

全球导航卫星系统脆弱性计算机仿真环境设计及其评估方法实现

赵欣¹, 战兴群¹, 杜刚¹, 李社军²

(1. 上海交通大学 航空航天学院, 上海 200240; 2. 中国伽利略卫星导航有限公司, 北京 100098)

摘要: 设计并搭建了全球卫星导航系统(GNSS)脆弱性计算机仿真验证环境,并对GNSS信号传输环境的评估方法进行了计算机仿真实现;GNSS脆弱性仿真验证环境由空间信号环境子系统、空间段脆弱性仿真子系统、脆弱性评估验证子系统组成,可提供包括GNSS信号传输全链路干扰的仿真、验证与缓解;文章着重介绍了该仿真环境的系统构成及功能,对GNSS信号传输环境的评估方法进行了细分,并完成了脆弱性评估验证平台环境的软硬件实现,通过既定的评估方法及验证标准步骤及途径,完成了空间段脆弱性链路仿真,SAIM对星间链路的监测,GNSS脆弱性评估软件实现数据等结果分析,实验结果证明系统方案合理有效。

关键词: GNSS脆弱性;评估;监测;仿真环境;

GNSS Vulnerability Assessment Method and Its Simulation Environment Design

Zhao Xin¹, Zhan Xingqun¹, Du Gang¹, Li Shejun²

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

2. Chine Galileo GNSS Co., Ltd., Beijing 100098, Chine)

Abstract: I introduces the design and construction of global navigation satellite systems (GNSS) vulnerability simulation environment. The simulation environment contains simulation of the signal-in-space environment, simulation of the vulnerabilities in the space segment, vulnerability assessment and validation. 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. Through the evaluation method established and verification procedures and approaches, Complete the space segment vulnerability link simulation, monitoring the inter satellite link SAIM, analysis of the GNSS vulnerability assessment software to realize data results. The experimental results show that the system scheme is reasonable and effective.

Keywords: GNSS vulnerability; assessment; verification; simulation environment

0 引言

随着全球导航卫星系统(GNSS)在世界范围内军事、国民经济、日常生活等几乎所有领域的广泛使用,人类越来越依赖GNSS所提供的定位、导航与授时(PNT)服务。而影响GNSS服务信号有很多因素^[1],包括有意干扰和无意干扰,以及来自自然现象的干扰。这些干扰所带来的影响涉及方方面面,例如,电力系统运行中断,通信、运输、金融服务的瘫痪,甚至危机生命安全等等。

GNSS脆弱性是指GNSS在各类因素影响下系统端维持正常工作、用户端维持正常服务质量的程度。其内涵指在各类故障、干扰因素发生时,系统及服务质量受到影响的程度。为此,通过对GNSS脆弱性各段影响因素,影响机理的深入研究,设计了GNSS脆弱性环境仿真系统,对GNSS脆弱性影响因素进行进一步分析、比较从而实现其有效探测和缓解。最后提出了解决GNSS脆弱性的根本出路和具体方法以及以后GNSS脆弱性的研究方向和存在难题^[2]。

收稿日期:2014-05-10; 修回日期:2014-06-14。

基金项目:国家高技术研究发展计划(863计划)课题(2013AA12A206)。

作者简介:赵欣(1977-),男,山东青岛人,博士,主要从事卫星导航、电气自动化等方向的研究。

1 GNSS脆弱性仿真环境原理及设计

GNSS脆弱性物理仿真验证平台设计要考虑信号可能受到的各种环境影响因素以及信号的评估验证流程。根据GNSS系统组成,GNSS脆弱性影响因素主要分为空间段、环境段、用户段^[3]。建立仿真评估验证平台首先应具备射频信号产生能力,因此需要实现各个卫星导航频段(GPS L1/L2/L5, Galileo E6等)信号的仿真,这些导航信号与环境中的干扰因素结合实现仿真复杂环境中信号传播的功能,在信号仿真的同时,与实际信号一起由信号跟踪系统进行接收,以实现模拟环境信号的比对与校正;其次,卫星信号质量的好坏需要一定的监测和评估手段,能够对受各种脆弱性因素影响的GNSS信号进行详细分析,因此要建立信号质量监测处理子系统;第三,空间段是卫星导航系统的核心,空间段的脆弱性直接影响卫星导航系统的性能,因此一个完整的GNSS仿真系统必须包含一个能够实现针对空间段脆弱性情景的仿真系统;最后,利用上述所建立的GNSS脆弱性仿真平台子系统,将其仿真输出与参考信号一起进行评估并对相关技术进行验证,最终将获得的评估验证结果显示于综合控制平台上。

