dr. Yuhong Zhang, Dr. Guisheng Liao, Dr. Yongliang Wang, Dr. Lingrang Zhang, and Dr. Xiaochu Chen). Together we have enjoyed memorable school years. I am also grateful to my other co-authors at the Key Lab for Advanced Signal Processing at China Civil Aviation University, as well as Associate Professor Tieqiao Hu, Dr. Lunlong Zhong, and many other Ph.D. and master students involved in related research works.

Parts of the formal texts of this book were tentatively finished on September 11, 2015. From September 14 to September 18, at the ION GNSS+ 2015 meeting held in Tampa, Florida, USA, I led two co-authors of this book in efforts to further improve our draft by communicating face to face with our colleagues from all around the world. I fondly remember how I became interested in GNSS interference mitigation 12 years ago in Florida. Now, after attending this meeting in the beautiful city of Tampa, I feel extremely grateful and delighted to have come back with this book to where this journey started. This foreword was composed all at once on my return flight from Tampa to Beijing in a single session.

On the return flight from Tampa, Florida  
September 2016

Renbiao Wu

Adaptive Interference Mitigation in GNSS

Wu, R.; Wang, W.; Lu, D.; Wang, L.; Jia, Q.

2018, XIX, 274 p. 136 illus., Hardcover

ISBN: 978-981-10-5570-6