doi:10.19306/j.cnki.2095-8110.2024.06.007

GNSS 授时干扰技术发展综述

陈力超,曾芳玲,欧阳晓凤,芮梓轩

(国防科技大学电子对抗学院,合肥 230037)

摘　要:随着全球卫星导航系统(GNSS)的发展,其授时功能已广泛应用于电力、通信等国家关键基础设施与国防领域。但由于卫星导航信号固有的脆弱性,授时服务极易受到恶意干扰,卫星授时安全日益受到世界关注。目前现行技术大都以干扰导航定位目的为主,对授时的干扰往往容易被忽略,实际上对授时结果的干扰对目标的危害性更大且极为隐蔽。首先,从授时基本干扰方式、授时干扰技术和授时干扰效果评估技术 3 个方面梳理了 GNSS 有意授时干扰关键技术的研究现状。其次,分析了 GNSS 授时干扰技术目前存在的科学问题。最后,对相关技术未来的发展趋势进行了展望。

关键词:卫星授时安全;压制干扰;欺骗干扰;干扰效果评估;GNSS

中图分类号:V474.2　　**文献标志码**:A　　**文章编号**:2095-8110(2024)06-0084-16

Overview of the development of GNSS timing interference technology

CHEN Lichao, ZENG Fangling, OUYANG Xiaofeng, RUI Zixuan

(College of Electronic Engineering, National University of Defense Technology, Hefei 230037, China)

Abstract: With the development of the global navigation satellite system (GNSS), its timing function has been widely used in critical national infrastructures such as power and communications, as well as in the field of national defence. However, due to the inherent vulnerability of satellite navigation signals, the timing service is easily affected by malicious interference, and the security of satellite timing has increasingly attracted global attention. At present, most of the existing technologies mainly focus on the interference with the purpose of navigation and positioning, while the interference with the timing is often ignored, in fact, the interference with the timing results can be more harmful and extremely covert to the target. Firstly, the research status of key GNSS timing interference technologies is sorted out from three aspects, which are basic jamming mode, timing interference technology and timing interference effect evaluation technology. Secondly, the current scientific problems of GNSS intentional timing interference technology are also analyzed. Finally, the future development trend of related technologies is predicted.

Key words: Satellite timing security; Suppression interference; Spoofing; Interference effect evaluation; GNSS

收稿日期: 2024-07-02;**修订日期**:2024-08-25

作者简介:陈力超(2002—),男,硕士研究生,主要从事卫星导航对抗方面的研究。

通信作者:欧阳晓凤(1989—),女,博士,讲师,主要从事卫星导航对抗方面的研究。

0　引言

全球卫星导航系统(global navigation satellite system,GNSS)在全球范围内提供全天候的位置、速度和时间(position, velocity, and time,PVT)服务,已成为最主要的定位和授时手段之一。随着现代信息技术的飞速发展,人们对时间频率的需求不断增加,网络覆盖范围也日益扩大。几乎所有需要定时和时间同步的场景都依赖于 GNSS 进行授时和定时[1],并且随着科技发展逐渐呈现出高精度、高可靠及高安全的特点[2]。GNSS 授时服务已被广泛应用于科学研究、大地测量、航空航天、远程时间传递与比对以及军事战争等领域[3-4]。值得注意的是,2020 年 2 月,美国总统签署了关于负责任使用 PVT 服务的行政令[5],旨在保护依赖该服务的精密设施免受干扰,表明世界各国对于 GNSS 服务的安全性予以充分重视。

由于 GNSS 信号的开放性及其信号接收功率低等特点,2011 年在华盛顿举行的会议上强调了不利空间气候对全球定位系统(global positioning system, GPS)的影响[6],GNSS 信号还受到诸如太阳耀斑、闪烁及射频等无意环境干扰因素的影响[7-8],GNSS 信号的安全性问题逐渐暴露。除了常规方式的“硬杀伤”外,还存在众多“软杀伤”,如电磁欺骗干扰、赛博攻击、大气环境干扰及多径效应等。2016 年 1 月 26 日,美国空军在操作卫星时意外导致数据库出现微小错误,进而引发 GPS 授时系统出现误差,使得全球用户经历了几小时的 GPS 授时问题;2017 年 1 月 18 日,欧洲伽利略卫星导航系统在轨运行的 18 颗卫星上 9 台原子钟出现了故障并停止运行,这一状况甚至危及到了整个系统的安全。由于本文主要关注刻意的授时干扰技术,对射频干扰、大气环境干扰等无意干扰不再赘述,感兴趣的读者可参阅文献[9]。从几次 GNSS 系统时间故障中可以发现,时间信息对系统运行具有重要影响,使得有意和无意发生的授时干扰事件逐渐受到关注,也推动了授时干扰技术成为当前的研究热点。

根据接收机对抗机理,GNSS 有意干扰技术一般包括压制式干扰和欺骗式干扰技术。林肯实验室研究表明,1 W 功率的干扰机可以使 85 km 以内的 C/A 码接收机无法正常工作,反映出 GNSS 信号的脆弱性以及授时信息受扰的危害性。此外,相关研究和实验已充分证明对 GNSS 接收机实施压制干扰能够阻滞其正常获取时间信息[10-12],且干扰装置实现简单、高效,使得压制干扰成为当前 GNSS 干扰的典型手段。

与压制干扰机理不同,欺骗干扰主要通过发射与 GNSS 信号相同或基本相同的干扰信号,使目标接收机作出错误的判断,具有隐蔽性和威胁性[13-14],这使得针对 GNSS 授时信息的欺骗干扰方法成为导航对抗领域的新兴研究热点。尤其对于精密授时系统,本地时间与卫星发播的信号必须保持严格的同步,授时错误将会破坏系统的时间同步,导致一系列的系统问题[15],继而产生严重后果,对组网的国家重要基础设施(电力[16]、移动通信及互联网星座)等产生极其重大的影响。对 GNSS 授时接收机实施欺骗干扰可以引入破坏系统时间基准的时间误差,从而使电力和通信系统[17]瘫痪,甚至引发大规模停电等严重后果。2017 年 9 月,众多智能手机因遭受 GNSS 欺骗干扰出现异常行为,并由此引发如服务器异常、时间授时错误等一系列安全故障;2022 年,德克萨斯州的干扰事件导致其机场 GPS 出现异常,迫使其关闭跑道,至今仍未查明根源;在黑海地区,关于假信号威胁飞机导航系统的报道数量激增,其中一份报道描述了飞机时钟的世界协调时(universal time coordinated,UTC)发生了重大变化,时间变化范围从几小时至 12 h 不等。

