doi:10.11887/j.cn.201503001 http://journal.nudt.edu.cn

复杂干扰环境下的卫星授时接收机加固技术*

朱祥维,伍贻威,龚 航,刘文祥,王飞雪
(国防科技大学 电子科学与工程学院,湖南 长沙 410073)

摘 要:对目前导航卫星授时接收机面临的干扰模型和应对措施进行了归纳总结。结合授时接收机工作原理和特点,给出了授时接收机加固的通用框架。在此基础上,对授时接收机加固技术的发展趋势进行了分析,提出了基于钟差辅助和网络辅助的两种干扰检测方法。前者充分利用了多系统多卫星钟差数据的冗余性和本地时钟的特性,后者则利用了授时接收机网络具备数据通信和广域覆盖的特点。通过干扰检测结果给出完好性评估并引导授时接收机的工作模式,可以提升复杂干扰环境下卫星授时的可靠性和完好性。

关键词:卫星导航;干扰;欺骗;授时接收机;干扰监测;欺骗检测
中图分类号:TN967.1 **文献标志码**:A **文章编号**:1001-2486(2015)03-001-09

GNSS timing receiver toughen technique in complicated jamming environments

ZHU Xiangwei, *WU Yiwei*, *GONG Hang*, *LIU Wenxiang*, *WANG Feixue*
(College of Electronic Science and Engineering, National University of Defense Technology, Changsha 410073, China)

Abstract: The threat models and spoofing attack detection technology about navigation satellite timing receiver were summarized. Combined with the operating principle and characteristics of timing receiver, a general framework of timing receiver reinforcement technology was presented. On this basis, two interference detection methods of clock aided method and network aided method were proposed according to the analysis of development tendency of timing receiver reinforcement technology. The former took the advantage of multi satellite clock difference redundancy and the local clock characteristics, while the latter took the advantage of the GNSS timing receiver network with the characteristics of data communication and wide coverage. The interference detection results can be used to integrity assessment and guide the GNSS timing receiver working mode, thus improving the satellite timing reliability and integrity in complicated interference environment.

Key words: satellite navigation; interference; spoofing; timing receiver; interference monitoring; spoofing detection

GPS等卫星导航系统出现以后,在军事和民用领域都产生了革命性的影响。基于卫星的定位、导航和授时(Positioning, Navigation and Timing,PNT)设备广泛应用于国民经济各个行业。然而卫星信号有先天的脆弱性,易受阻挡、干扰,甚至欺骗。有报道指出,一个价值29美元的设备就可以对GPS信号进行阻塞甚至欺骗[1]。2008年英国政府测试使用两个低成本干扰器阻塞了北海三十公里范围内的GPS信号[2]。

2011年12月4日,伊朗防空部队俘获了一架美国"RQ-170"无人侦察机。据称当时重构了这架无人机的GPS坐标,使其降落在了伊朗境内[3]。2012年6月,Humphreys教授团队利用硬件成本不到1000美元的欺骗干扰生成设备,控制利用GPS民用信号导航的无人机俯冲接近地面后又拉升[4]。文献[5]也介绍了通过欺骗手段俘获和控制无人机的方法。文献[6]指出,一个欺骗干扰攻击可能导致电力网络中的电机跳脱。这些实验有效地证明了民用GPS信号的脆弱性和安全隐患。

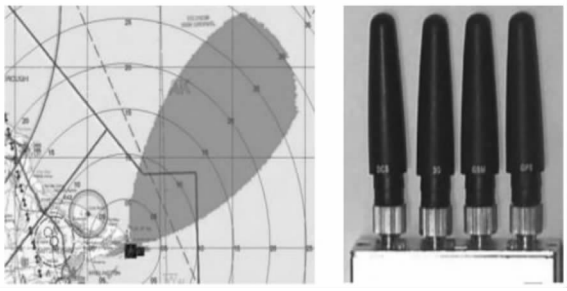

图1 GPS干扰器的作用范围
Fig. 1 The working scope of GPS jammer

* **收稿日期**:2015-03-27
基金项目:国家自然科学基金资助项目(61403413)
作者简介:朱祥维(1980—),男,山东日照人,副研究员,博士,E-mail:zhuxiangwei@nudt.edu.cn

而如何解决全球导航卫星系统(Global Navigation Satellite System,GNSS)应用中PNT服务的可靠性和可信度,提升服务的完好性已经成为迫在眉睫的任务。2014年,GPS之父Parkinson提出了防护加固与增强(Protect Toughen and Augment,PTA) GPS框架[7]。

1　干扰类型及特点

复杂电磁环境下,GNSS卫星授时接收机面临的干扰可分为三类:自然环境的干扰、压制式干扰和欺骗式干扰。

1.1　自然环境的干扰

这类干扰往往是无意的干扰,没有明显的针对接收机的干扰或攻击意图。当接收机处于复杂电磁环境中的时候,遭受这类干扰的可能性很大。自然环境的干扰主要可以分为如下几类[8-9]:

1)带内射频干扰。对于GPS接收机来说,这里的带内是指介于1565~1585MHz之间的频带。带内射频干扰包括谐波、寄生振荡和交叉调制分量等。

2)带外射频干扰。带外射频干扰主要是靠近GPS载波频率的强信号干扰,它可以通过接收机的射频滤波器对接收机造成影响。

3)其他环境干扰。环境干扰包括反射多径、地形遮拦和其他由自然环境造成的干扰。

1.2　压制式干扰攻击

用干扰机发射干扰信号,以某种方式遮蔽GNSS信号频谱,使敌方GNSS接收机降低或完全失去正常工作能力,称为压制式干扰。主要包括[10]:

1)瞄准式干扰。GNSS卫星信号有其独特的码型,采用频率瞄准技术,使干扰载频精确对准信号载频,针对特定码型的卫星信号实施干扰,使该信号在一定区域内失效。

2)阻塞式干扰。这种干扰的特点是针对GNSS信号的载频采用一部干扰机扰乱该地域出现的所有卫星信号,并且存在多种干扰体制,干扰效果不尽相同,其中干扰效果比较好的是宽带均匀频谱干扰体制。

3)相关式干扰。相关干扰是利用干扰信号的码序列与GNSS信号的伪码序列有较强的相关性这一特点实施干扰。与不相关干扰相比,它有较多的能量可以通过接收机窄带滤波器。因而,可以以较小的功率实现与其他方式相当的干扰效果。