如图1所示。空间信号环境仿真子系统设计首先是射频信号的仿真和获取。射频信号分为仿真信号和真实信号,如图所示。真实信号支路:实验室楼顶多模天线及多星座多模接收机

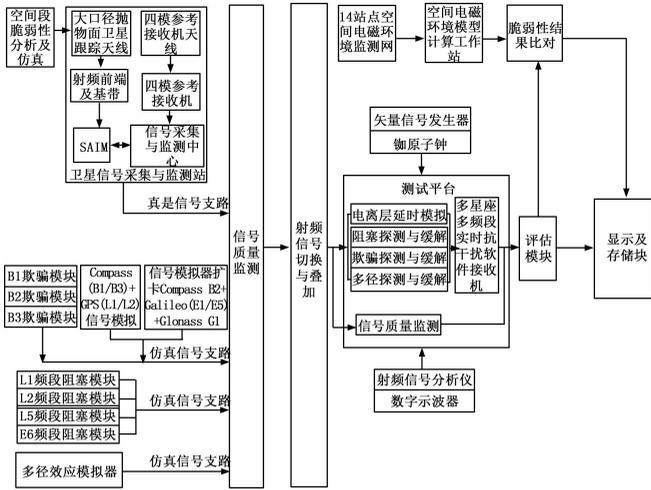


图 1 GNSS 信号环境仿真与脆弱性评估验证环境流程

中相应的多模宽带射频前端负责接收来自 BD/GPS/Galileo/GLONASS 的真实信号。空间段脆弱性分析及仿真模块为大口径抛物面卫星跟踪天线提供输入——依据当前空间段的失效模式及可能影响而改变该天线的跟踪策略，为空间段脆弱性的缓解方法研究提供依据，该大口徑抛物面卫星跟踪天线的实施方案详见实施细则部分。大口徑跟踪天线传来的信号经射频前端和数字基带处理后，为 SAIM 模块提供输入，SAIM 模块处理的结果输入到信号采集与监测中心，由工作站完成相应的分析和存储任务。仿真信号支路 1 负责提供由 BD/GPS/GLO-NASS 和 Galileo/GPS 模拟器提供的仿真信号；此外，用这两类信号模拟器作为 B1、B2、B3 欺骗信号源。需要特别说明的是，由于与 BD 相关的 GNSS 脆弱性是本课题的脆弱性仿真分析评估系统研究的侧重点，此外 BD 的信号特征在当前所有 GNSS 信号中具有代表性，因而欺骗信号源确定为只针对 BD 的信号产生，不考虑 GPS/Galileo/GLONASS 的信号。仿真支路 2 负责提供由阻塞模块提供的阻塞信号。为此，将研制四个频段（L1、L2、L5、E5，囊括了 BD/GPS/Galileo/GLONASS 所有频段上民用信号的阻塞信号发生器，通过可调中心频率和可调带宽的方法实现具体的软硬件。仿真信号支路 3 负责多径效应的模拟。

以上一路真实信号及三路仿真信号通过射频信号切换及叠加模块实现不同的组合，适应后续测试平台中多项脆弱性关键技术研究的输入要求。测试平台获取来自切换及叠加模块的信号，实现以下功能：阻塞探测与缓解、欺骗探测与环节、多径探测及缓解以及电离层全球延迟时空特征分析。这些模块输出的缓解策略被应用到后续的多星座多频段实时抗干扰接收机的研制中。与此同时，信号质量监测模块也以切换及叠加模块为输入，其监测结果与多星座多频段实时抗干扰接收机的输出一并送入后续的评估模块中，由评估模块决定脆弱性各项指标的阈值和数值。为了验证评估的正确性，系统同时接收由 14 个站点组成的空间电磁环境监测网传来的监测数据，进行空间电磁环境模型的生成和比对，进而生成另一路脆弱性指标的数值结果^[4]。将前述脆弱性评估的结果与这组结果进行对比，完成脆弱性评估结果的验证。验证结果送入显示及存储模块。