目前,针对 GNSS 授时信息的压制或欺骗干扰技术已进行了大量研究,随着 GNSS 授时安全问题日益凸显,梳理现有针对卫星导航授时服务的干扰机理、实施方法及其效果评估技术十分必要,对于维护 GNSS 信息安全、增强授时信息获取能力及提升定位、导航与授时(positioning, navigation and timing, PNT)体系对抗能力有着深远意义。考虑到现有的干扰手段包含压制和欺骗两种方式,且在实践过程中通常需要将二者综合运用。因此,本文首先介绍了授时的基本干扰方式;其次,分别阐述了授时压制干扰与欺骗干扰技术的发展现状;接着,对授时干扰效果评估指标的建立进行了系统性描述;最后,对授时干扰技术的未来发展作出展望。

1　授时基本干扰方式与应用

卫星导航系统通常由空间段、运控段和用户段组成,卫星 PNT 服务的干扰一般针对用户段展开,即针对 GNSS 接收机实施定位或授时干扰,GNSS 授时接收机处理流程如图 1 所示。

假设通过解算得到的 4 颗导航卫星的坐标分别为 $(x_i,y_i,z_i)(i=1,\cdots,4)$,用户位置坐标为$(x_0,$

y_0, z_0），接收机时间相对于导航系统的系统时间的钟差为 δt_u，不考虑电离层、对流层等延时误差时有

$$\begin{cases}\rho_1 = \sqrt{(x_0-x_1)^2+(y_0-y_1)^2+(z_0-z_1)^2}+c\delta t_u\\ \rho_2 = \sqrt{(x_0-x_2)^2+(y_0-y_2)^2+(z_0-z_2)^2}+c\delta t_u\\ \rho_3 = \sqrt{(x_0-x_3)^2+(y_0-y_3)^2+(z_0-z_3)^2}+c\delta t_u\\ \rho_4 = \sqrt{(x_0-x_4)^2+(y_0-y_4)^2+(z_0-z_4)^2}+c\delta t_u\end{cases} \tag{1}$$

式中，$\rho_i(i=1,\cdots,4)$ 为用户到导航卫星的伪距实际测量值，通过解算出钟差 δt_u 完成授时过程。压制式干扰主要影响接收机的捕获过程，而欺骗式干扰主要影响跟踪与解算过程，使其无法获得或获得错误的伪距、卫星位置等信息，最终干扰接收机的授时过程，具体影响接收机的处理环节详见第 2,3 章。

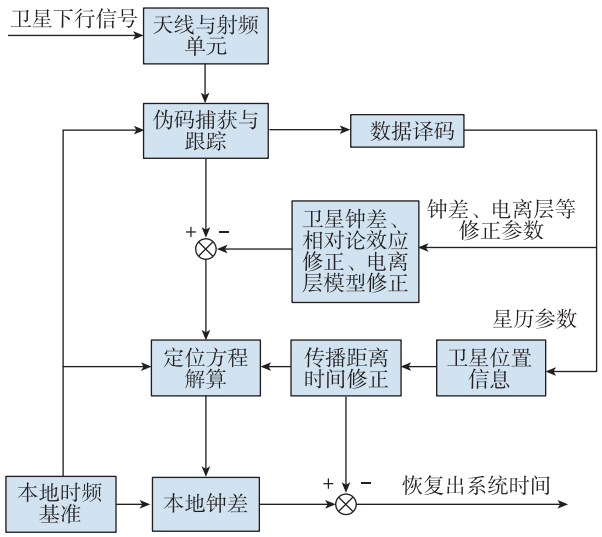

图 1 GNSS 授时接收机处理流程

Fig. 1 GNSS timing receiver processing flow

1.1 压制干扰

卫星信号到达地面时能量十分微弱，仅为 −160 dBW 左右，因此对于压制式干扰技术，通过直接发射强干扰信号，显著降低接收机接收端的信噪比，造成导航信号模糊不清或完全淹没在干扰信号中而无法识别，进而干扰目标接收机的授时过程。一般 C/A 码接收机的抗干扰裕度在 30 dB 左右，P 码接收机在 43 dB 左右，干扰信号与卫星导航信号的干信比须大于接收机的抗干扰裕度。由于干扰装置发射功率相较导航信号偏大，导致隐蔽性差，虽然目前以压制式干扰为主的抗干扰技术也逐渐成熟[18-19]，但由于压制式干扰较容易实现，美国军方认为其仍是 GNSS 导航授时接收机面临的主要威胁，也是 GNSS 干扰的主要组成部分[20]。

1.2 欺骗干扰

欺骗式干扰通过发射与 GNSS 信号相同或基本相同的干扰信号，使目标接收机接收到欺骗信号中的错误信息，从而作出错误的判断。欺骗信号常因与真实信号的结构、参数及功率相似而难以被识别，因此欺骗干扰危害性强、检测难度高。欺骗式干扰按产生方式分为转发式干扰与生成式干扰。

1.2.1 转发式干扰

GNSS 接收机面临的转发式干扰，首先通过接收目标卫星信号，经处理后分通道给信号增加传播时延，随后直接发送出去。此干扰方式利用导航信号的延时特性，通过改变接收机测得的伪距，即给出假的“球半径”，实现目标的授时错误。一般的多站转发式干扰系统示意图如图 2 所示。

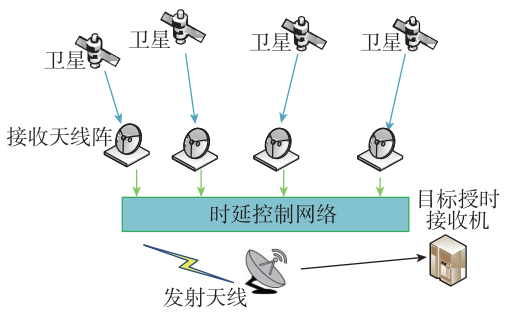

图 2 转发式欺骗干扰系统示意图

Fig. 2 Schematic diagram of a forwarding spoofing system

1.2.2 生成式干扰

生成式干扰的基本方式是根据 GNSS 信号伪码结构，复现与真实信号相关性最大的伪随机码，随后在生成的伪码上调制与真实信号格式完全相同的虚假导航信息。这一过程需要对真实信号的码相位、多普勒频移等参数进行估计，以确保欺骗信号到达目标接收机时与真实信号的参数和调制方式保持一致。信号同步是生成式欺骗干扰的基础[21]，文献[22]建立了欺骗信号的数学模型，并给出了信号同步及诱骗方法介绍。文献[23]详细阐述了针对 GPS 信号的结构及接收机工作原理，并阐述了如何人为伪造 GPS 信号。

