GNSS 欺骗防护技术国内外研究现状及展望

边少锋, 胡彦逢*, 纪兵

海军工程大学导航工程系, 武汉 430033

* 通信作者. E-mail: daohang-yanfeng@163.com

收稿日期: 2016-03-30; 接受日期: 2016-08-18; 网络出版日期: 2017-01-18

国家重点基础研究发展计划 (973)(批准号: 2012CB71992) 和国家自然科学基金 (批准号: 41631072, 41274013, 41504029) 资助项目

摘要 随着电磁环境的日益复杂特别是军事对抗强度的日益加大, 卫星导航应用的潜在安全隐患已成为现实威胁. 传统的卫星导航抗干扰技术大多针对压制干扰, 对欺骗干扰考虑不多, 而欺骗干扰对用户造成的危害并不亚于压制干扰. 本文简要介绍了欺骗干扰防护技术的研究背景, 包括概念、原理、应用案例等, 深入分析和总结了国内外抗欺骗干扰技术主要研究进展, 最后重点阐述了当前抗欺骗干扰方法存在的问题和未来欺骗防护技术的发展趋势.

关键词 全球导航卫星系统, 接收机, 欺骗, 反欺骗

1 引言

1.1 简介

全球导航卫星系统 (global navigation satellite system, GNSS) 能够在全球范围内提供全天候的位置、速度和时间 (position, velocity & time, PVT) 服务, 各主要大国都在大力发展各自的 GNSS 系统, 美国的 GPS (global positioning system), 欧洲的 Galileo, 中国的 BDS (BeiDou navigation satellite system), 以及俄罗斯的 GLONASS (global navigation satellite system) 并称当今世界四大 GNSS 系统. 此外, 正在建设中的区域卫星导航系统还有印度的区域导航卫星系统 IRNSS (Indian regional navigation satellite system)、日本的准天顶卫星系统 QZSS (Quasi-Zenith satellite system). 当前我国的 BDS 经历了十几年的发展历程, 已经取得了突破性进展, 已于 2012 年面向亚太地区提供服务, 并将于 2020 年左右实现全球覆盖的目标 [1, 2].

当前 GNSS 已从最初的军用导航定位服务深入到许多专业应用领域, 并引起了众多领域的巨大变革. 民用领域, 当前已广泛应用于智慧城市 [3]、精密农业、GIS 技术 [4]、电网监控、林渔业 [5]、物联网 [6]、地震监测 [7]、地质调查、海洋测绘及海洋环境监测等众多行业及其他对定位、测速和授时有需

引用格式: 边少锋, 胡彦逢, 纪兵. GNSS 欺骗防护技术国内外研究现状及展望. 中国科学: 信息科学, 2017, 47: 275–287, doi: 10.1360/N112016-00073
Bian S F, Hu Y F, Ji B. Research status and prospect of GNSS anti-spoofing technology (in Chinese). Sci Sin Inform, 2017, 47: 275–287, doi: 10.1360/N112016-00073

图 1 (网络版彩图) 被伊朗军方俘获的 CIA 操纵的无人侦察机 “RQ-170”

Figure 1 (Color online) Drone “RQ-170” controlled by CIA is captured by the Iranian military

求的领域. 随着我国自主建设运行的 BDS 的快速发展, 目前我军的作战平台、武器装备乃至单兵都在逐步配备北斗导航终端以替换原来的 GPS 设备, 为我国的国防现代化建设保驾护航.

然而, 电磁环境的日益复杂对卫星导航安全应用提出了严峻的挑战, GNSS 抗干扰技术已成为国内外研究的热点方向. 针对卫星导航接收机的干扰主要分为两大类: 压制干扰与欺骗干扰. 以前导航领域所讨论的 GNSS 接收机抗干扰技术主要针对的是压制干扰, 而对欺骗干扰较少考虑. 压制干扰是以大功率压制干扰机发射单频、扫频、伪码等压制信号使得目标接收机失锁无法正常工作, 其首要目标在于使 GNSS 终端精度下降甚至不可用. 欺骗干扰指的是通过产生与真实信号高度相似的欺骗卫星信号或者转发真实卫星信号, 其首要目标是在隐蔽的条件下使得 GNSS 终端得到虚假的时间、位置、速度等信息, 达到欺骗目的^[8~10]. 相比之下, 欺骗干扰不需要太强的功率, 隐蔽性好, 这也使得欺骗干扰源具有较强的生存能力. 从某种程度上来讲, 欺骗干扰带来的危害比压制干扰更为严重.

学术界对抗欺骗干扰的研究起步于 21 世纪初, 这明显晚于 GNSS 抗压制干扰的研究. 一方面是因为欺骗式干扰在早期被认为是一种高成本、高复杂度而几乎无法实现的干扰方式; 另一方面也是在和平年代, 人为释放干扰容易造成安全事故而被法律所禁止. 许多无意干扰 (一般属于压制式干扰) 时常发生, 影响了 GNSS 的应用, 而欺骗式干扰一般都是有意干扰, 在未发生战争时不容易引起重视.

1.2 应用背景

2011 年 12 月, 伊朗宣布成功俘获了美国中央情报局 (CIA) 操纵的用于搜集关于伊朗核设施情报的隐形无人侦察机 “RQ-170” (图 1¹⁾), 该无人机误以为降落在了指定的美军基地, 而事实上该无人机降落到了距离美军基地 140 英里的伊朗领土内. 据有关专家分析, 伊朗军方是通过切断无人机与基地联系的通信链路后, 迫使无人机处于自动驾驶状态, 然后采用欺骗攻击手段实现对无人机的俘获.

2012 年 6 月美国德克萨斯州立大学的 Todd Humpherys 团队在大学田径场内演示了使用硬件成本还不到 1000 美元的 GPS 民用信号欺骗设备通过释放欺骗干扰信号改变了一架小型无人机的飞行路径 (如图 2²⁾所示), 对此美国媒体进行了公开报道 (如图 3²⁾所示). 随后, 受对此持怀疑态度的美国国家安全局官员邀请, Todd Humpherys 团队在美国白沙导弹靶场再次进行成功演示, 这更加刺激了美国政府和军方的神经.