根据干扰的样式又可以分为:脉冲干扰和连续波干扰两大类。其中脉冲干扰包括单频脉冲、线性调频脉冲等;连续波干扰包括扫频干扰、单频干扰、窄带干扰和宽带干扰等,如图2所示。

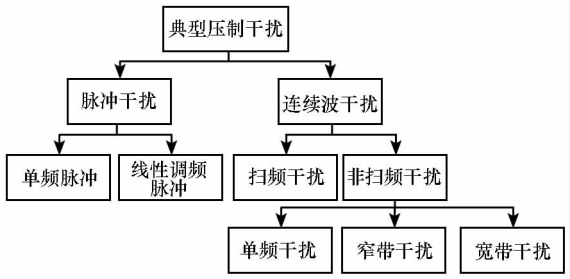

图2　典型压制干扰分类

Fig. 2　Classification of GPS suppression interference

1.3　欺骗式干扰攻击

欺骗式干扰是指发射与GNSS信号具有相同参数的假信号,使GNSS接收机产生错误的定位/授时信息[11]。欺骗干扰攻击比压制式干扰可能更具危害性,因为欺骗攻击甚至不会使接收机产生任何错误警报,这可能会给系统带来较长时间的危害。

欺骗干扰的过程一般分为两个步骤,即干扰信号的产生和干扰信号的发射。欺骗干扰信号的产生方式主要可分为两类:生成式干扰和转发式干扰[12]。

1)生成式干扰。这种干扰方式将自身产生的信号直接发射给接收机,使其产生错误的解算位置,达到欺骗的目的。其优点是导航信号和发射时间都由自身灵活决定,可以滞后或提前信号的发射,还可以在导航电文中给出错误的位置信息。其缺点是需要了解信号和导航电文的结构,难以对军用信号实施干扰。

2)转发式干扰。这种干扰设备通过自己的天线接收真实的卫星信号,经过适当的延迟处理后再发射给干扰区域内的接收机。该方法不需要知道信号的伪随机码,可以对军用信号进行干扰。但是,相对于生成式干扰,转发式干扰的灵活性稍差,干扰信号的时延只能大于真实信号的时延,其欺骗只能通过改变伪距的方式来实现[13]。特别针对卫星授时的转发式干扰,可以参见文献[14]。

根据欺骗干扰的发射方式,可以分为两大类:单天线发射和多天线发射[14]。

1)单天线发射。单天线发射在信号发射之前不对信号进行分离,而是直接发射或转发出去。这样,通过单天线发射的信号一般是多颗卫星信号的叠加,目标接收机容易检测到这些信号具有相同的到达角,因此这种欺骗方式容易被接收机识破。

2)多天线发射。多天线发射通过不同的天线发射来自不同卫星的欺骗干扰,可以独立调节

各个信号的时延,对欺骗过程有较强的可控性。但这种方式对硬件的要求比较高,需要实现信号的分离,对离散分布的天线还需要较长的线路来实现互联和控制。

容易发现,上述干扰方式经过组合可以形成四种欺骗式干扰方案,即生成式单天线欺骗干扰,生成式多天线欺骗干扰,转发式单天线欺骗干扰和转发式多天线欺骗干扰。

1.4　小结

由卫星授时和定位原理可知,GNSS 正确授时与定位主要依赖于两个条件:一是正确地测量来自至少四颗卫星的伪距;二是获得有效的导航电文。由前文考虑的干扰样式可知,环境干扰、压制式干扰可能造成电文误码率增加、伪距等测量值超差甚至接收机无法工作;欺骗干扰也是从信号测量层和数据电文层两个层面进行伪造和攻击。从干扰产生的机理来看,压制干扰侧重于从能量上攻击,欺骗干扰则更多从信息上攻击。

2　压制干扰监测技术

压制干扰对 GPS 接收的重要影响是降低载噪比(C/N_0)。随着 C/N_0的降低,接收机的码环和载波环的热噪声增加[15-17],使得自动增益控制(Automatic Gain Control,AGC)电平、相关器功率输出、载波相位、伪距及其变化率测量误差增加[18],导致定位授时误差增大。如果 C/N_0将降到接收机的跟踪门限以下,接收机将失去正常工作能力。

2.1　单机层面干扰监测

从接收机结构上可以将干扰监测分为相关前干扰检测和相关后干扰检测。相关前干扰检测主要是通过天线、自动增益控制(Automatic Gain Control,AGC)增益、模数转换器(Analog-to Digital Converter,ADC)以及载噪比等接收机观测量的提取来实现,而相关后干扰检测是通过观测相关器输出功率、相关器输出功率方差等进行。常用方法[17-23]如下。

1)AGC 电平监测。AGC 信号电平会根据跟踪接收有用信号的功率增加量而不断升高,当 AGC 信号电平过高时,其误码率也会增大,原因可能是同频干扰信号的影响。在输入信号功率接近正常接收门限值时,接收机的正常锁定动作不能完成,则表明接收机遭受异常干扰。文献[10]针对传统 AGC 的不足,提出了基于限幅比例的大动态 AGC 算法,该算法能够适应不同的干扰类型。

2)误码率监测。利用误码率可有效、直接改善干扰大小及有无的判断效果。对于某一调制系统来说,设备自身出现的解调损失可实时进行测定,通常的信号附加噪声导致的接收信号信噪比恶化量也可以进行估计,因此利用实际接收信号的误码率便可分析计算系统的外部干扰[18]。

3)载噪比监测。若载噪比偏高,但在系统正常工作的门限区域内,同时接受误码率也较高,则可基本推断系统受到外来同频信号干扰;若载噪比小于系统设定接收载噪比值,则可基本推断系统受到宽带噪声干扰[24-25]。