平台从信号输入、参数调整、算法互换、用户场景等不同层面对不同环境下的脆弱性原因及相应的对抗措施进行评估和验证，并给出相应的综合分析报告。

2 评估方法及验证标准

主要针对验证平台产生的各频段信号（包括载波、伪随机码、导航电文及其他附加的信号成分）进行以下评估，针对评估方法，主要以误检率、检出率为评价标准。评估方法及验证标准步骤及途径如图 2 所示。

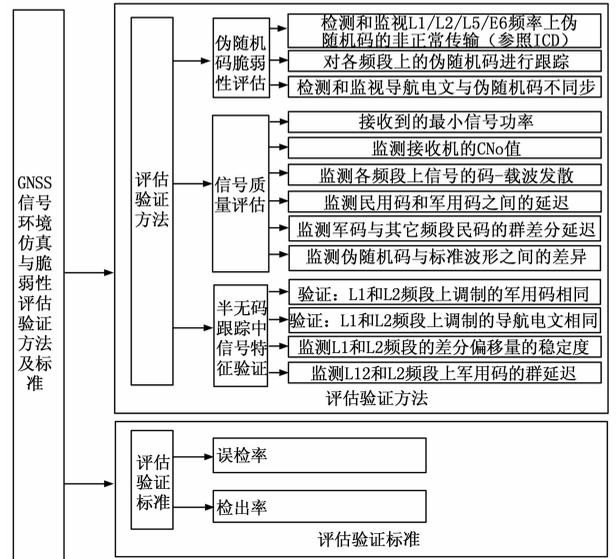


图 2 评估方法及验证标准步骤及途径

2.1 伪随机码脆弱性评估

(1) 检测和监视 L1/L2/L5/E6 频率上伪随机码的非正常传输（参照 ICD）；

(2) 无论导航电文中标示信号健康与否的那位是否置 1，都对各频段上的伪随机码进行跟踪；

(3) 检测和监视导航电文与伪随机码不同步的情况。

2.2 信号质量评估

(1) 接收到的最小信号功率是否达到或超过 ICD 上指定的数值；

(2) 对于标示为健康的卫星信号，连续不间断地监测接收机的 C/N₀ 值，报告 CN₀ 突然降低或突然升高的情况；

(3) 监测各频段上信号的码-载波发散（code-carrier divergence）在 100-7200 秒时间内是否低于 ICD 规定的数值；

(4) 监测 L1 频段上的军用码与其它频段上的民用信号之间的群差分延迟是否低于规定的数值。

2.3 半一无码跟踪（semi-codeless tracking）中的信号特征验证

(1) 验证：L1 和 L2 频段上调制的导航电文是否相同；

(2) 监测 L1 和 L2 频段的差分偏移量（differential bias）的稳定度是否在规定范围内；

软件体量及运行环境分析来说，软件在两个部分中体现，一类是在硬件平台的 DSP 上，对实时性要求比较强，包括中频、射频模块，体量约在 4~5 千行的 C 语言程序；另一类是在工作站上运行的软件，而且这些软件在多个工作站并行运

行。由于所采集的和实时处理的数据大概达到每秒几兆至几十兆的流量, 因此选用的计算机应该具备的配置为 8 个 CPU, 16G 内存, 由于涉及的场景比较多, 需有多台计算机联网并行完成。估计该部分软件的体量约在 10 万行。