2013 年 4 月在荷兰阿姆斯特丹举行的黑客安全大会 (hack in the box, HITB) 上, 同样身为商业飞行员的德国某网络安全公司工程师 Hugo Teso 宣称, 经过四年的努力, 他成功研发出一套名为

1) 图 1(a) 来源于 <http://military.china.com/news2/02/11078239/20120704/17296475.html>, 图 1(b) 来源于 <http://52wmf.blog.163.com/blog/static/8942082201111711225490/>.

2) <http://www.foxnews.com/tech/2012/0625/drones-vulnerable-to-terrorist-hijacking-researchers-say/>

图 2 (网络版彩图) 无人直升机欺骗干扰演示现场

Figure 2 (Color online) Demo site of spoofing attack on UAV

图 3 (网络版彩图) 美国新闻媒体对无人机欺骗演示试验进行公开报道

Figure 3 (Color online) The American news media publicly reported demonstration experiment on UAV cheating

图 4 (网络版彩图) Hugo Teso 设计的黑客攻击应用程序“PlaneSploit”(Android 版)主界面

Figure 4 (Color online) Main interface of hacking application “PlaneSploit” (for Android) designed by Hugo Teso

图 5 (网络版彩图) Texas 大学网站提供的游艇欺骗试验演示场景

Figure 5 (Color online) Demo scene of the yacht cheating experiment offered by the website of University of Texas

PlaneSploit 的应用软件 (如图 4³⁾所示), 可以绕过飞机的安全检查系统并接管飞机上的电脑系统, 让飞机“随他的步调起舞”。在这次模拟展示中, Hugo Teso 通过 PlaneSploit “完全操控飞机”, 成功实现了更改飞行路线、改变空调设置, 甚至能够让飞机坠毁。Hugo Teso 还表示, 该软件已能够破坏目前大多数飞机所使用的飞行管理系统 (FMS)。

2013 年 6 月, Todd Humpherys 教授团队为了演示了 GPS 欺骗干扰对航海交通工具的安全性威

3) <http://biz.xinmin.cn/2013/04/13/19714232.html>

胁,使用民用欺骗干扰设备释放欺骗信号成功欺骗了一艘价值 8000 万美元的私人豪华游艇,在欺骗攻击下该游艇逐渐偏离了预定航线(如图 5⁴⁾所示)。

2014 年 3 月马来西亚吉隆坡国际机场飞往北京首都国际机场的航班 MH370 失联,至今未发现残骸,有专家推测 MH370 很可能遭到了欺骗干扰攻击,导致偏离航线,燃油耗尽后坠毁,从技术角度来讲欺骗干扰技术具备这种潜在攻击力,在当前对此事件尚无定论的情况下并不排除这种可能性。Seo 等^[11]针对欺骗干扰对无人机导航系统的诱骗可行性进行了分析及试验验证。结果表明,虽然无人机本身具有一定的欺骗防护能力,但当欺骗实施方知晓无人机的运动状态时可以实现对无人机诱骗。Baziar 等^[12]设计了一种借助软件接收机和真实信号以产生欺骗干扰信号的方法,该方法实用性强,无需昂贵的硬件设备,降低了欺骗干扰实施的复杂度和成本。

1.3 目的和意义

随着卫星导航技术的发展,卫星导航系统的完好性、可用性、定位精度等都得到了大幅度地提升和完善,但欺骗干扰带来的安全隐患尚没有引起足够的重视。当今社会对 GNSS 依赖性越来越大,如何提高卫星导航系统的安全性,已经成为当今卫星导航领域的重要议题。当前我国在该领域研究尚未全面地、系统地展开,针对我国的 BDS 应用仍然缺乏必要的欺骗防护措施, BDS 为我国的国防安全提供重要保障,但 BDS 本身的安全亟需建立可靠的防护体系。

本文主要是对当前国内外欺骗与反欺骗技术研究现状进行分析总结,并指出当前存在的一些问题,为进一步深入开展 GNSS 欺骗与反欺骗技术研究提供一定的理论指导,也希望能够引起国内相关部门和科研人员的重视。本文第 2 节和第 3 节分别介绍了国外研究现状和国内研究现状,并分析了现有方法的应用范围和特点;第 4 节总结了全文。

2 国外研究现状

2001 年美国国家运输系统中心的 Volpe^[13]在其提交给美国国家运输部的技术报告中首次评估了欺骗式干扰对全球定位系统的危害性,学术界和工业界才正式开始了对抗欺骗式干扰技术的研究。针对卫星导航接收机抗欺骗干扰技术方面的研究,美国处于绝对领先地位,起步较早,成果也最多。具有代表性的科研机构有美国德克萨斯州立大学、美国康奈尔大学等,一些研究项目背后也不乏美国政府和军方的支持。其他国家包括加拿大卡尔加里大学、伊朗科技大学等,在这方面也取得了一定的研究成果。抗欺骗干扰技术主要分为三类:第一类,信号加密认证技术;第二类,信号特征检测技术;第三类,辅助信息检测技术。

2.1 信号加密认证技术

这主要是针对民用信号的,因为军用信号如 GPS 的 P(Y) 码在设计之初就采取了加密措施,只对政府和军方等特定授权用户,想要对其实施欺骗是比较困难的。早在 2003 年 Scott^[14]就提出了对民码信号加密认证的思想,以有效应对欺骗干扰的攻击。信号加密认证技术又分为三大类:导航电文加密技术(NMA)、扩频码加密技术和无码互相关技术。

导航电文加密技术方面,2011 年 Wesson 等^[15]针对 GPS L2 和 L5 频点上的民码导航电文(CNAV)设计了一种基于后向兼容的加密方法。2012 年, Wesson 等^[16,17]设计了一种 NMA 加密认证方法,该

4) http://radionavlab.ae.utexas.edu/index.php?option=com_content&view=article&id=324:spoofing-on-the-high-seas&catid=29&Itemid=2

方法采用了数字签名技术,在应对转发式欺骗干扰且虚警率为0.1%时,检测概率可以达到97%以上.2014年Kerns等^[18]在PLANS会议上做了一篇关于NMA技术报告,对GPS的NMA技术发展蓝图进行了规划.

针对扩频码加密技术类似于P(Y)码加密原理,即在GPS的C/A码上调制一个加密的安全码,Kuhn^[19]设计了一种基于短周期隐藏的扩频码加密方法.导航电文加密认证技术和扩频码技术能够有效抵御欺骗干扰的攻击,但是需要由国家层面对整个信号体制进行更改,成本高昂,短期内难以实现.当前对GPS民码信号的加密措施仍处于论证阶段.