由于欺骗信号在部分数据上进行了修改，使得接收机不仅得到错误的伪距，还可能使其他 PVT 信息也发生错误，从而实现目标的授时错误。根据实现的复杂性，生成式干扰攻击可分类为简单、中等和复杂攻击[24]。典型的生成式欺骗干扰系统示

意图如图 3 所示。

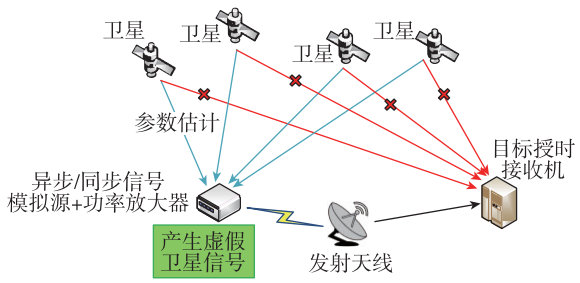

图 3　生成式欺骗干扰系统示意图

Fig. 3　Schematic diagram of generative spoofing system

1.3　国内外技术应用对比

早在 20 世纪 80 年代 GPS 建设之初，美国和俄罗斯就已经开始研究 GPS 干扰技术，并已成功研制出数代 GPS 干扰机产品。国内学者从伊朗捕获美军无人机事件后开始重点关注 GNSS 干扰技术，起步相对较晚。目前，中国电子科技集团有限公司、国防科技大学及信息工程大学等机构开展了相关研究，并在近些年逐渐开展了针对卫星 PNT 干扰效果的验证，以及干扰环境下 GNSS 接收机 PNT 信息可用性相关的评估测试。

由于欺骗干扰技术属于敏感话题，许多研究和技术细节未能公开，但从公开发表的文献资料来看，国内外欺骗干扰技术理论性研究差距不大，主要的差距在于实际检验场景和实验规模不同。例如，俄罗斯通过构建“磁场-21”等组网干扰系统实现大范围协同干扰，并在黑海区域实施常态化 GPS 欺骗，已通过战场的实际检验；美国海军也分别在 2017 年和 2019 年开展了大型分布式干扰实验，已收集相当丰富的 GNSS 干扰数据，并对复杂对抗环境下各型装备的定位、定时性能进行了检验。根据公开文献资料，国内针对多节点协同导航、授时干扰的技术研究主要在理论仿真层面，其工程实现水平可能还存在一定差距。

2　授时压制干扰技术研究现状

在未设置特定算法的前提下，通常在对卫星导航定位终端进行干扰的同时，接收机的授时结果也会被影响，且影响的效果往往不可控。对 GNSS 的干扰，一般使用的频段为 L 波段或 S 波段，由于导航信号在到达地球表面时功率已到达－160 dBW，因此授时设备很容易受到干扰而无法正常工作。具体实施有两种方案，第一种是通过直接发射强功率干扰信号使授时接收机失去对导航信号的锁定，转而重新进入捕获跟踪状态，此时真实信号已淹没在干扰信号中，最终导致授时接收机无法授时，但此方案无法精确欺骗目标接收机的授时偏差，可控性差；第二种方案则是采用辅助欺骗式干扰进行目标接收机的欺骗，首先发射强功率信号使目标接收机重新进入捕获跟踪状态，转而发射包含错误时间信息的欺骗信号，此时目标接收机会捕获到欺骗信号，此方案通过欺骗信号设置特定的参数，可控性强。

对于压制式干扰技术，干扰的目的是使目标接收机无法正常工作，即无法准确地捕获、跟踪卫星信号，在定位与授时干扰上的针对性相似，因此，压制干扰在对定位、授时接收机的干扰方法上并无明显区别。对定位与授时接收机影响效果的共同点在于都会使得接收信号的载噪比快速下降，且定位、授时信息停止更新或异常告警。而影响效果的不同点在于，对于定位接收机，无其他定位模块的接收机会直接失去定位数据，含有其他定位辅助模块（如惯性测量单元、移动基站辅助等）的接收机则会切换至辅助定位模块；对于授时接收机，受到压制干扰时，授时功能则依靠自身的基准时钟模块（如原子钟、晶振等）进入较低精度的守时状态。例如文献[11]所述，在重度干扰下，某雷达北斗授时设备的守时精度以 17 ns/s 速度下降，而北斗授时设备精度将以4 μs/s 的速度下降，10 min 后精度降低 2.4 ms，干扰环境的设置如图 4 所示。

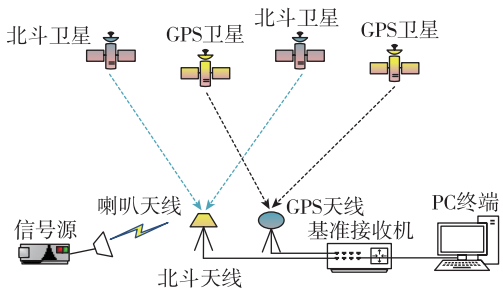

图 4　授时压制干扰环境示意图

Fig. 4　Schematic diagram of timing suppression interference environment

根据压制信号的样式可大致分为噪声干扰、音频干扰、扫频干扰、脉冲干扰和匹配频谱干扰，干扰机理如图 5 所示。表 1 汇总了 5 种干扰样式的各项指标对比情况，根据干扰场景、目标信号样式的不同可以选择最佳的干扰样式与干扰参数，以达到最好的授时干扰效果。目前，针对压制式干扰识别与