此外,随着现代信号处理技术的发展,还有一些更为复杂的干扰检测方法,比如循环平稳特征检测法、匹配滤波器检测法、极化分析法及时频分析法等。

2.2　系统层面干扰监测

除了上述单机层面的干扰监测方法外,还有一些通过组网来实现 GNSS 干扰监测的系统[26-27]。典型的 GNSS 干扰监测系统有:美国 NAVSYS 公司建设的干扰监测定位系统(Jammer and Interference Location System,JLOC)、美国国家大地测量机构(National Geodetic Survey,NGS)基于连续运行参考站(Continuously Operating Reference Stations,CORS)网络的 GPS 干扰监测系统、中欧地球动力学参考网络(Central Europe Geodynamics Reference Network,CEGRN)建立的 GPS 电磁环境监测系统等[10,28]。这些典型系统一般采用多个独立天线,具有独立的接收通道,多站组合,对特定区域干扰信号进行监测/定位。文献[29]针对航空无线电导航频段(Aeronautical Radio Navigation Service,ARNS),分析了 DME/TACAN 等陆基无线电导航系统对 GPS L5 和 Galileo E5 等新型 GNSS 导航信号的影响。此外,在系统层面实现干扰监测和定位一体化已经成为技术发展趋势[30-31]。

3　欺骗干扰检测技术

根据欺骗检测技术特征的不同,本文将这些技术分为三大类:加密、检验和冗余。其中检验类是通过与已知信息的比对来判断欺骗干扰的存在,又可以细分为三类:检测、校验、辅助。下面分别进行简要介绍。

3.1　信号体制加密[32-34]

信号体制加密指的是采用鉴权的方式在信号格式中插入某些播发前无法让攻击方预知的秘密

信息,用户通过对这些秘密信息的真实性进行判断,来检测所跟踪的信号是否真实。通常包括扩频码加密和电文加密两种方式。民用导航信号可借鉴军用信号的加密方式,在民用信号的导频序列中每隔一段时间加入一段加密序列,使得生成欺骗干扰的成本升高。在目前导航电文中存在的预留字节中加入电文加密认证,使得欺骗干扰者不能自行生成导航电文,同时使得接收机能够通过电文区分欺骗干扰和真实信号。

3.2　信号层参数检测

1)信号功率检测[35-37]。包括绝对功率检测、信号功率变化率检测、相对功率检测和载噪比检测。对接收机来说,欺骗干扰功率往往大于真实信号,这样可以通过设置一个合理的功率上限,可判定为存在欺骗干扰。欺骗干扰源一般位于近地空间,其与接收机的位置变化会产生相对较大的功率变化,则可以通过功率变化率检测欺骗攻击。由于卫星发射的各频点信号功率保持一定比例,通过检测各频点信号的相对功率,也可判定是否存在欺骗攻击。

2)AGC 增益检测[38]。由于卫星导航信号到达地面的功率很低,AGC 的主要作用就是调整接收链路的增益大小。而存在欺骗干扰信号时(转发式欺骗放大真实 GNSS 信号的同时放大了噪声),AGC 增益会快速降低,以此可作为检测欺骗干扰的判据。

3)多普勒检测[37]。由于各颗卫星相对于接收机的运动速度和运动方向不同,因而接收机接收到的真实信号的频率各不相同。若欺骗干扰采用转发式和单天线发射,则难以模拟出各卫星信号的不同载频。

4)频点间互相关检测[32,39]。导航卫星各频点调制相同的 P(Y)码,在剥离载波后,将两频点的 P(Y)码进行互相关,通过检测是否产生相关峰来判断是否存在欺骗干扰。这种方法仅对生成式欺骗干扰有效,因为军码信号是难以伪造的。

5)多天线到达角检测[40-44]。利用接收机的天线阵列可以通过检测所接收各路信号的到达角来检测欺骗干扰:一般而言,实际卫星信号的到达角不会在一段时间完全相同,而由同一干扰台发出的欺骗干扰到达角则基本一致。为了节省实现资源,天线阵也可以通过单天线虚拟形成[44]。

6)伪码/载波速率一致性检测[32]。一般情况下,卫星与接收机之间相对运动是稳定的,因此接收机的码片滑动和多普勒频移变化是一致的。若欺骗设备在码和载波频率上控制不好,则可检测到欺骗带来的异常。

7)残留信号检测[45]。残留信号检测的前提是欺骗干扰信号无法抑制实际信号,可分为捕获阶段的残留信号检测和跟踪阶段的残留信号检测。捕获阶段检测是通过检测载波多普勒-伪码相位二维搜索是否存在两个相关峰,来判定是否存在欺骗干扰。跟踪阶段检测是在接收机锁定真实信号时,针对较复杂的欺骗干扰提出的。

3.3　信息解算层校验

1)星历/历书校验[46-47]。现有导航接收机能够存贮导航卫星星历等信息,此信息在一段时间内保持有效。利用存储星历或历书与当前接收的星历或历书进行校验。如果发现有明显不一致,则说明接收机有可能受到欺骗干扰。

2)电文时钟校验[46-47]。卫星导航接收机收到的卫星导航电文中包含时钟信息,不同卫星的时钟信息应该是保持同步的,在非同步攻击中的电文信息出现时钟信息前后会有突变,以此可作为遭受欺骗攻击的依据。

3)本地时钟及变化率校验[32]。利用静态情况下解算钟差及变化率或单星时差基本保持稳定的特点,当解算出的本地时钟特性发生突变时即可怀疑受到了欺骗干扰。

4)定位解算结果检验[32]。对于坐标位置已知的授时接收机,可以将定位解算结果与已知坐标对比,如果存在较大偏差,则可以认为受到欺骗攻击。

3.4　外部辅助抗欺骗

将卫星导航接收机的解算结果与其他导航定位手段的测量结果对比,如解算结果偏差超出可接受范围,则认为存在被欺骗的可能。

1)与其他导航系统组合[37]。在卫星导航出现之前,地面无线电导航就已广泛应用(罗兰系统、塔康系统等),可比较卫星导航接收机解算结果与地面无线电导航系统测量结果,以确认是否受到欺骗干扰。

2)与惯导单元组合[45,48]。独立式惯导设备不依赖外界信息,可独立地提供多种较高精度的导航参数(位置、速度、姿态),将惯导和卫星导航组合,可以有效地判别导航结果的真实性。对于授时接收机来说,本地频标也可以视为一种“惯性”单元。

3)与实时定位系统结合。随着物联网和移动互联网的发展,实时定位系统(Real Time

Location Systems, RTLS)越来越普及,其中基于 WiFi、RFID、iBeacon 等的定位手段也可以辅助 GNSS 接收机进行欺骗检测[49]。