无码相关技术方面,康奈尔大学的Psiaki等^[20]对这方面进行了理论分析和试验验证,并在实时性检测理论方面进行了有益地探索^[21~23].无码相关技术利用的是原有信号体制同一频点上军码和民码正交关系,如果欺骗信号只针对民码实施攻击,就会破坏这种正交关系,也就为欺骗信号检测提供了前提条件.它相对于导航电文加密和扩频码加密措施的最大优点是无需更改现有信号体制,通过GNSS终端即可实现欺骗检测,但它的缺点是自身无法进行检测,需要借助其他GNSS终端通过网络互连协同检测,且需要保证参考接收机未受到欺骗攻击,当参考接收机和用户接收机之间的距离较近时容易造成漏警.

2.2 信号特征检测技术

针对这方面的研究成果相对较多,这类方法无需更改信号体制,有的只需要对接收机内部程序进行升级,有的需要对内部硬件结构更改,也可做成单独的抗干扰模块对接收机进行加装.这类方法依靠接收机终端本身就可以实现欺骗检测,具有灵活高效的特点.

加拿大卡尔加里大学的Dehghanian等^[24,25]提出了一种针对捕获阶段欺骗攻击的多峰值三元假设检验方法,该方法在城市多径环境下可以有效检测欺骗攻击的存在;Jafarnia等^[26]针对欺骗干扰对接收机噪声水平的抬高作用进行了建模分析,提出了一种基于信号功率、噪声功率、载噪比等多因素综合的欺骗检测方法,可以有效减小接收机的易感染区,大大增加成功实施欺骗攻击的难度.

Akos^[27]提出了一种基于信号能量的AGC(自动增益控制)欺骗检测算法,欺骗干扰的引入会使得接收信号总能量增加,进而使AGC增益减小,这种方法不需更改接收机硬件结构,较容易实现.该方法对于直接转发式欺骗干扰具有较好的检测效果,因为噪声成分占信号总能量的大部分,直接转发式欺骗干扰在放大信号的同时也放大了噪声,使得用户接收机接收到的信号总能量明显增加,而对于产生式欺骗干扰,如果只稍高于真实信号,不会引起AGC增益的明显变化.另一方面,用户接收机工作环境变化时,接收到信号质量本身也会变化,此类检测算法可靠性会降低.

Jafarnia等^[28]提出了一种基于运动接收机时间状态监测的欺骗检测方法,分别针对5种假设条件建立了欺骗检测模型:(1)随机运动(状态已知);(2)匀速圆周运动;(3)随机运动(状态未知);(4)匀速直线运动(与欺骗干扰源之间的相对未知关系未知);(5)运动规律未知.Broumandan和Jafarnia^[29]提出了一种接收机运动情况下的功率互相关检测算法.这两种基于接收机运动情况下的欺骗检测算法是建立在欺骗干扰源无法准确掌握用户接收机运动状态前提下的,也就是说一旦假设不成立,欺骗干扰源准确掌握用户接收机运动状态并实时调整控制策略,这类欺骗检测算法很可能失效.

多普勒频移量与信号发射频率成正比^[30],以GPS的L1频点为例,载波多普勒频移量与调制在该频点上的C/A码的码多普勒频移量比值是一个固定的常数,如果欺骗干扰对码和载波分别控制时忽略了此特征,此方法便可以有效检测欺骗干扰的存在.当欺骗干扰攻击处于稳定跟踪过程中的目标接收机时,如果欺骗信号载频与真实信号载频相近但不完全同步,会导致目标接收机跟踪环路输出均

方幅值发生明显跳动现象甚至失锁。一旦欺骗攻击成功牵引目标接收机的跟踪环路至欺骗信号上来,欺骗信号的码相位和载频逐渐远离真实信号的码相位和载频,这种明显的跳动现象逐渐消失。通过检测这个牵引过程中的幅值跳动特征,便可检测出欺骗干扰^[31]。

Psiaki 等^[32]出了一种基于双天线载波相位差分的欺骗检测算法,该算法根据各卫星欺骗信号均来自同一方向的假设,通过双天线载波测得的载波相位差值特征检测欺骗的存在。该方法需要对真实信号来向进行准确估计,复杂度较高^[33]。

欺骗信号码相位相对于真实信号码相位滑动的过程中会引起超前、即时、滞后支路相关输出值的异常变化。鉴于此, Lim 等^[34]提出了一种基于跟踪环路相关输出异常检测的欺骗检测方法,该方法复杂度低,但当欺骗信号码相位和真实信号码相位逐渐远离时该方法将失效。

2.3 辅助信息欺骗检测技术

在用户接收机遭到欺骗攻击的情况下,惯性/磁性传感器、计程仪、高精度时钟等设备提供的辅助信息可以为欺骗检测提供很好的帮助。惯性模块能够不依赖外界信息自主导航(抗干扰能力强),高精度时钟在一段时间内时间保持稳定度高,一旦接收机遭到欺骗攻击,这些辅助设备输出的信息与接收机本身输出的信息会有明显偏差,检测出这种异常将能够有效识别欺骗干扰的存在^[35~37]。Lee 等^[38]提出了一种加速度计辅助的欺骗检测算法,对比加速度计输出信息和 GPS 输出信息差异以检测欺骗干扰引起的异常。

此外,多系统、多频点组合接收机也可以有效抵御欺骗干扰的攻击。如果欺骗干扰攻击其中的单系统、单频点,那么不同系统之间会出现明显的异常,很容易觉察到欺骗攻击的存在,但是具体到哪个系统信号受到攻击需要借助相应的欺骗检测手段进行识别。利用外界辅助信息的欺骗检测方法和采用多频点、多系统组合模式具有很好的抗欺骗干扰能力,但这也增加了用户方的成本,且高精度时钟、惯性元器件等的成本限制了其适用范围。

3 国内研究现状

《第四届中国卫星导航学术年会总结报告》将卫星导航欺骗与反欺骗技术列为“北斗/GNSS 用户终端技术”分会领域的关键技术和热点问题,并指出“无论对于欺骗还是反欺骗技术,都尚未形成完善的分析方法和评估机制”。历届年会在该方向均有所涉及,但实质性的研究成果还不多。