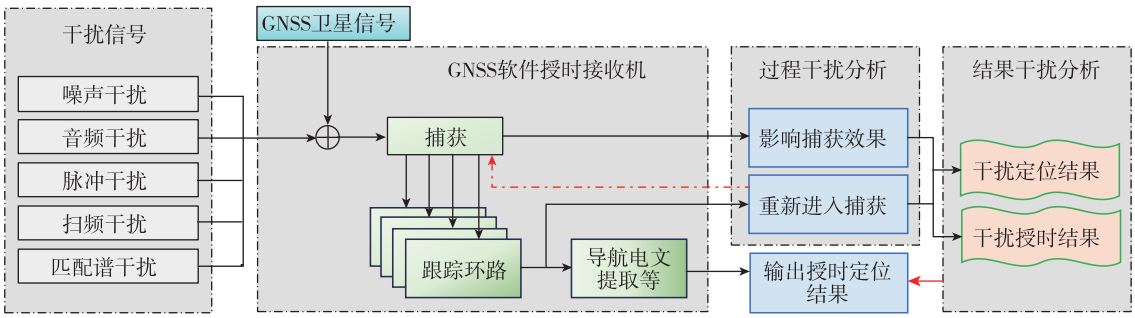

图 5 授时压制干扰机理框图

Fig. 5 Block diagram of jamming mechanism of timing suppression

表 1 压制干扰信号样式研究现状

Tab. 1 Research status of suppression interference signal styles

压制干扰信号样式	简单描述	基本类型	关键干扰效果影响参数	干扰监测滤除难易程度	干扰实现难易程度	主要重点研究进展
噪声干扰	将产生的随机噪声信号调制到目标导航信号的调制频率	噪声调频、噪声调幅、部分频带噪声干扰[28]	干扰功率、最大调幅系数、有效调频指数、调制带宽	噪声调幅、调频干扰一般为宽带干扰，不易被时频域滤波技术滤除；部分频带噪声干扰带宽较窄，易被检测滤除[29-30]	简单	噪声干扰效果对比分析，得出不同干扰参数调制下对 GNSS 接收机的影响及应对策略[31-32]
音频干扰	利用一个或多个特定频点下的音频信号对导航信号进行干扰，本质是带宽内的正弦信号[33-34]	单音干扰、多音干扰	干扰功率、音频位置、幅度与音频个数	频谱较窄，易被滤波器所滤除[35]	简单	音频位置、幅度与个数（多音干扰）上的优化设计[36]，并通过确定接收机热噪声基底以减少频域滤波的影响[37]
脉冲干扰	干扰机瞬间发射功率很大但持续时间很短的脉冲信号	单一类型	干扰瞬时功率、脉冲信号占空比、脉冲频率、载波频率[38-39]	由于在时域上特征明显，频域带宽较窄，易被时域消隐法等技术筛除	简单	干扰效果对比分析，给出不同环境下最佳干扰方式[40-41]；设计脉冲与窄带混合干扰方式，使其干扰的影响效果大于单一干扰，传统抗干扰手段失效[42]
扫频干扰	属于窄带干扰，可在一个扫描周期内将干扰信号的中心频率从低频段移动到高频段，具有频率突变、分段扫描特性[43]	线性扫频干扰、非线性扫频干扰	干扰功率、中心频率、扫频速度、扫频带宽	通过机器学习等方式可鉴别类型[44]，但传统方法难以准确识别参数	简单	不同接收机参数下的扫频速度等干扰参数优化设计，提升干扰样式的随机性、捷变性[45]
匹配谱干扰	干扰信号与目标授时接收机接收的信号具有相同的功率谱密度	BPSK，BOC 等载波调制样式，与目标信号一致	干扰功率、基带信号调制样式	与目标信号具有较强的相关性，不易被检测，但无法获得与真实信号相同的扩频增益[46]	复杂	非合作条件下的基带信号调制参数匹配、伪码序列相关性增强技术，进一步提升匹配谱干扰与目标信号的相关性[47]

抑制的研究已相对成熟[25-27]，这对于压制式干扰的有效性也提出了一定挑战。

综上，压制式干扰的类型相对比较传统和固定，主要包括结构相对简单的噪声干扰、音频干扰、脉冲干扰、频率能突变的扫频干扰和匹配卫星信号扩频码的匹配谱干扰。压制式干扰的可配置干扰参数相对较少，并且干扰信号容易被侦察设备识别并加以抑制，但由于干扰信号易生成、干扰设备结构相对简单且成本低廉，对于当前导航授时的干扰仍有很好的应用前景。

3　授时欺骗干扰技术研究现状

目前，针对不同的应用需求，授时欺骗干扰从结果上可以分为两种：一是同时欺骗目标接收机时间和位置信息；二是只改变目标接收机时间信息而不影响定位结果，以免被目标检测到欺骗，即只欺骗时间不欺骗位置。因此，如何针对特定目标设计欺骗干扰样式，是当前授时欺骗干扰技术的关键问题之一。下面，结合 GNSS 授时接收机基带处理模块的信号处理过程，分析不同授时欺骗方法针对的接收机阶段。具体而言，即针对码跟踪环、载波跟踪环和电文参数解算 3 种授时干扰方法，而前述压制干扰技术针对的是捕获跟踪环阶段，其干扰机理如图 6 所示。实际上，授时欺骗干扰技术可以认为是相干干扰，以授时接收机的相关信号处理通道为目标，通过使大部分欺骗信号进入授时接收机，使得目标接收机接收到错误的授时信息[48]。