3 GNSS 脆弱性评估平台软硬件实现

3.1 GNSS 脆弱性仿真评估平台结构及原理

GNSS 脆弱性仿真评估平台由以下模块组成: 2 台卫星信号模拟器、2 个欺骗干扰模块、4 个阻塞干扰模块、1 个多径效应软件模块、1 套四模参考站天线系统 (包含两个接收机天线、1 台 GPS/BeiDou 双模接收机、1 台 Galileo/Glonass 双模接收机和一台服务器)、1 台多模多频软件接收机及射频前端模块、1 个射频信号切换与叠加模块、电离层/对流层仿真软件、空间段脆弱性仿真系统 (星间链路仿真) 以及 1 个数据处理服务器组成^[5]。

仿真评估平台结构如图 3 所示, 综合控制计算机通过串口连接阻塞干扰器 (L1/L2/L5/E6)、欺骗干扰器 (GPS/BeiDou)、多径仿真模块, 通过网络连接空间段脆弱性仿真计算机, 进行仿真参数的配置和控制生成。其中, 两个模拟器组合使用分别能够实现对 GPS、Galileo、Glonass 和 BeiDou 的四系统信号的仿真生成; 阻塞干扰器用于产生 L1/L2/L5/E1 频段的阻塞干扰, 欺骗干扰器生成 GPS L1 和 BeiDou B1 的欺骗信号。多径的仿真结合 GNSS 模拟器进行, 定制的模拟器能够嵌入多径模块来进行多径的信号生成。

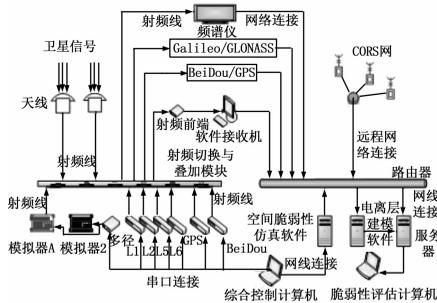


图 3 脆弱性仿真评估平台结构图

平台通过一个射频切换与叠加模块, 将接收到的真实卫星信号、GNSS 模拟信号、阻塞干扰、欺骗干扰、非 GNSS 干扰、多径干扰信号进行切换和叠加, 根据仿真不同的脆弱性情景进行组合输出相应射频信号, 该信号通过 GNSS 四模接收机或软件接收机进行接收, 同时由频谱仪进行分析, 接收设备的分析结果通过网络存储至服务器中^[6]。服务器通过网络实时获取 CORS 网的卫星观测数据进行数据处理, 用于建立大气模型及其参数的计算, 实现电离层、对流层环境的实时仿真。结合空间脆弱性仿真软件实现多种卫星故障模式下, 星间测距值的仿真输出, 以仿真系统星间链路脆弱性情景。空间段脆弱性仿真模块根据不同的空间段脆弱性情况, 生成模拟脆弱性环境数据, 为 SAIM 模块提供输入。包括卫星脆弱性数据、地面测控系统星间链路数据、卫星星间链路数据等。输出各卫星星历 (轨道、时钟等参数)、星间测距值以及地面观测值等。卫星星历包括导航电文、卫星工作状态等参数, 以及星座内所有卫星的预报轨道与时钟参数 (即星历)。

SAIM 模块对空间段脆弱性模块产生的脆弱性情景数据进

行分析, 监测卫星各重要参数, 分析包括星间链路测距值、导航电文正确性、卫星工作状态等数据。

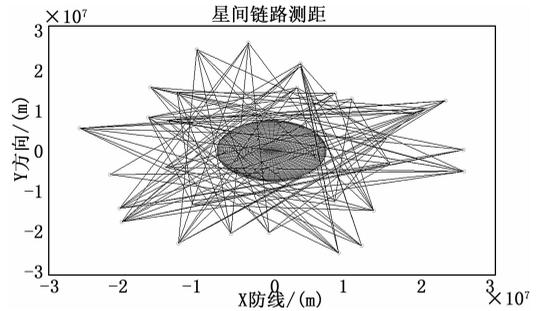


图 4 空间段脆弱性链路仿真

图 4 中, 球体部分代表地球的电离层, 连线代表仿真的星间链路测距, 图 5 为 SAIM 对星间链路的监测结果, 列出了根据该链路测距值计算同一时刻每颗卫星的检验统计值情况, 每颗卫星自有的检验统计量分别与自有的统计值阈值作比较, 可以判断出空间链路故障状态。