通过整理国内相关文献,发现国内关于欺骗与反欺骗技术的研究可以追溯到杨景曙^[39]2005 年发表在《电子学报》上的一篇题为“通过区域映射实现诱导的 GPS 干扰系统”的文献(在当时国外刚起步不久且尚无丰富理论依据的背景下能够针对该方面技术进行探索很难得)。该文提出了“区域映射”理论,对后续研究具有一定的指导意义,但限于当时条件,许多问题仍需进一步的深入研究。张颂等^[40]对单站转发式欺骗干扰模型进行了分析;闫占杰等^[41]分析了转发式欺骗干扰的时延影响;张会锁等^[42]分析了转发式欺骗干扰实现诱导欺骗的策略;周轩、吕红丽等^[43,44]总结了当前的反欺骗技术研究现状;李四海等^[45]提出了一种惯性信息辅助条件下的 GNSS 欺骗检测方法,可以有效应对单天线发射模式的欺骗干扰,但需要惯性等辅助设备对姿态、基线长度进行精确测量;孙闽红等^[46]提出了一种采用极大似然估计方法的抗欺骗算法,该算法可以在一定程度上对欺骗干扰进行抑制,但在信噪比 = 干噪比 = 8 dB 时,误码率仍高达 30%,尚无法满足实际应用,需要进一步的深入和完善;唐超年等^[47]从 GNSS 信号体制端提出了一种具有抗欺骗性能的新型信号加密认证结构,该信号结构通过在

导航电文数据中使用椭圆曲线数字签名算法来保证电文信息的真实性,进而保证定位结果的真实性。

Liang 等^[48,49]在无码互相关技术方面开展了较深的研究,提出了一种多接收机联网协同检测方法,在参考接收机受欺骗的情况下仍然能够实现对欺骗干扰的有效检测。

国防科学技术大学王飞雪教授团队的黄龙博士^[50~52]在攻读博士期间对 GNSS 欺骗与反欺骗技术进行了较深入的研究,对欺骗干扰在跟踪环路部分成功实施欺骗攻击的功率条件进行了定量分析^[51],建立了针对授时接收机的转发式欺骗干扰模型^[52]。国防科学技术大学的朱祥维等^[53]结合当前的反欺骗技术,设计了授时接收机抗欺骗体系。

在欺骗位置点与卫星距离小于转发信号传播路径时,转发延时为负数,这是工程实践中不可能实现的。针对该问题,胡彦逢等^[54,55]、王海洋等^[56]针对转发式欺骗干扰负延时问题提出了补偿方法。姚李昊等^[57]指出单天线自然转发,用户接收机输出的位置与干扰源天线相位中心一致,改变钟差,但不改变位置(排除舍入误差等因素)。这类似于 GNSS 转发天线,将室外信号转播至室内。胡彦逢和曹可劲^[58]提出一种基于接收机时钟频率漂移检验的欺骗检测算法,该算法结构简单,易于工程应用。胡彦逢和边少锋等^[59]设计了一种欺骗干扰功率控制算法,在一定程度上可以提高欺骗干扰攻击的攻击效果,增强了攻击的隐蔽性。姚李昊和陈飞强等^[60]提出了一种基于多普勒测速的单节点欺骗检测方法,文中针对的欺骗干扰仍然是自然转发式欺骗干扰,也就是用户机的速度与其运动状态无关,而与转发器的运动状态有关。惯性传感器测得的速度可以真实反映接收机本身的运动状态(惯性信息自主导航,不受外界信息干扰的特点),将其与接收机接收卫星信号计算得出的速度值进行对比,差异超过一定范围就说明此时接收机接收到的信号很有可能是欺骗信号。此方法是利用惯性信息辅助检测手段,但针对的不一定只有转发式欺骗干扰,对于欺骗干扰源来讲,想要使欺骗速度始终与接收机本身真实速度保持一致是比较困难的,这就给欺骗干扰检测创造了机会。

赵陆文等^[61]创新性地提出了一种跟踪阶段欺骗检测方法,通过对 PLL 环鉴相器输出信号进行谱分析,就能检测出信号中是否含有欺骗信号,这就是基于载波相位跟踪谱分析检测欺骗信号的基本原理。该方法针对的是欺骗信号与真实信号码相位相差在 1 个码片之内,载频也尽量做到一致(由于多普勒频移的影响,几乎不可能做到同频同相),这就导致接收机在解调后仍然有残余信号(低频)存在,通过频谱分析可以识别欺骗干扰的特征。该方法仍有一些有待深化和完善的地方:(1)残余低频能量的本质可以进一步明确化,有助于发现新的问题,避免以偏盖全,此特点不一定是欺骗干扰才具有的特点;(2)若载波环跟踪有误差,无法将载波理想的解调出来,这时候也会影响欺骗检测;(3)此种场景与多径具有很大的相似性,如何避免因多径存在引入的判别误差需要进一步讨论;(4)此种欺骗干扰模式仍然缺乏必要的应用分析,是为了实现什么目的,码相位始终在 1 个码片之内也是比较困难的,且在跟踪阶段中码环搜索范围内,这样欺骗信号与真实信号之间相互影响无法避免。

中国电子科技集团公司第五十四研究所李雅宁等^[62]针对基于循环相关捕获的欺骗检测、双天线载波相位差检测技术和残留信号检测三方面欺骗检测技术进行分析,认识相对比较客观,对后续研究具有一定的理论指导意义。

胡彦逢等在 GNSS 欺骗与反欺骗技术方面也开展了系统研究。在欺骗干扰技术方面,研究了实现时间欺骗、位置欺骗和速度欺骗的内部机理;对欺骗干扰在接收机捕获阶段和跟踪阶段的影响进行了系统分析^[59,63],提出了一种转发式欺骗干扰钟差补偿策略^[54],并进行了相应的仿真试验验证;在导航对抗背景下对北斗实施欺骗攻击的可行性进行了分析^[64],并提出了一种针对卫星导航接收机的欺骗干扰功率控制策略^[59],可以有效地增强欺骗攻击的隐蔽性。在欺骗防护技术方面,提出了一种基于时钟频率漂移特征检验的欺骗干扰识别算法,可以有效应对单天线发射模式的欺骗干扰^[58];提出了一种基于双差载波相位的欺骗干扰识别算法,该算法无需求解整周模糊度即可实现对欺骗干扰特征的有效

识别⁵⁾; 针对欺骗攻击条件下的信号模型, 设计了一种新型信号质量检测算法, 在应对单天线和多天线欺骗干扰时均具有较好检测效果⁶⁾.