4)与其他传感器对比。气压高度计、磁罗经、重力仪等传感器可提供一些辅助信息给接收机参考。

3.5　冗余分析抗欺骗

冗余包括多星、多系统、多接收机等多个层面的冗余。

1)接收机自主完好性检测。对于坐标位置未知的接收机,可以采取自主完好性检测(Receiver Autonomous Integrity Monitoring, RAIM)的方法[50]。基本原理即通过选取接收到的 5 颗卫星信号中任意 4 颗解算接收机当前位置,通过比较 5 次的解算结果,若存在很大差异,说明存在欺骗干扰。这种方法在欺骗干扰较少的时候可行,如果欺骗攻击(例如单天线发射)同时欺骗所有信号,就限制了 RAIM 的使用。

2)多接收机间伪码相关性[51-55]。如果两台接收机正同时接收来自一颗卫星的 GNSS 信号,它们会收到一段相同的伪码,两者会产生一个互相关峰。如果没有产生互相关峰,则证明受到了攻击。相对于民码来说,利用军码更加可靠[51-52]。当然,如果两台接收机受到来自同一个攻击者的攻击,则仍然会产生互相关峰,为此,可以考虑距离较远的两台甚至多台接收机[52-55]。

3)多接收机的矢量跟踪回路[56-58]。该方法利用了多个装置的接收机的位置信息,不但能更好地检测出压制干扰和欺骗攻击,而且能有效地进行故障检测;缺陷是需要传输基带数据,计算量比较大。文献[56]对该策略做了验证实验,结果表明该策略能够降低干扰存在情况下的授时误差。

4)多接收机间电文交叉检测[59-60]。通过对多台接收机电文的交叉检测,容易检测出数据级的攻击和接收机故障。对压制干扰攻击也有一定效果。

3.6　小结

对上文的欺骗干扰检测方法进行归纳总结,其结果如表 1 所示。

4　授时接收机加固方法

对于电力、通信、金融等对授时和同步可靠性要求非常高的系统来说,一旦受到干扰和攻击,可能导致系统瘫痪,带来巨大的经济损失。下面结合授时接收机的特点,借助干扰检测技术,给出授时接收机加固的技术框架。

表 1　欺骗干扰检测技术对比表

Tab. 1　Spoofing detection techniques comparison

		检测方法	适用范围	所需能力
加密		信号体制加密	欺骗干扰为非密信号	授权解密能力
检验	检测	信号功率检测	欺骗具有更高信噪比	标校过的功率
		AGC 增益检测	欺骗干扰功率大于噪声	标校过的 AGC 增益
		多普勒检测	单天线发射转发式欺骗干扰	卫星多普勒先验值
		频点间互相关检测	对生成式欺骗干扰有效	具备军码接收能力
		多天线到达角检测	欺骗干扰来自同一方向	具备多个接收天线
		伪码/载波一致性检测	欺骗干扰伪码/载波速率不匹配	伪码/载波多普勒测量
		残留信号检测	欺骗干扰信号无法抑制实际信号	附加残留检测通道
	校验	星历/历书校验	伪造星历、历书变化不连续	历书、星历存储
		电文时钟校验	伪造的卫星时钟变化不连续	时钟信息存储
		本地时钟及变化率	静态情况下钟差及变化率保持稳定	接收机频标无跳变
		定位解算结果检验	欺骗未模仿已知坐标位置	接收机位置已知
	辅助	与其他导航系统组合	其他导航系统未受欺骗攻击	具备多系统接收能力
		与惯导单元组合	惯导单元精度与 GNSS 匹配	具备惯性测量单元
		与实时定位系统结合	实时定位系统的精度足够高	具备实时定位系统
		与其他传感器对比	其他传感器结果可靠	具备相应精度传感器
冗余		接收机自主完好性检测	欺骗干扰较少的时候	接收机具备 RAIM 功能
		多接收机间伪码相关性	接收机间距离较远	需要具备通信链路
		多接收机的矢量跟踪回路	欺骗攻击不知道接收机位置	需要传输基带数据
		多接收机间电文交叉检测	电文数据级的攻击	需要传输电文数据

4.1　授时接收机工作原理

卫星授时接收机由天线、射频前端、基带处理和时间生成四部分组成。其中天线完成各频点信号的接收;射频模块对导航射频信号进行变频、AGC 控制等;基带部分又可以分为信号层和数据层,完成信号捕获、跟踪和伪距、载波相位测量,并进行授时/定位解算。时间生成模块根据干扰检测结果选择工作模式。于守时模式工作时,信息处理单元输出的钟差信息无效,接收机时间由本地频标维持。在授时模式工作时,选择最优卫星信号组合和授时方式进行处理得到钟差信息,然后通过驯服滤波模块控制本地频标,进而驱动时频信号和时间信息的生成,工作流程如图 3 所示。

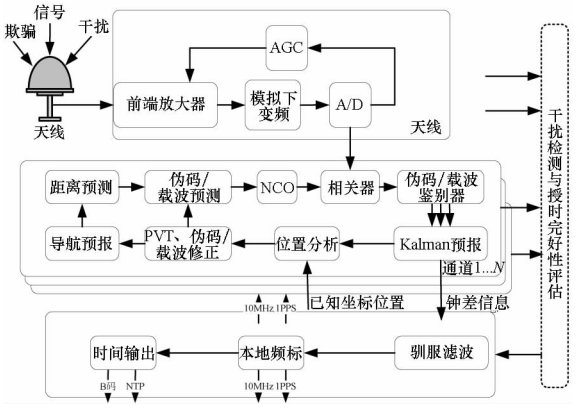

图 3　卫星授时接收机系统框图

Fig. 3　GNSS timing receiver system block diagram

4.2　多层次接收机加固架构

对上文归纳总结的各种干扰检测方法进行分析,可以发现:压制干扰监测方法更多停留在信号参数层面;压制干扰和欺骗干扰的检测都在向系统化、网络化方向发展,通过多站多机来提升检测能力;各种干扰检测方法都有局限性,目前尚未出现可以适用任意干扰攻击的检测技术。

因此,在授时接收机干扰检测方面,需要统筹考虑压制干扰和欺骗攻击,结合已有的干扰检测算法和授时接收机结构,建立一个合理的干扰检测架构。

结合授时接收机的实现结构和处理流程,可以得到攻击检测的四个层次,即信号调理、跟踪环路、导航电文和位置/钟差解算。文献[56]和文献[58]对四个层面的干扰检测技术进行了总结,给出了授时接收机加固的实现架构,如图 4 所示。