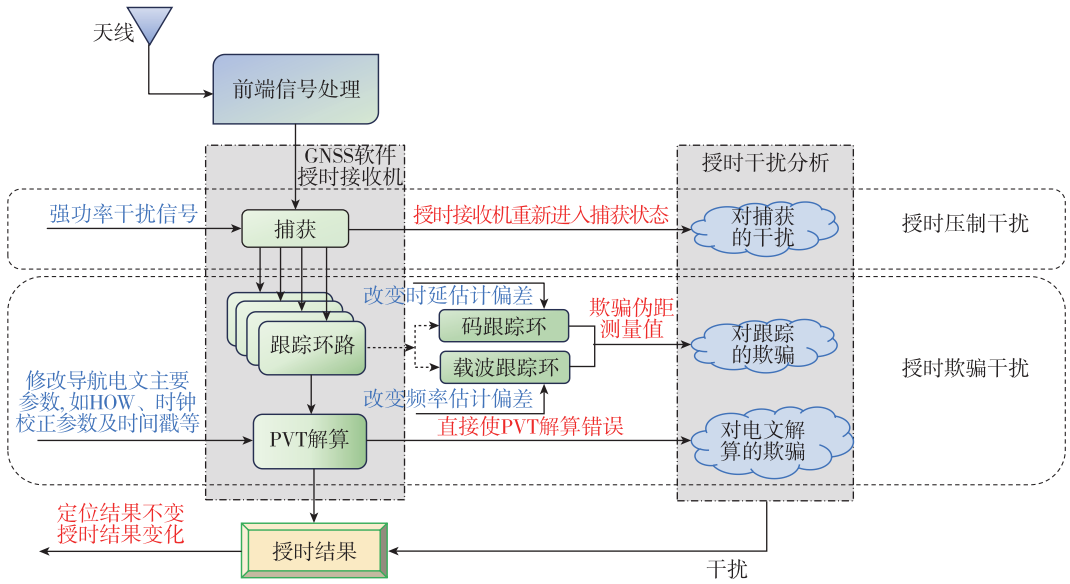

图 6　授时欺骗干扰机理框图

Fig. 6　Block diagram of timing spoofing mechanism

3.1　针对码跟踪环的授时欺骗方法

实际上，授时欺骗的数学原理即通过改变目标接收机的伪距测量结果，从而使得最终解算出的钟差发生偏移，针对码跟踪环的授时欺骗可通过改变码跟踪环的时延估计偏差实现。国防科技大学黄龙等[49]从授时接收机的授时原理出发，通过注入虚假的导航信息，经接收机解算后得到错误的伪距信息，提出了一种在定位结果不变的情况下拉偏目标接收机授时结果的算法。由于授时接收机内部的位置校验完好性监测手段，此算法保证了目标接收机得到的定位解算方程两边的增量相同，且各路转发信号与其直达信号的时延偏差相同，其本质是转发式干扰。实验结果表明，此干扰系统对目标接收机的定位结果影响非常小，可以以极大概率对授时时差进行有效控制，具有明显的隐蔽性，不易被目标系统检测。

利用码跟踪环的一种牵引式侵入接收机[50-51]的攻击过程如图 7 所示，其中，红色虚线表示欺骗信号相关峰，蓝色实线表示实际导航信号相关峰。在第一阶段，为实现隐蔽效果欺骗信号功率一般低于实际导航信号，二者码相位对齐后到达第二阶段，随后在第三阶段提升功率，迫使接收机失锁并重新捕获跟踪到欺骗信号，最终在第四阶段实施具体授时欺骗过程。

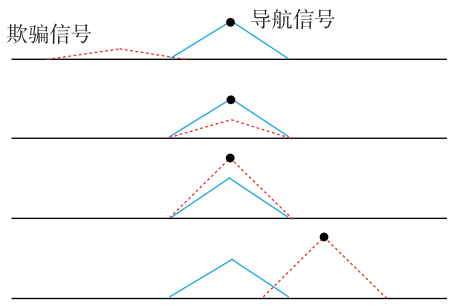

图 7　牵引式侵入接收机的攻击过程示意图

Fig. 7　Schematic diagram of the attack process of the traction intrusion receiver

海军工程大学团队[52]提出的授时欺骗算法同样基于伪距定位算法，根据欺骗设备的个数分为单站与双站转发式欺骗模型。对于授时欺骗方法类似于前述黄龙提出的算法，同时基于多普勒速度的原理进一步提出了虚假速度的算法。该算法通过精确调整多普勒频移和时间延迟实现接收机接收到虚假位置与虚假速度。但由于无法获得完整的实验测试设备，该团队只进行了位置欺骗测试以验证伪距欺骗的有效性，并没有对虚假时间与虚假速度作进一步验证。

2022 年，信息工程大学的 Gao 等[53]通过修正伪距、修正卫星位置以及修正伪距和卫星位置 3 种时间欺骗算法，其基于 Curtin Group 提供的开源数据，改变相应的伪距和卫星位置数据，利用仿真和实际实验对 3 种时间欺骗算法的有效性和性能进行了验证和评估。结果表明，通过修改电文参数的方式修改伪距的授时干扰相较于修改卫星位置的效果更佳，但修改卫星位置方式更具隐蔽性，实际运用时可根据目标接收机的防御手段灵活选择干扰方式。

3.2 针对载波跟踪环的授时欺骗方法

载波环通过复制与接收载波信号的相位或频率一致的载波，将接收信号与复制载波进行相乘混频，剥离接收信号的载波后，从而实现对接收载波信号的相位或频率的精确测量。针对载波跟踪环的授时欺骗方法，即通过干扰使接收机对载波环的频率估计错误。解放军电子工程学院团队[54]针对卫星授时对于 GNSS 信号稳定度的高敏感性，提出了一种改进的转发式干扰方法，通过在基带信号中引入人为的码率偏移，在时域上拉伸或压缩伪码信号的码元宽度，以模拟多普勒频移，多普勒频移示意图如图 8 所示。仿真结果表明，在加入干扰后通过改变拉伸系数，本地 C/A 码与接收到的伪随机码互相关值的峰值发生偏移，且在定位结果不变的前提下对目标接收机的授时造成影响，该影响与伪距观测值的增量呈线性相关。此干扰模式可在目标接收机锁定状态下连续不断地改变其相关峰偏移，具有较强的可控性与隐蔽性。

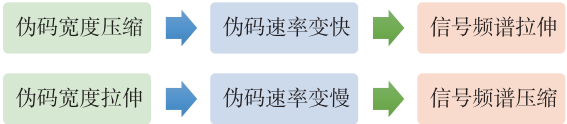

图 8 载波跟踪环下的多普勒频移

Fig. 8 Doppler shift under carrier tracking loop

由于很难自主构建与重放实际授时欺骗场景，2019 年，高扬骏等[55]利用德克萨斯大学无线电导航实验室提供的多组不同欺骗场景下的高保真欺骗数据集 TEXBAT(Texas spoofing test battery)中的 3 组场景建立时间欺骗模型，欺骗器通过接收真实的 GNSS 信号，生成与该信号精确码相位对齐的欺骗信号。由于很难精确对准目标接收机信号的载波相位，该模型采用了两种相位对齐策略[56]，通过改变信号的码相位实现目标接收机授时偏差。实验结果表明，接收机授时效果易受干扰影响，对于不同的时间欺骗场景可以从不同角度在几乎不改变定位的前提下影响着接收机的授时效果。