4 总结与展望

总体来看, 国外研究起步较早, 并取得了许多研究成果, 一些技术甚至已经到了工程应用阶段; 国内研究由于起步晚, 且重视程度还远远不够, 系统性、深入的研究尚未全面展开, 虽取得了一些有益的成果, 但实质性的突破还不多, 不少文献仍然停留在理论概念的探讨上. 2015 年 10 月在长沙举办的大地测量会议上, 我国卫星导航方向的领军人物国防科技大学的王飞雪在讲座中强调: 近几年, 美国的高校、企业对这方面的研究越来越重视, 其中一些项目具有政府和军方资助背景, 相比之下, 我国在这方面的重视程度还远远不够, 这将使我国的 BDS 在民用安全和军事导航对抗方面处于极其被动的处境, 这一严峻形势亟需引起国内相关主管部门和科研工作者的重视.

GNSS 抗欺骗干扰技术是当前国内外卫星导航领域研究的热点问题, 因其兼具较高的理论创新价值和工程应用背景, 吸引了越来越多的科研工作者投入到该方面的研究. 抗欺骗干扰方法一般并不具有普适性^[10], 而欺骗干扰模式灵活多变的特点决定了抗欺骗干扰方法的多样性, 这是欺骗干扰区别于压制干扰的另一个重要特点.

总体来看, 目前针对抗欺骗干扰技术的研究已经取得了不少有益的成果, 但远未完善, 尚有许多问题没有得到较好的解决. 作者在消化、吸收和借鉴国内外主要代表性成果的基础上, 并结合近几年所在研究团队在该领域的研究积累, 对抗欺骗干扰技术的发展趋势总结如下:

(1) 注重欺骗干扰方法的研究, 促进抗欺骗干扰方法的革新. 欺骗与抗欺骗之间是“矛”与“盾”的关系, 过去更多地是针对抗欺骗干扰方法的研究, 而对欺骗干扰总习惯于假设欺骗干扰是某一种模式, 并没有充分考虑欺骗干扰灵活多变的特点; 现在必须重视对欺骗干扰的研究, 否则, 一旦对方新的欺骗干扰模式对己方实施攻击, 之前的欺骗防护手段很可能失效. 结合欺骗干扰与抗欺骗干扰的攻防辩证关系, 研究欺骗干扰技术, 以进一步促进抗欺骗干扰技术的革新.

(2) 抗欺骗方法的可靠性、稳定性仍需进一步增强. 欺骗干扰有其独有的特点, 也有与噪声、压制干扰、多径等因素相似的特点, 当前针对欺骗干扰的检测算法可靠性和稳定性仍需进一步提高, 例如噪声水平检测等检测方法并不能完全确定一定是由欺骗干扰引起的. 多径信号存在的情况与欺骗干扰信号存在的情况具有高度的相似性, 很容易造成判别模糊, 且一些抗多径算法很有可能与当前的抗欺骗算法有冲突, 甚至有可能造成把真实信号当成多径信号消除掉. 这些问题都是亟需解决的难点问题.

(3) 欺骗干扰抑制、消除技术, 乃至欺骗干扰反向跟踪技术的研究. 欺骗干扰的第一目标是使得用户机得到虚假的位置、速度、时间等信息, 那么识别出欺骗相当于粉碎了欺骗干扰的第一企图, 但有些时候并无其他可靠导航手段的情况下如何有效抑制欺骗干扰便显得很有必要. 当前针对抗欺骗干扰技术的研究基本上属于欺骗检测的范畴, 而鲜有欺骗干扰抑制方面的研究. 另一方面最好的防守是进攻, 对于欺骗干扰的反向定位研究也是未来值得研究的方向.

(4) 天线阵技术等方面技术的融合. 天线阵技术在 GNSS 抗压制干扰领域发挥着重要而对作用, 但其在欺骗干扰防护方面研究还不多, 相比其他抗干扰技术天线阵技术有重要的优势. 有理由相信天线

5) Hu Y F, Bian S F, Ji B. GNSS spoofing detection technique using fraction parts of double-difference carrier phases. J Navigation, 2016 (under revision)

6) Hu Y F, Bian S F. GNSS spoofing detection based on new signal quality assessment model. GPS Solut, 2016, (minor revision)

阵技术在欺骗干扰检测和欺骗干扰抑制乃至欺骗干扰反向定位方面均可发挥重要的作用,这可以作为未来研究抗欺骗干扰技术的一个重要的方面。此外,研究欺骗干扰防护技术可以根据 GNSS 具体应用领域的不同,融合滤波理论等理论,这些都可能衍生出新的更可靠、实用的欺骗防护技术。

致谢 本文的写作得到了李忠美博士、陈成博士等同志的帮助,在此向他们表示感谢!感谢评审专家提出的宝贵意见和建议,这些建议十分有益于作者对本文进一步地修改和完善,并对后续研究工作提供重要指导和帮助。