最后, 脆弱评估计算机从服务器中获取各类观测数据进行脆弱性评估。

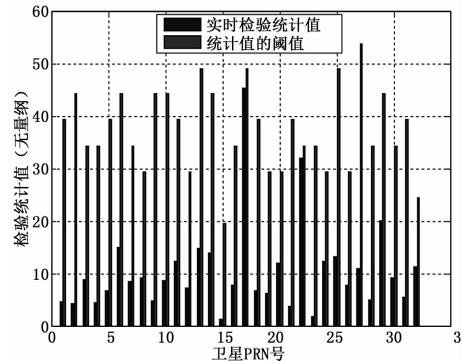


图 5 SAIM 对星间链路的监测结果

3.2 GNSS 脆弱性评估流程设计

由于各种脆弱性因素引起的影响是交互的, 因此判断影响的来源需要先提出脆弱性影响的判断方法, 然后进一步分类排除。如图 6, 根据卫星数和几何分布情况、载噪比异常、伪距测量定位异常及导航电文轨道参数异常等脆弱性影响后果, 形成了相应的判断方法: 利用预报星历进行卫星可用性/几何分布判断, 根据 C/No 周期变化特性及理论值方法判断 C/No 异常, 根据已有接收机位置判断定位精度及误差以及对真实电文进行电文校验的方法。这样, 可以评估内容总结为定位差异性、星座运行完好性、导航数据正确性、空间环境稳定性这 4 个定性指标^[7]。

从脆弱性影响程度来说, 对导航系统产生最严重的后果即引起卫星信号异常, 接收机无法正常接收, 因此, 应先判断卫星信号的正常与否, 图中通过瞬时卫星数、卫星号及卫星分布情况与预测信息 (卫星电文、预报产品等) 一致性来进行评估。接收机接收到的这种卫星分布异常的情况通常可以进一步判断出接收机附近电磁干扰、电离层闪烁、信号遮挡、卫星故障的发生。

当脆弱性影响不足以中断卫星信号时, 接收机即可正常接

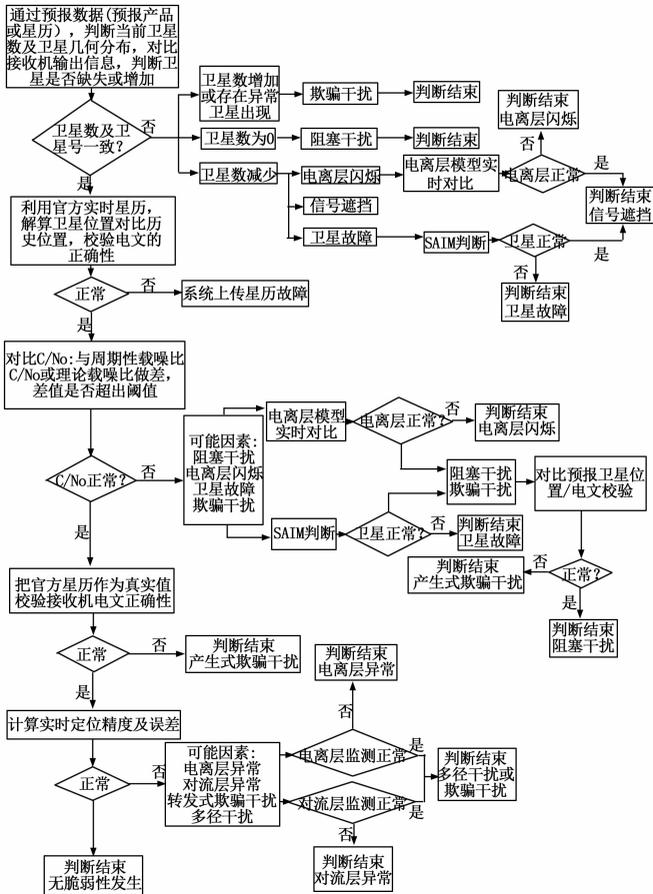


图 6 评估流程设计图

收, 这种情况下, 我们可以利用载噪比 C/N_0 的周期性规律或理论值进行实时校验, 由此可以分类出弱化的电磁干扰、电离层异常或多径情况的发生。通过上述的判断后, 考虑到微弱的脆弱性影响, 仍然需要进一步判断脆弱性发生情况, 由于接收机能够正常接收卫星信号, 即可以进行定位。那么, 通过已知的接收机位置来获取定位精度, 从而判断脆弱性影响的程度^[8]。另外, 通过 RAIM、SAIM 等算法进行离线处理, 可以提供辅助判断功能。