3.3 针对电文参数的授时欺骗方法

导航电文及其传输的参数是 GNSS 卫星广播给用户的一组二进制码，用于记录卫星轨道、卫星时钟校正参数、电离层延迟校正参数及卫星工作状态等信息，是用户导航定位的重要数据。与图 7 所示的目标授时接收机伪码跟踪环路相关峰值牵引不同，通过修改导航电文的欺骗算法可能不会移动相关峰值，因此接收机较难检测到欺骗信号。

针对电文参数的授时欺骗方法也是授时欺骗干扰的热点研究方向。西北工业大学[57]在 2018 年提出了修改导航电文中的交接字(hand over word, HOW)的方法，HOW 被伪造后，TLW(telemetry word)也会被欺骗，导致接收机解算得到错误的卫星发射时间，计算出错误的伪距和卫星位置，最终实现授时钟差的偏移。结果表明，该团队所提出的算法可以有效对目标接收机实施欺骗干扰，同时得到修改后 HOW 值与直角坐标系各坐标欺骗距离的关系。这种通过修改 HOW 的方法对于接收机来说是不可预测的，在误差较小时不易被检测到，具有隐蔽性强、效率高的优点。

2020 年，Mehmet 等[58]提出了针对导航电文中的时间戳和信号传播时间对接收机进行欺骗的方法，通过选择牵引式锁定和压制式辅助两种方式之一，以干扰接收机的捕获跟踪环路。结果表明，修改时间戳的方式比修改信号传播时间的方式更有效。同年，陈建平等[59]以修改时间戳的方式成功实现授时单元输出信号精度的降低，并使授时接收机解析出错误的时间信息。

最近的一项针对电文参数欺骗研究来自信息工程大学的高扬骏团队[60]，其基于导航电文数据块的理论计算，通过修改导航电文主要参数对授时质量的定性影响作出判断，并对卫星时钟校正参数进行灵敏

度分析。该团队首次提出通过修改卫星时钟校正参数的方式对授时信息进行干扰，并提出阶跃型与缓变型两种授时欺骗方式。实验采用 Curtin GNSS-SPAN Group 提供的开源观测数据，该授时欺骗算法通过修改接收星历中的卫星时钟校正参数来实现，实验结果成功验证了两种欺骗方法的有效性。

对于导航电文的 4 个时间电文参数，即在单频接收机中修改卫星时钟校正模型方程的 a_{f0}，a_{f1} 和 a_{f2} 这 3 个系数以及群波延时校正值的偏移量 ΔT_{GD}，卫星时钟偏置也会随之发生变化，且由于卫星信号传输时间的改变，伪距观测值也会相应发生改变，最终导致 PVT 结果偏差。导航电文总的参数影响分析如图 9 所示，简要概括了导航电文参数对 PVT 解算的影响。

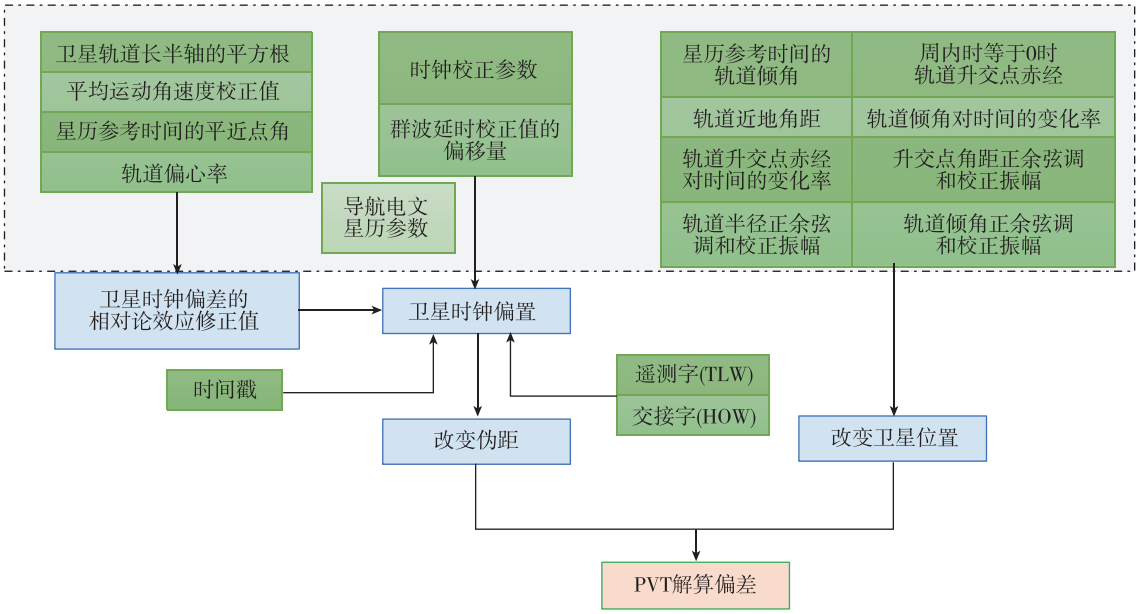

图 9　导航电文参数影响分析

Fig. 9　Navigation message parameter influence analysis

分析表明，针对电文参数的授时欺骗方法非常适用于不具备导航电文监控功能或不保存有效星历或历数的授时接收机。传统的移动相关峰欺骗方法实际上是对接收机基带数字信号处理阶段进行欺骗，而修改导航电文欺骗算法实际上是对接收机 PNT 信息解算阶段进行欺骗，导航电文授时欺骗的方式多样，如何选定最佳导航电文组合进行欺骗以干扰特定的环境，是未来针对导航参数进行授时欺骗的重点研究方向。

4　授时干扰效果评估指标研究现状

随着 GNSS 授时干扰技术的发展，建立一种衡量授时干扰效果的指标体系尤为关键，其能够更好地量化干扰对于授时接收机产生的影响，选定最佳评估指标能够显著提升干扰技术的有效性及干扰效能。干扰效果评估过程是一项比较复杂的系统工程，无论是对于 GNSS 的定位或是授时功能，效果评估都是干扰和抗干扰技术研发的基础性工作，所涉及的因素众多。根据目前国内外所建立的干扰效果评估指标，可以大致分为两个层面，一是信号处理层面，二是信息处理层面。其中信号处理层面依据授时接收机的工作流程划分为捕获、跟踪和电文解算 3 方面的干扰效果评估指标；信息处理层面是直接对授时接收机进行监测，即当干扰存在时对授时接收机输出信息的直接判断，分为干扰效率信息与干扰授时信息两方面。授时干扰效果评估指标体系如图 10 所示。