参考文献

- 1 Yang Y X. Progress, contribution and challenges of compass/Beidou satellite navigation system. *Acta Geod Cartogr Sin*, 2010, 39: 1–6 [杨元喜. 北斗卫星导航系统的进展, 贡献与挑战. *测绘学报*, 2010, 39: 1–6]
- 2 Tan S S, Zhou B, Guo S T, et al. Studies of compass navigation signals design. *Sci Sin Phys, Mech & Astron*, 2010, 40: 514–519 [谭述森, 周兵, 郭盛桃, 等. 我国全球卫星导航信号设计研究. *中国科学: 物理学 力学 天文学*, 2010, 40: 514–519]
- 3 Liu J N, Liu H. Continuous operational reference system — infrastructure of urban spatial data. *Geom Inform Sci Wuhan Univ*, 2003, 28: 259–264 [刘经南, 刘晖. 连续运行卫星定位服务系统 —— 城市空间数据的基础设施. *武汉大学学报: 信息科学版*, 2003, 28: 259–264]
- 4 Lv G N, Yuan L W, Yu Z Y. Challenges to development and socialization of GIS technology. *Geo-Inf Sci*, 2013, 15: 483–490 [闰国年, 袁林旺, 俞肇元. GIS 技术发展与社会化的困境与挑战. *地球信息科学学报*, 2013, 15: 483–490]
- 5 Li W Q, Fu X, Wang W Y, et al. Application of BeiDou 2nd generation satellite navigation system in marine data buoy supervision and management. *Shandong Sci*, 2012, 25: 21–26 [李文庆, 付晓, 王文彦, 等. 北斗二代卫星导航系统在海洋资料浮标监控与管理中的应用. *山东科学*, 2012, 25: 21–26]
- 6 Liang J B, Deng Y R, Guo L J, et al. Research and application of remote monitoring for power transmission and transformation facilities based on satellite internet of things. *Electric Pow Construct*, 2013, 34: 6–9 [梁俊斌, 邓雨荣, 郭丽娟, 等. 基于卫星物联网的输变电设施远程监控研究与应用. *电力建设*, 2013, 34: 6–9]
- 7 Wang L, Zhang Q, Huang G W, et al. Experiment results and analysis of landslide monitoring by using GPS PPP technology. *Rock Soil Mech*, 2014, 35: 2118–2124 [王利, 张勤, 黄观文, 等. GPS PPP 技术用于滑坡监测的试验与结果分析. *岩土力学*, 2014, 35: 2118–2124]
- 8 Humphreys T E, Ledvina B M, Psiaki M L, et al. Assessing the spoofing threat: development of a portable GPS civilian spoofer. In: *Proceedings of the Institute of Navigation GNSS*, Georgia, 2008. 2314–2325
- 9 Shepard D P, Humphreys T E, Fansler A A. Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks. *Int J Crit Infrastruct Prot*, 2012, 5: 146–153
- 10 Psiaki M L, Humphreys T E. GNSS spoofing and detection. *Proc IEEE*, 2016, 104: 1258–1270
- 11 Seo S H, Lee B H, Im S H, et al. Effect of spoofing on unmanned aerial vehicle using counterfeited GPS signal. *J Posit Nav Tim*, 2015, 4: 57–65
- 12 Baziar A R, Moazedi M, Mosavi M R. Analysis of single frequency GPS receiver under delay and combining spoofing algorithm. *Wir Pers Commun*, 2015, 83: 1955–1970
- 13 Volpe J. Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System: Final Report. National Transportation Systems Center. 2001
- 14 Scott L. Anti-spoofing & authenticated signal architectures for civil navigation systems. In: *Proceedings of the 16th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GPS/GNSS 2003)*, Oregon, 2003. 1543–1552
- 15 Wesson K D, Rothlisberger M P, Humphreys T E. A proposed navigation message authentication implementation for civil GPS anti-spoofing. In: *Proceedings of the 24th International Technical Meeting of the Satellite Division of the Institute of Navigation*, Oregon, 2011. 20–23
- 16 Wesson K D, Rothlisberger M P, Humphreys T. Practical cryptographic civil GPS signal authentication. *Navigation*, 2012, 59: 177–193
- 17 Wesson K D, Shepard D, Humphreys T. Straight talk on anti-spoofing. *GPS World*, 2012, 23: 32–39

- 18 Kerns A J, Wesson K D, Humphreys T. A blueprint for civil GPS navigation message authentication. In: Proceedings of Position, Location and Navigation Symposium-PLANS, California, 2014. 262–269
- 19 Kuhn M G. An Asymmetric Security Mechanism for Navigation Signals. Heidelberg: Springer-Verlag, 2005: 239–252
- 20 Psiaki M L, O'Hanlon B W, Bhatti J, et al. GPS spoofing detection via dual-receiver correlation of military signals. IEEE Trans Aero Elec Sys, 2013, 49: 2250–2267
- 21 O'Hanlon B W, Psiaki M L, Humphreys T E, et al. Real-time spoofing detection in a narrow-band civil GPS receiver. In: Proceedings of the 23rd International Technical Meeting of the Satellite Division of the Institute of Navigation, Oregon, 2010: 21–24
- 22 O'Hanlon B W, Psiaki M L, Humphreys T E, et al. Real-time spoofing detection using correlation between two civil GPS receiver. In: Proceedings of the 25th International Technical Meeting of the Satellite Division of the Institute of Navigation, Tennessee, 2012: 3584–3590
- 23 O'Hanlon B W, Psiaki M L, Bhatti J A, et al. Real-time GPS spoofing detection via correlation of encrypted signals. Navigation, 2013, 60: 267–278
- 24 Dehghanian V, Nielsen J, Lachapelle G. GNSS spoofing detection based on signal power measurements: statistical analysis. Int J Nav Observ, 2012: 313527
- 25 Dehghanian V, Nielsen J, Lachapelle G. GNSS spoofing detection based on receiver C/N0 estimates. In: Proceedings of the 25th International Technical Meeting of the Satellite Division of the Institute of Navigation, Tennessee, 2012: 2878–2884
- 26 Jafarnia-Jahromi A, Broumandan A, Nielsen J, et al. GPS spoofer countermeasure effectiveness based on signal strength, noise power, and C/N0 measurements. Int J Satell Commun Network, 2012, 30: 181–191
- 27 Akos D M. Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC). Navigation, 2012, 59: 281–290
- 28 Jafarnia-Jahromi A, Daneshmand S, Broumandan A, et al. PVT solution authentication based on monitoring the clock state for a moving GNSS receiver. In: Proceedings of the European Navigation Conference, Vienna, 2013. 1–11
- 29 Broumandan A, Jafarnia-Jahromi A, Dehghanian V, et al. GNSS spoofing detection in handheld receivers based on signal spatial correlation. In: Proceedings of the Position Location and Navigation Symposium, South Carolina, 2012. 479–487
- 30 Xie G. Principles of GPS and Receiver Design. Beijing: Publishing House of Electronics Industry, 2009. 321–322 [谢钢. GPS 原理与接收机设计. 北京: 电子工业出版社, 2009. 321–322]
- 31 Jafarnia-Jahromi A, Lin T, Broumandan A, et al. Detection and mitigation of spoofing attacks on a vector-based tracking GPS receiver. In: Proceedings of the 2012 International Technical Meeting of the Institute of Navigation, California, 2012. 790–800
- 32 Psiaki M L, Powell S P, O'Hanlon B W. GNSS spoofing detection: correlating carrier phase with rapid antenna motion. GPS World, 2013, 24: 53–58
- 33 Psiaki M L, O'Hanlon B W, Powell S P, et al. GNSS spoofing detection using two-antenna differential carrier phase. In: Proceedings of the 27th International Technical Meeting of the Satellite Division of the Institute of Navigation, Florida, 2014: 2776–2800
- 34 Lim S, Lim D W, Chun S, et al. Design and performance evaluation of GPS spoofing signal detection algorithm at RF spoofing simulation environment. J Position Nav Tim, 2015, 4: 173–180
- 35 Bardout Y. Authentication of GNSS position: an assessment of spoofing detection methods. In: Proceedings of the 24th International Technical Meeting of the Satellite Division of the Institute of Navigation, Oregon, 2011. 436–446
- 36 Hwang P Y, McGraw G. Receiver Autonomous Signal Authentication (RASA) based on clock stability analysis. In: Proceedings of Position, Location and Navigation Symposium-PLANS, California, 2014. 270–281
- 37 Khanafseh S, Roshan N, Langel S, et al. GPS spoofing detection using RAIM with INS coupling. In: Proceedings of Position, Location and Navigation Symposium-PLANS, California, 2014. 1232–1239
- 38 Lee J, Kwon D, An D, et al. GPS spoofing detection using accelerometers and performance analysis with probability of detection. Int J Contr Autom Syst, 2015, 13: 951–959
- 39 Yang J S, Zeng F L, Sheng H, et al. A jamming system through section mapping for GPS navigation. Acta Elec Sinic, 2005, 33: 1036–1038 [杨景曙, 曾芳玲, 盛琥, 等. 通过区域映射实现诱导的 GPS 干扰系统. 电子学报, 2005, 33: 1036–1038]

