GNSS vulnerabilities: simulation, verification, and mitigation platform design

Xin ZHAO, Xingqun ZHAN* and Kai YAN

School of Aeronautics and Astronautics, Shanghai Jiao Tong University, Shanghai 200240, China

(Received 16 November 2012; final version received 11 May 2013)

This paper introduces the design and construction of global navigation satellite systems (GNSS) vulnerability simulation, verification, and mitigation platform. The platform contains five modules: simulation of the signal-in-space environment, simulation of the vulnerabilities in the space segment, signal quality monitoring and data processing, vulnerability assessment and validation, and integrated control. It provides a set of integrated simulations of different types of interference in the GNSS signal propagation domain, including electromagnetic interference, atmospheric disturbances, multipath, and interference in the inter-satellite link. This paper focuses on the design of the main system modules and testing through an experimental analysis. The results demonstrate both the effectiveness and realism of the modules and overall platform.

Keywords: GNSS vulnerability; spoofing; jamming; ionosphere delay; multipath effect

1. Introduction

Robustness of global navigation satellite systems (GNSS) to vulnerability is the ability to maintain normal operation and to provide users with normal service quality under different types of interference. Vulnerability arises from different sources including satellite malfunction, communication interference in the inter-satellite link and in the satellite-ground links, atmospheric anomalies (ionosphere/troposphere), electromagnetic interference, as well as multipath effects and receiver failures.

GNSS is widely used for many applications including military operations and financial services, and end-users around the world are increasingly dependent on the positioning, navigation and timing services provided by GNSS. However, there are many factors that affect GNSS service quality including intentional and unintentional interference, as well as natural interference (1). These types of interference could result in severe damage to many systems and networks including energy, telecommunication, transport, and financial.

Based on the factors that influence GNSS signal interference, this paper designs and constructs a platform for the simulation, verification, and mitigation of GNSS vulnerabilities. The platform enables the analysis and comparison of various GNSS vulnerabilities, and the development and validation of effective detection and mitigation techniques. Finally, this paper proposes fundamental methods to address GNSS vulnerabilities and identifies future research directions.

2. Platform design

The design of a GNSS vulnerability simulation, verification, and mitigation platform must consider all potential interference factors, as well as the methods and techniques for signal assessment and validation. GNSS vulnerability factors are associated with the space segment, atmosphere and the user segment (2). The platform generates radio frequency signals for GPS L1/L2/L5 and GALILEO E6.

Combined with the interference factors, GPS and GALILEO navigation signals could be used to realize the function of the simulation of signal propagation in complex environments. The platform has the ability to process both simulated and real signals to enable comparison and verification of the simulated signals. Furthermore, the platform determines signal quality through the implementation of a signal quality monitoring and data processing module. The vulnerabilities of the space segment are simulated with a dedicated module; the simulation outputs are then evaluated and compared with reference signals, thereby validating the individual modules. The simulation results are then displayed on the integrated control platform (Figure 1).

2.1. Signal-in-space environment simulation

Complex GNSS signals need to be simulated including effects such as ionospheric scintillation/disturbance (3), abnormal tropospheric delays, multipath effects, electromagnetic interference, and sun-earth geographical events, such as solar flares, spot outbreaks, and geomagnetic storms which cause satellite failures and signal interruptions and which decrease signal-to-noise ratios (4) resulting in degraded accuracies or even system outages.

Among these vulnerabilities, the most significant influence is from ionospheric disturbances, multipath, and electromagnetic interference, which can mainly be divided into jamming and spoofing interference.
The signal-in-space environment simulation module includes two GNSS simulators, two spoofing interference devices, four jamming interference devices, multipath effect software, a multi-GNSS reference station antenna tracking system, and a radio frequency signal switching and combination module.

The output signals of this module are as follows:

**Real signal:** is generated by the space segment vulnerability simulation module, tracked by the GNSS satellites parabolic servo tracking antenna. Its main purpose is to track and observe satellite signals, analyze, and record signal anomalies and potential interference effects.

**Real signal 2:** following reception of the real signal with the multi-GNSS reference station antenna, the

---

**Figure 1.** Platform structure diagram.

**Figure 2.** Spectrum of single-frequency interference produced by the jamming device.

**Figure 3.** Normalized discriminator outputs for varying code delays.

**Figure 4.** Normalized discriminator outputs for varying reflection coefficients.
received signal is used as an input to the multimode multiple frequency receivers for quality monitoring.

**Simulated signal 1:** GNSS signals are generated by two sets of navigation simulators. Simulator A is used to generate GPS L1/BeiDou B1, Galileo E1, and GLONASS G1, and simulator B for GPS L2/BeiDou B2, B3, and the interference signal.

**Simulation signal 2:** simulation of the BeiDou nominal B1 signal followed by B1 signal spoofing.

**Simulated signal 3:** simulation of jamming interference on the bands of L1/L2/L5/E5.

**Simulated signal 4:** simulation of multipath on several channels.

With single-frequency interference for example, it produces a single frequency signal at 1565 MHz by using a jamming device and the signal was analyzed by the AgilentMXA N9020 high performance spectrum analyzer.

![Data Quality Monitoring Center](image)

**Figure 5.** Flow diagram of the signal monitoring and processing module.

![Ionosphere Delay Using Grid Points](image)

**Figure 6.** Display of ionosphere delay using grid points.
In Figure 2, the signal frequency of the single-frequency interference is 1575.42 MHz and its power was about $-20.58 \text{ dBm}$, which was sufficient to affect the nominal reception of GPS L1 signals.