4.1　信号处理层面

首先信号进入接收机经下变频后进入捕获状态，针对干扰信号对捕获性能的影响程度可以通过捕获时间与捕获概率 2 个指标来评价。进入跟踪状态时，为准确获取导航信息，需在跟踪阶段动态搜索由捕获阶段获得的粗略载波信息与码相位等信息的更新变化，因此在干扰环境下会产生载波跟踪误差与码跟踪误差，将影响授时接收机的授时效果。其中接收机跟踪性能主要受载噪比、载波相位

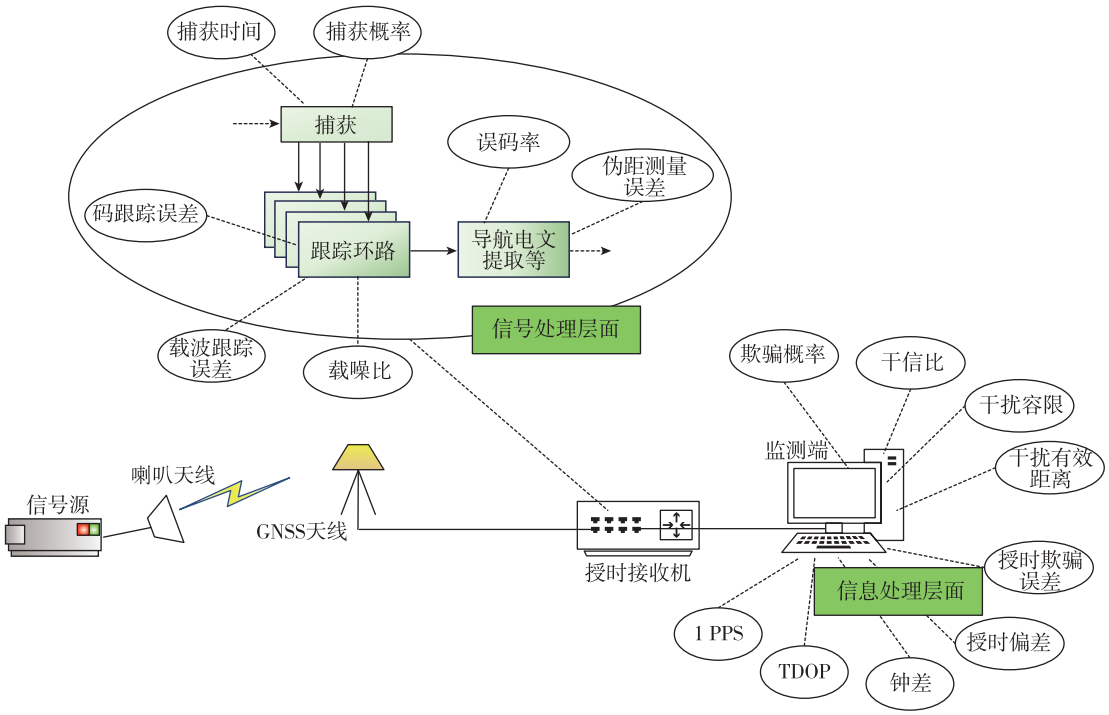

图 10 授时干扰效果评估指标体系

Fig. 10 Evaluation index system of timing interference effect

和码相位的影响[61]。另外,星座图特性、跟踪灵敏度以及跟踪相位噪声等也可作为评估接收机跟踪性能的重要指标[62]。彻底剥离中频信号中的载波和伪码后,经相关运算最终完成数据码编译成导航电文的过程,以此得到精确的伪距等测量值。因此,对于电文解算阶段干扰的评价指标可由通信性能上的解码误码率与测距性能上的伪距测量误差表示。以上指标具体介绍与相关研究如表 2 所示。

表 2 干扰效果评估指标基本介绍

Tab. 2 Basic introduction of interference effect evaluation metrics

序号	指标	基本描述	主要研究
1	捕获时间	衡量信号捕获的快慢程度	利用捕获时间对比干扰对于宽带与窄带的捕获性能影响[31];联合捕获时间与捕获时间方差[63],更好评估干扰效果
2	捕获概率	对接收机正常捕获卫星信号可能性的量化评估	利用接收机对干扰信号的捕获概率衡量干扰效果[64]
3	载噪比	描述信号的清晰程度	评估载噪比降低验证干扰对卫星信号质量的影响[65];通过实验得出干扰对于品质因数与载噪比的影响[66]
4	码跟踪误差	伪随机码和本地生成的参考码之间的时间偏差	对比不同跟踪环路算法下码相位和码频率的跟踪误差[67]
5	载波跟踪误差	在跟踪导航卫星信号的载波频率和相位时所产生的误差	跟踪精度主要由相位抖动误差与动态应力误差决定[65];对比宽带与窄带干扰下的载波跟踪与码跟踪误差的影响[32]
6	误码率	衡量电文解调精确性的指标	基于误码率提出起始点、起始线及起始线干性比等指标,并得出最佳压制式干扰样式[40];结合干性比与误码率分析不同干扰信号的干扰效果[46]
7	伪距测量误差	伪距测量值与实际值的差值,基本度量标准是位置协方差	结合多个指标的定量分析表征在窄带和宽带干扰下的干扰效果[65];
8	干扰容限	使接收机不能正常解调所需的最小干扰功率	干扰容限通常与干扰有效距离共同评估干扰效果[68];提出基于 3D-IRT 的方法,大幅提升电波传播建模计算精度[69]
9	干扰有效距离	描述干扰信号的有效作用范围	针对多源干扰建模出多源干扰下的有效作用区域与面积[70]

考虑到实际的应用场景，只针对单个模块进行指标分析对于干扰效果的判断仍缺少可信度。由于以上研究只针对接收机内部的信号处理性能进行分析，评估局限于信号处理层面，对于授时性能的影响并不能从监测端进行直观的判断，因此还需要进一步建立更加直观的评估指标。

4.2　信息处理层面

4.2.1　效率信息监测

效率信息监测即研究所发射干扰信号的功率对于干扰效果的直观影响，包括干扰容限与干扰有效距离等评估指标，相关描述见表 2。假定干扰源与接收机传输空间为自由空间，则根据自由空间传播损耗计算公式可以推导出干扰有效距离为

$$d=\frac{\lambda_j\ 10^{\frac{L_p}{20}}}{4\pi}=\frac{\lambda_j\ 10^{\frac{J_t+G_t-J_r+G_J-L_f}{20}}}{4\pi} \tag{2}$$