- 40 Zhang S, Yang J S, Pan G F, et al. GPS inducing jamming system through a single transmitter. *Modern Radar*, 2010, 32: 19–26 [张颂, 杨景曙, 潘高峰, 等. 通过单站转发实现诱导的 GPS 干扰系统. *现代雷达*, 2010, 32: 19–26]
- 41 Yan Z J, Wu D W, Liu H B, et al. Analysis of time-delay in GPS repeater deception jamming. *J Air Forc Eng Univ (Natural Science Edition)*, 2013, 14: 67–70 [闫占杰, 吴德伟, 刘海波, 等. GPS 转发欺骗式干扰时延分析. *空军工程大学学报 (自然科学版)*, 2013, 14: 67–70]
- 42 Zhang H S, Gao G G, Kou L, et al. Deceptive jamming technology of GPS based on the track induction method. *J Project Rock Miss Guid*, 2013, 33: 149–152 [张会锁, 高关根, 寇磊, 等. 利用轨迹诱导的欺骗式 GPS 干扰技术研究. *弹箭与制导学报*, 2013, 33: 149–152]
- 43 Zhou X, Li G X, Cai D B, et al. GNSS anti-spoofing techniques: review and prospect. In: *Proceedings of China Satellite Navigation Conference, Wuhan, 2013* [周轩, 李广侠, 蔡锭波, 等. 卫星导航系统反欺骗技术: 回顾与展望. 第四届中国卫星导航学术年会, 武汉, 2013]
- 44 Lv H L, Zhai J Y, Wang W. The spoofing threat and anti-spoofing measurements analysis for satellite navigation. In: *Proceedings of China Satellite Navigation Conference, Wuhan, 2013* [吕红丽, 翟建勇, 王伟. 卫导接收机欺骗干扰威胁和反欺骗措施分析. 第四届中国卫星导航学术年会, 武汉, 2013]
- 45 Li S H, Liu Y, Zhang H S, et al. Inertial measurements aided GNSS spoofing detection technique. *J Chin Inert Tech*, 2013, 21: 336–340 [李四海, 刘洋, 张会锁, 等. 惯性信息辅助的卫星导航欺骗检测技术. *中国惯性技术学报*, 2013, 21: 336–340]
- 46 Sun M H, Wang H Q, Zhang H, et al. Performance analysis of maximum likelihood detection for satellite navigation receiver anti-spoofing. *Sci Sin Inform*, 2014, 44: 1048–1058 [孙闽红, 王海泉, 张茜, 等. 卫星导航接收机抗欺骗干扰极大似然检测性能分析. *中国科学: 信息科学*, 2014, 44: 1048–1058]
- 47 Tang C, Sun X Y, Ji Y F. Research on GNSS civil navigation message encryption and authentication technology. *Comput Simul*, 2015, 32: 86–90 [唐超, 孙希延, 纪元法, 等. GNSS 民用导航电文加密认证技术研究. *计算机仿真*, 2015, 32: 86–90]
- 48 Liang H, Work D B, Gao G X. Cooperative GNSS authentication: reliability from unreliable peers. *Inside GNSS*, 2013, 8: 70–75
- 49 Liang H, Work D B, Gao G X. GPS signal authentication from cooperative peers. *IEEE Trans Intell Transp Syst*, 2014, 16: 1–12
- 50 Huang L, Tang X M, Wang F X. Anti-spoofing techniques for GNSS receiver. *Geom Inform Sci Wuhan Univ*, 2011, 36: 1344–1347 [黄龙, 唐小妹, 王飞雪. 卫星导航接收机抗欺骗干扰方法研究. *武汉大学学报: 信息科学版*, 2011, 36: 1344–1347]
- 51 Huang L, Lv Z C, Wang F X. Spoofing pattern research on GNSS receivers. *J Astron*, 2012, 33: 884–890 [黄龙, 吕志成, 王飞雪. 针对卫星导航接收机的欺骗干扰研究. *宇航学报*, 2012, 33: 884–890]
- 52 Huang L, Gong H, Zhu X W, et al. Research of re-radiating spoofing technique to GNSS timing receiver. *J Nation Univ Def Tech*, 2013, 35: 93–96 [黄龙, 龚航, 朱祥维, 等. 针对 GNSS 授时接收机的转发式欺骗干扰技术研究. *国防科技大学学报*, 2013, 35: 93–96]
- 53 Zhu X W, Wu Y W, Gong H, et al. GNSS timing receiver toughen technique in complicated jamming environments. *J Nation Univ Def Tech*, 2015, 37: 1–9 [朱祥维, 伍贻威, 龚航, 等. 复杂干扰环境下的卫星授时接收机加固技术. *国防科技大学学报*, 2015, 37: 1–9]
- 54 Hu Y F, Cao K J, Li B, et al. Repeater deception jamming research on clock error compensation algorithm. In: *Proceedings of China Satellite Navigation Conference, Nanjing, 2014* [胡彦逢, 曹可劲, 李豹, 朱银兵. 转发式欺骗干扰钟差补偿算法研究. 第五届中国卫星导航学术年会, 南京, 2014]
- 55 Hu Y F. Research on GNSS spoofing technology. Dissertation for Master Degree. Wuhan: Naval University of Engineering, 2014 [胡彦逢. 卫星导航欺骗式干扰技术研究. 硕士学位论文. 武汉: 海军工程大学, 2014]
- 56 Wang H Y, Yao Z C, Fan Z L, et al. A negative time-delay correction method for repeater deception jamming signal. *Telecommun Eng*, 2015, 55: 1255–1259 [王海洋, 姚志成, 范志良, 等. 一种针对转发式欺骗干扰信号的负延时补偿方法. *电讯技术*, 2015, 55: 1255–1259]
- 57 Yao L H, Geng Z L, Nie J W, et al. The characteristics of single antenna repeater jamming coordinates mappings. *GNSS World Chi*, 2015, 40: 19–24 [姚李昊, 耿正霖, 苏映雪, 等. 对单天线转发式欺骗干扰坐标系映射特性分析. *全球定位系统*, 2015, 40: 19–24]
- 58 Hu Y F, Cao K J, Bian S F, et al. GNSS spoofing detection algorithm based on clock frequency drift monitoring. *Syst*