接下来简要介绍每一步对策:

C1. 信号功率检查。欺骗攻击的功率往往高于正常的 GNSS 信号,接收信号功率的升高可能意味着欺骗攻击。

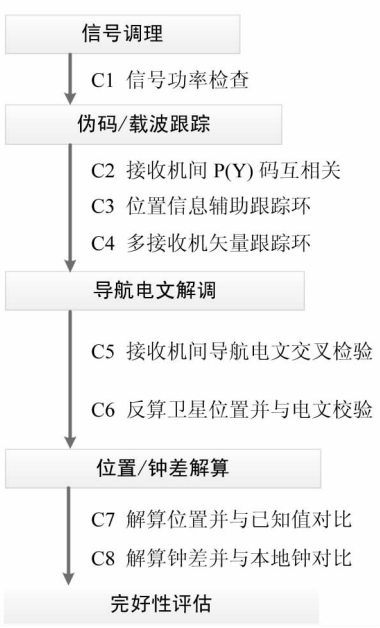

图 4　授时接收机多层加固架构

Fig. 4　Multi-layer toughen architecture of timing receiver

C2. 接收机间 P(Y)码相关性验核。两个接收机接收同一卫星的 P(Y)码没有产生互相关峰,则证明受到了攻击。但是,如果两台接收机受到来自同一个攻击者的攻击,则仍然会产生互相关峰。该方法需要将高速基带采样数据传输至数据网络,代价颇高。

C3. 位置信息辅助跟踪环。利用授时接收机已知的位置信息,可以算出卫星与接收机之间的相对位置与相对速度在视线(Line Of Sight,LOS)方向的投影,以此来预测攻击情况。

C4. 多接收机矢量跟踪环。这个方法利用了多个接收机的位置信息,对信噪比比较低的信号特别适用,缺陷是计算量比较大。

C5. 接收机间导航电文交叉检验。这个方法容易检测出数据级的欺骗攻击,对压制干扰攻击也有一定效果。

C6. 反算卫星位置并与电文校验。由于各接收机的位置固定且已知,可以由多个接收机联立方程组解出卫星的位置,如果与导航数据不匹配,则说明存在攻击。这个方法的精度跟接收机与卫星的相对几何位置有关,建议选择位置较分散的接收机。

C7. 解算位置并与已知值对比。容易发现,对单个接收机来说,这个方法对转发攻击是有效的。因为所考虑的每个接收机拥有其他接收机的位置信息,如果某个接收机发现别的接收机的位

置数据不正确了,便是受到了攻击。

C8. 解算钟差并与本地时钟对比。毕竟欺骗攻击和接收端故障不是经常发生的,可以统计接收端的时钟数据,根据这些数据特征考察新解出的时间值,分析攻击的可能性。文献[58]指出,由于接收机时钟的随机性和易变性,这个方法通常是作为辅助手段。

文献[58]对干扰检测策略与威胁模型的关系进行了归纳,本文对其进行了重新梳理,如表 2 所示。其中星号代表某策略对相应的威胁模型是有效的,空心圈代表某策略只能作为相应威胁模型的辅助检测,实心点则代表某策略对相应的威胁模型是无效的。

表 2　安全加固技术与威胁模型的关系

Tab. 2　Relation between threat model and safety toughen technique

干扰检测方法	威胁模型			
	干扰	生成式欺骗		转发式欺骗
		数据层	信号层	
C1 信号功率检查	●	o	o	o
C2 接收机间相关性验核	●	*	*	●
C3 位置信息辅助跟踪环	*	●	●	*
C4 多接收机矢量跟踪环	*	o	o	o
C5 导航电文交叉检验	o	*	●	●
C6 反算卫星位置并对比	●	o	o	*
C7 解算位置并对比	●	*	*	*
C8 解算钟差并对比	●	o	o	o

4.3　基于钟差辅助的干扰检测

文献[56]和文献[58]对授时接收机的稳健性提出了多层次的稳健性架构,重点是针对信号处理环路方面,特点是充分利用位置信息辅助。这些方法对转发式欺骗效果较差,而且文献[10]针对授时接收机已知位置设计了相应的欺骗攻击,从而使得位置信息辅助失效。其实,充分利用多星多系统间钟差数据特征和数据冗余性,以及接收机本地时钟的特性,是提高授时接收机稳健性的有效措施。

鉴于此,本文提出了一种基于多源钟差数据辅助的干扰检测方法,如图 5 中“钟差数据辅助”模块所示,该方法在信息处理层面充分利用多 GNSS 系统时间偏差关系以及本地频标信息,通过数据融合和最优滤波实现完好性和精度提升。此文,在信号分析方面,充分利用位置信息辅助和多 GNSS 系统之间交叉检验的优势,通过多信号参数检测等实现干扰检测,可以视为文献[56]和文献[58]中位置信息辅助的进一步延伸。

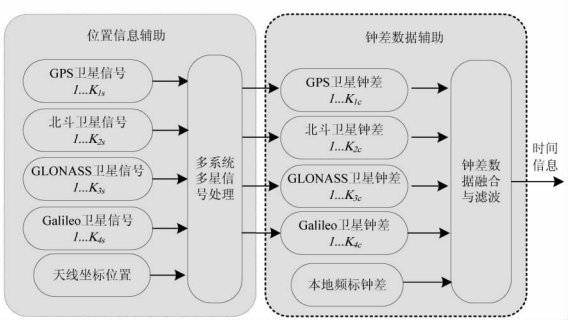

图 5　基于钟差和位置辅助的干扰检测原理框图

Fig. 5　Principle diagram of interference detection based on clock error and position aided

4.4　基于网络辅助的干扰检测

从实施欺骗攻击的难度来说,对同一个区域的接收机实施全方位干扰比对异地多机同时实施干扰要容易得多。文献[56]和文献[58]等提到了利用多个授时接收机的信息进行干扰检测,但是更多停留在接收机之间夹叉检验(比如 C2,C5),其对接收机和传输网络要求较高,接收机之间耦合度较高。

以通信基站授时系统为例,其特点是设备众多、分布较广、单机成本较低且存在数据通道。考虑到授时网络的特点,充分利用多台接收机特别是广域范围内的授时接收机的数据,本文提出一种基于网络辅助、多接收机数据融合的干扰检测方法,如图 6 所示。