In Figures 3 and 4, the code phase error and carrier phase error were induced by the multipath signals (5) and the spectrum diagram of the single-frequency interference signal produced by the GPS L1 jamming device is shown in Figure 2.

2.2. Signal quality monitoring and data processing module

The signal quality monitoring and data processing module consists of a network of multi-mode and multi-frequency software receivers, high-precision GPS receivers, quad-mode reference station receivers, a high-performance spectrum analyzer, an oscilloscope, a signal analyzer, a GNSS satellite dish antenna servo tracking system, a universal software radio peripheral, and the data quality monitoring platform, as well as the processing software.

With this module, real and simulated signals are captured and monitored. The observations are stored and signal qualities are monitored for availability, continuity, ranging accuracy, and integrity.

Multi-mode multi-frequency software receivers are used to analyze and detect jamming and spoofing interference, as well as multipath, and the different types of interference are mitigated or eliminated by the corresponding anti-interference methods.

The simulation module of ionospheric delays is used to assess the impact of, and remove the ionospheric delays. Figure 6 illustrates the simulation of ionospheric interference in Guangdong and Haikou (4). The left figure corresponds to the distribution of equivalent ranging errors when the grid VTEC is added onto the L1 signal. The right figure displays the pierce points at the current epoch and the distribution of the monitoring stations (Figure 5).

2.3. Space segment vulnerability module

The GNSS space segment consists of a constellation of navigation satellites with the corresponding inter-satellite links (ISL) (6). This module is used to study the vulnerability of the constellation including of the ISL. Satellite-based failures include message data errors, clock acceleration errors, and pseudo-code signal. The space segment vulnerability simulation module and the results of the satellite autonomous integrity monitoring (SAIM) are shown in Figures 7 and 8.

The space segment vulnerability simulation module generates simulated data including vulnerability data, messages between OCS and satellites, and ISL measurements,
which are input to the SAIM module. The SAIM module analyzes the data and monitors essential parameters about the ISL ranging measurements, ephemeris accuracy, and satellite operation status.

2.4. Assessment and verification module
The main roles of assessment and verification modules are simulation, assessment, and verification of space segment signal. These modules include 14 site monitoring network of electromagnetic environment, model calculation workstation of space electromagnetic environment, display and storage, vulnerability simulation module of space segment, SAIM, etc. Figure 9 shows the functional architecture of the assessment and verification module.

2.5. Integrated control module
Integrated control module provides an integrated control platform for control platform of other subsystems including human–computer interaction, integrated call, vulnerability and the occurrence of interference module blocking jammers, deception jammer, atmospheric environment model settings, spatial link simulation scenarios, and simulation of multipath effects settings, etc (Figure 10).

This module integrates the four elements mentioned above into a control platform aimed at controlling the following:

1. Selection and combination of real and simulated signals generated by space environment simulation module and output of the signals;
2. Scenarios and models of the space segment vulnerability simulation module and settings of the SAIM monitoring module;
Parabolic dish antenna tracking in the signal-quality monitoring module;
Threshold parameters and human–machine interface display in the vulnerability assessment and verification module.

3. Conclusions
This paper has designed and constructed a platform for the simulation, verification, and mitigation of GNSS vulnerabilities. The system is able to simulate vulnerabilities among others of ISLs interference, atmospheric anomalies, and electromagnetic interference including that generated by human intervention, as well as multipath. It provides a platform for future research on GNSS vulnerabilities. The platform enables the evaluation of satellite navigation service quality enabling studies of enhanced models to better predict the manifestations and mitigate the impacts of GNSS vulnerabilities.

Acknowledgments
This study is supported by the National High Technology Research and Development Program of China (863 Program, No. 2011AA120503).

Notes on contributors
Zhao Xin is a postdoctoral researcher at the Shanghai Jiao Tong University. His study involves GNSS vulnerabilities and satellite navigation and positioning.
Zhan Xingqun is a professor at the Shanghai Jiao Tong University. He is mainly engaged in the field of satellite navigation technology and integrated navigation technology.
Yan Kai is a master at the Shanghai Jiao Tong University. His main research interests are GNSS vulnerabilities.

References
(1) American Meteorological Society. Understanding Vulnerability & Building Resilience. Washington, DC. http://bit.ly/mkRQu (accessed Jun 12, 2012).
(2) Rodriguez, I.; Garcia, C.; Catalán, C.; Mozo, A.; Tavella, P.; Galleani, L.; Rochat, P.; Wang, Q.; Amarillo, F. Satellite Autonomous Integrity Monitoring (SAIM) for GNSS Systems. Proceedings of the 22nd International Meeting of the Satellite Division of The Institute of Navigation, Savannah, GA, 2009; pp 1330–1342.
(3) Filjar, R. A Study of Direct Severe Space Weather Effects on GPS Ionospheric Delay. J. Navig. 2008, 61, 115–128.
(4) Thomas, M. Global Navigation Space Systems: Reliance and Vulnerabilities. The Royal Academy of Engineering: London, UK. http://bit.ly/feFB2i (accessed Jul 23, 2012).
(5) Shaw, G.; Grant, A.; Williams, P.; De Voy, M.; Mitigating the Effects of GNSS Interference – GLA Monitoring and Update on eLoran. In GNSS Interference, Detection & Monitoring Event; Digital Systems KTN (Location & Timing), March 2011.
(6) Dixon, C.S.; Hill C.J.; Dumville, M.; Lowe, D. The Testing Truth of GNSS Vulnerabilities. In ENC GNSS 2011 Conference, London, 29, November 2011.