- Eng Elect, 2015, 37: 1629–1632 [胡彦逢, 曹可劲, 边少锋, 等. 基于时钟频漂检验的卫星导航欺骗识别算法. 系统工程与电子技术, 2015, 37: 1629–1632]
- 59 Hu Y F, Bian S F, Cao K J. Spoofing power control strategy for GNSS receiver. J Chi Inertial Tech, 2015, 23: 207–210 [胡彦逢, 边少锋, 曹可劲, 等. GNSS 接收机欺骗干扰功率控制策略. 中国惯性技术学报, 2015, 23: 207–210]
- 60 Yao L H, Chen F Q, Nie J W, et al. The spoofing detection method based on single node doppler velocimetry. GNSS World Chi, 2015, 40: 6–10 [姚李昊, 陈飞强, 聂俊伟, 等. 基于多普勒测速的单节点欺骗检测方法研究. 全球定位系统, 2015, 40: 6–10]
- 61 Zhao L W, Miao Z M, Zhang B J, et al. A novel spoofing attack detection method in satellite navigation tracking phase. J Astron, 2015, 36: 1172–1177 [赵陆文, 缪志敏, 张北江, 等. 一种新的卫星导航跟踪段欺骗攻击检测方法. 宇航学报, 2015, 36: 1172–1177]
- 62 Li Y N, Yu B G, Gan X L. Research on anti-spoofing technology for navigation satellite receive. Rad Eng Chi, 2016, 46: 49–53 [李雅宁, 蔚保国, 甘兴利. 卫星导航接收端反电子欺骗技术比较研究. 无线电工程, 2016, 46: 49–53]
- 63 Peng X K. Spoofing jamming detection technology research on Beidou navigation receiver. Dissertation for Master Degree. Wuhan: Naval University of Engineering, 2015 [彭煊坤. 北斗导航接收机欺骗式干扰检测技术研究. 硕士学位论文. 武汉: 海军工程大学, 2015]
- 64 Li S L. Feasibility research on Beidou spoofing jamming technology under the condition of navigation countermeasures. Dissertation for Master Degree. Wuhan: Naval University of Engineering, 2016 [李松林. 导航对抗条件下北斗欺骗干扰可行性研究. 硕士学位论文. 武汉: 海军工程大学, 2016]

Research status and prospect of GNSS anti-spoofing technology

Shaofeng BIAN, Yanfeng HU* & Bing JI

Department of Navigation Engineering, Naval University of Engineering, Wuhan 430033, China

* Corresponding author. E-mail: daohang-yanfeng@163.com

Abstract With the increasing complexity of the electromagnetic environment and the increasing intensity of military confrontations, the potential security exposure in applications of satellite navigation has become a serious concern. Traditional GNSS anti-interference technology generally focuses on eliminating the jamming interference, while providing comparatively less attention to the elimination of spoofing interference. However, the potential risk induced by spoofing interference is no less than that caused by jamming interference. This paper first gives a broad overview of the research background on anti-spoofing technology, including the concept, theory, application cases, etc. Then it concludes and summarizes the research status of GNSS anti-spoofing technology in depth. Finally, it expounds emphatically some viewpoints on the prospect of GNSS anti-spoofing technology.

Keywords global navigation satellite system (GNSS), receiver, spoofing, anti-spoofing

Shaofeng BIAN was born in 1961. He received his Ph.D. degree from Wuhan Technical University of Surveying and Mapping in 1992. He was awarded the Alexander von Humboldt Research Fellowship, in 1996. He was founded by the National Science Foundation for Distinguished Young Scholars, in 2001. Currently, he is a professor in the Department of Navigation Engineering, Naval University of Engineering. His research interests include GNSS technology, gravity aided navigation, and map projection transformation.

Yanfeng HU was born in 1990. He received the B.S. degree in Radar Engineering and M.S. degree in Navigation, Guidance, and Control from the Naval University of Engineering, Wuhan, China, in 2012 and 2014, respectively. Currently, he is a doctoral student in the Department of Navigation Engineering, Naval University of Engineering. His research interests include GNSS spoofing and anti-spoofing technology.

Bing JI was born in 1978. He received the M.S. degree from the PLA Information Engineering University in 2005 and Ph.D. degree from Naval University of Engineering, in 2011. Currently, he is a lecturer in the Department of Navigation Engineering, Naval University of Engineering. His research interests include GNSS technology and underwater

matching navigation.