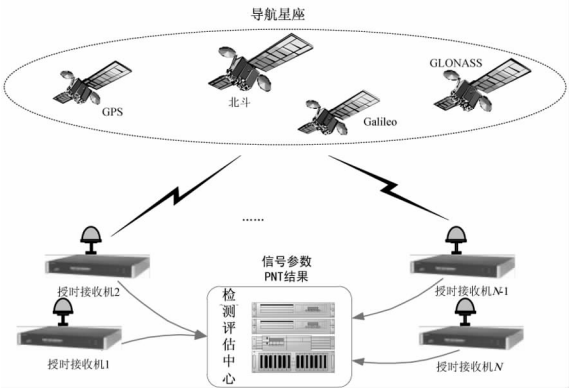

图 6　基于授时网络辅助的干扰检测评估方法

Fig. 6　Interference detection and evaluation method based on the timing receiver network aided

图 6 中的检测评估中心汇总全网范围内各接收机的信号参数和 PNT 解算结果,借助大数据挖掘的思路,通过一定模型算法,可以对欺骗干扰进行检测、评估和定位。毕竟,要实现大面积区域的欺骗干扰是非常困难的。基于网络的干扰检测系统不但可以进行干扰检测评估,还可以支持电磁环境分析、大气探测和地球动力学等研究。

5 结论

通信、电力、金融等系统中的GNSS授时接收机具有普通接收机不具备的特点,包括位置已知、具有本地时钟和多机联网等。这些特点为授时接收机更好地进行干扰检测提供了便利条件。本文对复杂电磁环境下授时接收机面临的干扰和欺骗攻击以及相应的检测策略进行了归纳总结。在充分考虑授时接收机特点和架构基础上,给出了多层次的授时接收机加固架构。在此基础上,考虑充分利用多卫星多系统间钟差数据特征和接收机本地时钟特性,提出了基于多源钟差数据辅助的干扰检测方法;进一步结合通信、电力等授时接收机网络,提出了网络辅助的干扰检测方法,通过对全网接收机信号参数和解算结果的汇总分析与数据挖掘,可以实现对干扰的检测、评估和定位。上述研究成果可为提升复杂干扰环境下GNSS卫星授时的可靠性和完好性提供有力支持。

参考文献(References)

[1] Gould J. Ausa: army seeks new positioning tech[N]. Defense News, 2014, 10:18.

[2] Last D D. GPS: the present imperfect[J]. Inside GNSS, 2010, 05: 60-64.

[3] Giray S M. Anatomy of unmanned aerial vehicle hijacking with signal spoofing[C]//Proceedings of International Conference on Recent Advances in Space Technologies, IEEE, 2013: 795-800.

[4] Shepard D P, Bhatti J A, Humphreys T E, et al. Evaluation of smart grid and civilian UAV vulnerability to GPS spoofing attacks[C]// Proceedings of the 25th International Technical Meeting of the Satellite Division of the Institute of Navigation, 2012: 3591-3605.

[5] Kerns A J, Shepard D P, Bhatti J A, et al. Unmanned aircraft capture and control via GPS spoofing[J]. Journal of Field Robotics, 2014, 31(4): 617-636.

[6] Shepard D P, Humphreys T E, Fansler A A. Going up against time: the power grid's vulnerability to GPS spoofing attacks[J]. GPS World, 2012(8):34-38.

[7] Parkinson B W. Assured PNT for our future: PTA[J]. GPS World, 2014(9):24-31.

[8] 王李军. GPS接收机抗干扰若干关键技术研究[D]. 南京:南京理工大学, 2006.
WANG Lijun. Study on some key techniques of GPS receiver anti-jamming[D]. Nanjing: Nanjing University of Science and Technology, 2006. (in Chinese)

[9] Dovis F, Musumeci L, Linty N, et al. Recent trends in interference mitigation and spoofing detection[J]. International Journal of Embedded and Real-Time Communication Systems, 2012, 3(3): 1-17.

[10] 黄婷. 卫星导航系统压制式干扰监测关键技术研究[D]. 长沙:湖南大学, 2014.
HUANG Ting. The key technology research on blanketing jamming monitoring of satellite navigation system[D]. Changsha: Hunan University, 2014. (in Chinese)

[11] Shepard D. Characterization of receiver response to spoofing attacks[D]. USA: University of Texas at Austin, 2011.

[12] 黄龙, 吕志成, 王飞雪. 针对卫星导航接收机的欺骗干扰研究[J]. 宇航学报, 2012, 33(7): 884-890.
HUANG Long, LYU Zhicheng, WANG Feixue. Spoofing pattern research on GNSS receivers[J]. Journal of Astronautics, 2012, 33(7): 884-890. (in Chinese)

[13] 耿正霖, 聂俊伟, 王飞雪. GNSS抗欺骗干扰技术研究[J]. 全球定位系统, 2013, 38(4): 65-70.
GENG Zhenglin, NIE Junwei, WANG Feixue. Study of GNSS anti-spoofing techniques[J]. GNSS World of China, 2013, 38(4): 65-70. (in Chinese)

[14] 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[J]. 国防科技大学学报, 2013, 35(4): 93-96.
HUANG Long, GONG Hang, ZHU Xiangwei, et al. Research of reradiating spoofing technique to GNSS timing receiver[J]. Journal of National University of Defense Technology, 2013, 35(4): 93-96. (in Chinese)

[15] Balaei A T, Dempster A G, Lo Presti L. Characterization of the effects of CW and pulse CW interference on the GPS signal quality[J]. Aerospace & Electronic Systems IEEE Transactions on, 2009, 45(4): 1418-1431.

[16] Bhuiyan M Z H, Kuusniemi H S, derholm S, et al. The impact of interference on GNSS receiver observables—a running digital sum based simple jammer detector[J]. Radioengineering, 2014, 23(3): 898-906.

[17] Ndili A, Enge P. GPS receiver autonomous interference detection[C]//Proceedings of IEEE Position Location and Navigation Symposium, 1998: 123-130.