3.3 脆弱性评估软件实现

如图 7 所示。



图 7 GNSS 脆弱性评估软件实现

证功能, 评估脆弱性因素对卫星导航/定位系统的影响程度以及对脆弱性研究的相关干扰、抗干扰、监测技术的验证功能。

评估模块以软件形式进行实现, 软件首先获取评估所需所有数据, 包括软件接收机观测数据、交大参考站接收机观测数据、IGS 站星历及大气环境参数、空间段仿真测距数据等, 根据相应算法对数据进行处理和分析, 获得评估结果。另外, 评估模块受综合控制计算机的参数控制, 对评估的指标和阈值进行设定等。最后将分析和评估的结果进行显示、存储以及报表生成。

4 结论

随着全球卫星导航系统的建设, 为了保证未来导航应用的可靠性、安全性, 必须对 GNSS 系统存在的脆弱性因素进行系统地研究, 论证和评估脆弱性干扰因素影响程度。本文设计了 GNSS 脆弱性环境仿真与缓解验证平台系统, 并对 GNSS 信号脆弱性的评估方法和验证标准进行了分析, 最后完成了脆弱性评估平台软硬件实现。GNSS 脆弱性环境仿真系统能够实现从星间链路干扰、大气环境及电磁环境异常、人为信号干扰、多径干扰等全链路脆弱性的仿真, 为后续脆弱性因素的研究和评估缓解提供了平台, 为接收机的应用以及抗干扰技术等研究提供有力的保障。总而言之, GNSS 脆弱性解决不是一朝一夕就能做到的, 必须经过长期的研究和积累, 其最后出路就是加强模型化技术研究, 针对物理环境, 要继续加强多径模型的研究; 针对日地环境, 建立预报模型是关键; 针对电磁环境, 建立预测模型才是硬道理^[9]。

参考文献:

- [1] American Meteorological Society. (2011). Understanding Vulnerability & Building Resilience [EB/OL]. AMS. Washington, DC. Available at: <http://bit.ly/rnkRQu>.
- [2] 曹冲. 全球卫星导航系统的最新动向与发展趋势 [J]. 卫星与网络, 2010, (93): 22-25.
- [3] Dixon J Hill C S, C Dumville M, et al. The Testing Truth of GNSS Vulnerabilities [A]. ENC GNSS 2011 Conference [C]. London, Nov. 29-Dec. 1, 2011.
- [4] Andy G Proctor, Charles W T Curry [Z]. GAARDIAN: A System To Detect GNSS Jamming and Interference. 2012.
- [5] Shaw G A, Grant P. Williams and M. De Voy; Mitigating the effects of GNSS Interference - GLA monitoring and update on eLoran; GNSS Interference, Detection & Monitoring Event; Digital Systems KTN (Location & Timing) [Z]. March 2011.
- [6] Global Navigation Space Systems: Reliance & Vulnerabilities [Z]. Royal Academy of Engineering, March 2011.
- [7] Thompson R J R, Wu J H, Asghar Tabatabaei Balaei, Andrew G. Dempster. Detection of RF interference to GPS using day-to-day C/N_0 differences [A]. 2010 International Symposium on GPS/GNSS [C]. Taipei, Taiwan, 2010, October 26-28.
- [8] 严凯, 战兴群, 秦峰, 等. GNSS 脆弱性环境仿真系统设计 [J]. 传感器与微系统, 2013, 32 (2): 24-29.
- [9] Zhao X, Zhan X Q, Yan K. GNSS Vulnerability Physical Simulation Verification and Mitigation Platform Design [J]. Geo-spatial Information Science, 16 (3): 149-154.