[18] 田爱国, 刘志春, 杜黎明,等. GPS干扰监测技术[J]. 全球定位系统, 2008, 33(3): 5-8.
TIAN Aiguo, LIU Zhichun, DU Liming, et al. GPS interference monitoring technique[J]. GNSS World of China, 2008, 33(3): 5-8. (in Chinese)

[19] 韩其位, 曾祥华, 李峥嵘,等. 卫星导航干扰监测技术的发展现状与趋势[J]. 航天电子对抗, 2009, 25(6):17-19.
HAN Qiwei, ZENG Xianghua, Li Zhengrong, et al. Recent development and prospect of interference monitoring for GNSS bands[J]. Aerospace Electronic Warfare, 2009, 25(6):17-19. (in Chinese)

[20] 楚恒林, 李献球. 卫星网络干扰信号的监测与定位技术[J]. 无线电通信技术, 2010, 36(3):48-50.
CHU Henglin, LI Xianqiu. Detection and location technique of satellite network interference signals[J]. Radio Communications Technology, 2010, 36(3):48-50. (in Chinese)

[21] 汪立萍, 张益龙. GPS防护及干扰监测与定位技术研究[J]. 航天电子对抗, 2012,28(6):32-34.
WANG Liping, ZHANG Yilong. GPS protection and technique of interference detection and location[J]. Aerospace Electronic Warfare, 2012, 28(6):32-34. (in Chinese)

[22] 范广伟, 晁磊, 刘莉. 卫星导航干扰监测技术[J]. 四川兵工学报, 2013, 34(6):125-128.
FAN Guangwei, CHAO Lei, LIU Li. Technology of interference monitoring for GNSS[J]. Journal of Sichuan Ordnance, 2013, 34(6):125-128. (in Chinese)

[23] Bastide F, Chatre E, Macabiau C. GPS interference detection and identification using multicorrelator receivers [C]// Proceedings of the 14th International Technical Meeting of the Satellite Division of the Institute of Navigation, 2001: 872 -881.

[24] Balaei A T, Dempster A G, Barnes J. A novel approach in detection and characterization of CW interference of GPS signal using receiver estimation of C/N0[C]// Proceedings of IEEE/ION Position, Location and Navigation Symposium, 2006:1120 -1126.

[25] Balaei A T, Dempster A G. A statistical inference technique for GPS interference detection [J]. IEEE Transactions on Aerospace & Electronic Systems, 2009, 45 (4): 1499 -1511.

[26] Chen L, Han C, Du L, et al. Analysis of GNSS IDM situation and its revelation to us[C]//Proceedings of China Satellite Navigation Conference, Lecture Notes in Electrical Engineering, 2012: 47 -57.

[27] Brown A, Reynolds D, Roberts D, et al. Jammer and interference location[C]//Proceedings of the 12th International Technical Meeting of the Satellite Division of the Institute of Navigation,1999: 137 -142.

[28] Simonsen K, Suycott M, Crumplar R, et al. LOCO GPSI: detection and location of GPS interference/ jamming[C]// Proceedings of the 17th International Technical Meeting of the Satellite Division of the Institute of Navigation, 2004: 555 -560.

[29] Gao G X, Heng L, Hornbostel A, et al. DME/TACAN interference mitigation for GNSS: algorithms and flight test results[J]. GPS Solutions, 2013, 17(4): 561 -573.

[30] Gromov K G. GIDL: generalized interference detection and localization system[D]. USA:Stanford University, 2002.

[31] Bours A, Cetin E, Dempster A G. Enhanced GPS interference detection and localisation[J]. Electronics Letters, 2014, 50(19):1391 -1393.

[32] 周轩, 李广侠, 蔡锭波, 等. 卫星导航系统防欺骗技术的回顾与展望[J]. 导航定位学报, 2013, 1(3): 79 -84.
ZHOU Xuan, LI Guangxia, CAI Dingbo, et al. Review and prospect of GNSS anti-spoofing techniques[J]. Journal of Navigation and Positioning, 2013, 1(3): 79 -84. (in Chinese)

[33] Wesson K, Rothlisberger M, Humphreys T. Practical cryptographic civil GPS signal authentication[J]. Journal of the Institute of Navigation, 2012, 59(3): 177 -193.

[34] Scott L. Anti-spoofing & authenticated signal architectures for civil navigation systems [C]//Proceedings of the 16th International Technical Meeting of the Satellite Division of the Institute of Navigation,2003: 1543 -1552.

[35] Key E L. Techniques to counter GPS spoofing[R]. Internal Memorandum, the MITRE Corporation, 1995.

[36] Jafarnia A J, Broumandan A, Nielsen J, et al. GPS spoofer countermeasure effectiveness based on signal strength, noise power, and C/N0 measurements[J]. International Journal of Satellite Communications and Networking, 2012, 30(4): 181 -191.

[37] Wen H Q, Huang P Y, Dyer J, et al. Countermeasures for GPS signal spoofing [C]//Proceedings of the 2005 International Technical Meeting of the Institute of Navigation, 2005: 13 -16.

[38] Akos D M. Who's afraid of the spoofer? GPS/GNSS Spoofing detection via automatic gain control (AGC) [J]. Navigation, 2012, 59(4): 281 -290.

[39] O'Hanlon B W, Psiaki M L, Bhatti J A, et al. Real time GPS spoofing detection via correlation of encrypted signals[J]. Navigation, 2013, 60(4): 267 -278.

[40] Montgomery P Y, Humphreys T E, Ledvina B M. Receiver-autonomous spoofing detection: experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer[C]// Proceedings of the 2009 International Technical Meeting of the Institute of Navigation,2009: 124 -130.

[41] Montgomery P Y, Humphreys T E, Ledvina B M. A multi-antenna defense: receiver-autonomous GPS spoofing detection[J]. Inside GNSS, 2009, 4(2): 40 -46.

[42] 张鑫, 庞晶, 苏映雪,等. 天线阵载波相位双差的欺骗干扰检测技术[J]. 国防科技大学学报, 2014, 36(4):21 -23.
ZHANG Xin, PANG Jin, SU Yingxue, et al. Spoofing detection technique on antenna array carrier phase double difference [J]. Journal of National University of Defense Technology, 2014, 36(4):21 -23. (in Chinese)

[43] Broumandan A, Jafarnia-Jahromi A, Dehghanian V, et al. GNSS spoofing detection in handheld receivers based on signal spatial correlation[C]//Proceedings of IEEE/ION. Position Location and Navigation Symposium (PLANS), 2012: 479 -487.

[44] Psiaki M L, Powell S P, O'Hanlon B W. GNSS spoofing detection using high-frequency antenna motion and carrier-phase data [C]//Proceedings of the 26th International Technical Meeting of the Satellite Division of the Institute of Navigation, 2013: 2949 -2991.

[45] Humphreys T E, Ledvina B M, Psiaki M L,et al. Assessing the spoofing threat development of a portable GPS civilian spoofer[C]// Proceedings of the 21st International Technical Meeting of the Satellite Division of the Institute of Navigation, 2008: 2314 -2325.

[46] Jafarnia-Jahromi A, Broumandan A, Nielsen J, et al. GPS vulnerability to spoofing threats and a review of antispoofing techniques [J]. International Journal of Navigation and Observation, 2012(2012): 1 -16.

[47] Shepard D P, Humphrys T E. Characterization of receiver response to a spoofing attack[C]// Proceedings of the 24th International Technical Meeting of the Satellite Division of the Institute of Navigation, 2011: 2608 -2618.

[48] 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[J]. 中国惯性技术学报, 2013, 21(3): 336 -340.
LI Sihai, LIU Yang, ZHANG Huisuo, et al. Inertial measurements aided GNSS spoofing detection technique[J]. Journal of Chinese Inertial Technology, 2013, 21(3): 336 -340. (in Chinese)

[49] Progri I. Geolocation of RF signals: principles and simulations[M]. USA:Springer Science & Business Media, 2011.

[50] Cheng X J, Cao K J, Xu J N, et al. Analysis on forgery patterns for GPS civil spoofing signals[C]// Proceedings of the 4th International Conference on Computer Sciences and Convergence Information Technology, ICCIT 09, 2009:353 -356.

(下转第 20 页)

[2] 张锴. 现代卫星导航信号恒包络发射与抗多径接收技术研究[D]. 长沙:国防科学技术大学,2013.
ZHANG Kai. Constant-envelope transmission and multipath mitigation for modern satellite navigation signals[D]. Changsha:National University of Deference Technology , 2013. (in Chinese)

[3] Zhao L, Amin M G, Lindsey A R. Subspace array processing for the suppression of FM jamming in GPS receivers [J]. IEEE Transactions on Aerospace and Electronic Systems, 2004, 40(1):80 - 92.

[4] Daneshmand S. GNSS interference mitigation using antenna array processing[D]. Canada:University of Calgary,2013.

[5] Daneshmand S, Broumandan A, Nielsen J, et al. Interference and multipath mitigation utilising a two-stage beamforming for global navigation satellite systems application [J]. IET Radar Sonar and Navigation, 2013, 7(1):55 - 66.

[6] Rougerie S, Carrie G, Vincent F, et al. A new multipath mitigation method for GNSS receivers based on antenna array[J]. International Journal of Navigation and Observation, 2012(2012).

[7] Daneshmand S, Broumandan A, Sokhandan N, et al. GNSS multipath mitigation with a moving antenna array[J]. IEEE Transactions on Aerospace and Electronic Systems, 2013, 49(1):693 - 698.

[8] Sahmoudi M , Amin M G. Optimal robust beamforming for interference and multipath mitigation in GNSS arrays[C]// Proceedings of IEEE international conference on Acoustics, Speech and Signal Processing, 2007, 3:III - 693 - III - 696.

[9] 王永良,陈辉,彭应宁,等. 空间谱估计理论与算法[M]. 北京: 清华大学出版社, 2004:26 - 30.
WANG Yongliang, CHEN Hui, PENG Yingning , et al. Spatial spectrum estimation theory and algorithm[M]. Beijing: Tsinghua University press, 2004:26 - 30. (in Chinese)

[10] 王纯. 卫星导航接收机自适应抗干扰方法研究[D]. 西安:西安电子科技大学, 2011.
WANG Chun. Research on adaptive interference suppression in satellite navigation receiver[D]. Xi'an:XiDian University, 2011. (in Chinese)

[11] Windrow B. Adaptive filters[M]. USA: Holt, Rinehart and Winston, 1971:563 - 587.

(上接第9页)

[51] Psiaki M L, O'Hanlon B W, Bhatti J A, et al. Civilian GPS spoofing detection based on dual receiver correlation of military signals[C]// Proceedings of the 24th International Technical Meeting of the Satellite Division of the Institute of Navigation, 2011: 2619 - 2645.

[52] Psiaki M, O'Hanlon B W, Bhatti J A, et al. GPS spoofing detection via dual-receiver correlation of military signals[J]. IEEE Transactions on Aerospace and Electronic Systems, 2013, 49(4): 2250 - 2267.

[53] O'Hanlon B W, Psiaki M, Humphreys T E, et al. Real-time spoofing detection using correlation between two civil GPS receiver[C]//Proceedings of the 25th International Technical Meeting of the Satellite Division of the Institute of Navigation, 2012: 3584 - 3590.

[54] Swaszek P F, Hartnett R J, Kempe M V, et al. Analysis of a simple, multi-receiver GPS spoof detector[C]//Proceedings of the 2013 International Technical Meeting of the Institute of Navigation, 2013: 884 - 892.

[55] Swaszek P F, Hartnett R J. Spoof detection using multiple COTS receivers in safety critical applications[C]// Proceedings of the 26th International Technical Meeting of the Satellite Division of the Institute of Navigation , 2013: 2921 - 2930.

[56] Heng L, Makela J J, Dominguez-Garcia A D, et al. Reliable GPS-based timing for power systems: a multi-layered multi-receiver architecture[C]// Proceedings of Power and Energy Conference at Illinois (PECI), 2014: 1 - 7.

[57] Jafarnia-Jahromi A, Lin T, Broumandan A, et al. Detection and mitigation of spoofing attacks on a vector-based tracking GPS receiver[C]// Proceedings of the 2012 International Technical Meeting of the Institute of Navigation, 2012: 790 - 800.

[58] Heng L, Chou D, Gao G X. Reliable GPS-based timing for power systems[J]. Inside GNSS, 2014(6): 38 - 45.

[59] Lo S, De Lorenzo D, Enge P, et al. Signal authentication: a secure civil GNSS for today[J]. Inside GNSS, 2009(5): 30 - 39.

[60] Heng L, Work D B, Gao G X. Cooperative GNSS authentication: reliability from unreliable peers[J]. Inside GNSS, 2013(5): 70 - 75.