式中，λ_j 为干扰信号波长；J_t 为干扰源发射天线功率；G_t 为干扰源发射天线增益；J_r 为接收机端的干扰功率；G_J 为指向干扰源的接收机天线增益；L_f 为接收机前端滤波引起的功率损耗；L_p 为空间传播损耗。

在评估授时干扰效果时，干扰效率层面与信号处理层面的指标主要应用于压制式干扰方式，常用于研究不同干扰信号功率或信号样式。对于压制式干扰的信号功率或信号最佳样式的相关研究，以上指标更为适用。

4.2.2　授时信息监测

授时信息监测即研究所发射干扰信号对于授时接收机授时效果的直观影响，包括精度因子(dilution of precision，DOP)、秒脉冲(1 pulse per second，1 PPS)、钟差、授时偏差及授时欺骗误差等指标。主要应用于欺骗干扰效果评估方面，对授时欺骗干扰的欺骗效果提升起到标定与指引作用。DOP 表示误差的放大倍数，对接收机定位与授时精度有很大影响，其完全取决于接收机可见卫星个数及其几何分布，与接收机的类型配置或信号特征无关。其中钟差精度因子(time dilution of precision，TDOP)越小，卫星几何分布越佳，授时精度就更高；反之 TDOP 值越大，授时精度就越低，在恶意干扰情况下可表征对干扰授时监测端效果的提升。文献[32]利用伪距测量误差与 DOP 的关系，通过测量 4 个不同地点的机场的 DOP 与 TDOP 值，计算得出北斗三号对全球的授时精度为 20 ns，在干扰环境下的授时精度增加到 50 ns 以上。

量化干扰授时效果的另一种常用方法是通过比对授时接收机输出 1 PPS，即基准秒脉冲信号以检验授时精度受干扰程度，1 PPS 是授时接收机主要输出时标信息，其误差越大即表明干扰效果越好。文献[12]与[71]都研究了干扰信号功率对于授时接收机 1 PPS 精度的影响，实验表明，干扰功率越大 1 PPS 精度受影响程度也越大，且当干扰信号消失时，接收机需要经历缓冲期才能恢复到原先的 1 PPS 精度。文献[72]利用 1 PPS 与 IRIG-B 码对时两种方式对授时接收机授时影响进行描述，通过实验得出了不同发射功率与不同诱骗距离对于授时接收机授时影响的定量描述。以上研究表明，1 PPS 精度测试是检测授时接收机受干扰程度较好的评估指标。

接收机相对系统时间的时间差即钟差 δt_u，是授时接收机最直接的授时参数，直接对钟差进行授时效果影响分析也是常用方式，在进行定位解算时可同步得到钟差值。文献[55,60]都用钟差变化量作为欺骗干扰程度的评估指标，实验表明欺骗信号可以影响授时接收机的钟差值，钟差变化量越大欺骗干扰效果越好。而作为用户终端最重要的授时指标，授时偏差能直接反映出授时干扰对于授时接收机的影响程度。设接收机时钟 t，接收机时钟解算的钟差 δt_u 与修正后接收机的时钟 T 的关系为 $T=t+\delta t_u$，当接收机受欺骗干扰时，接收机钟差偏移为 $\delta t'_u$，导致接收机修正后的时钟偏移为 $T'=t+\delta t'_u$，求得欺骗干扰对接收机的授时偏差为 $\Delta T=T-T'=\delta t_u-\delta t'_u$，可以看出授时偏差与时钟的偏差是等效的，只是授时偏差需要结合本地时钟计算而来。文献[49,54]通过直接分析欺骗干扰后授时接收机的授时结果，判断其变化情况，实验表明欺骗干扰能够对授时接收机的时差进行有效控制。对于授时欺骗干扰技术，能够使目标接收机的授时发生指定的偏差，授时欺骗误差可以评估授时欺骗技术控制授时偏差的准确度。Gao 等[53]通过人为设置目标接收机授时偏差，通过比对 3 种算法的授时欺骗误差大小，可以判断算法是否达到授时欺骗的目的。除此之外，对于电力系统时间同步攻击技术，相量测量单元(phasor measurement unit，PMU)精度是精确监测电力系统的重要基础，PMU 相角偏差、时间不确定度等也是电力系统时间同步重要的评估指标[11,73]。

导航授时干扰效能评估过程是一项复杂的系统工程，是干扰与抗干扰技术研发的基础性工作，

涉及的因素众多，而目前针对导航授时干扰研究的评估指标较单一，缺少完备的科学效能评估指标体系和结合真实场景系统全面的干扰效果量化分析。在复杂电磁环境下，如何对己方及目标 GNSS 授时对抗行动干扰效果进行有效评估，是一个具有挑战性的重要课题，兼具重要理论意义和重大军民应用价值。

5 技术局限与挑战

随着 GNSS 抗干扰技术的不断发展，GNSS 的抗干扰性能得到了极大提升，这对 GNSS 授时干扰技术的发展提出了新的挑战。

1）真实欺骗场景难以构建与重放

GNSS 干扰信号释放具有一定的风险性，采集需要花费大量人力和物力且出错概率较高，因此针对 GNSS 授时干扰的开源数据集数量也远少于其他传统通信等相关研究领域，目前 GNSS 欺骗数据集包括 GATEMAN，TEXBAT 及 OAKBAT 等。另外，由于电子干扰与抗干扰博弈过程本身比较复杂，导致真实欺骗场景难以构建与重放，不同场景下授时干扰对目标接收机的影响仍不明确，这些原因共同制约了研究人员对授时干扰技术的研究。

2）工程实现具有挑战性

虽然授时干扰的原理相对简单，但其工程实现却相当具有挑战性，要解决众多的理论和工程问题。目前的授时干扰文献主要集中在底层授时欺骗算法方面，大多数仍停留在仿真阶段，未详细涉及实际工程实现，且领域敏感性等原因很大部分技术原理并未公开。因此，如何进行工程实现仍需要进一步研究和探索。需要强调的是，转发式干扰有效的前提是 GNSS 接收机的码环与载波环退出原来的锁定，才能转而锁定转发式欺骗信号。相关研究表明，迫使 GPS 接收机的 C/A 码与 P(Y)码环路失锁的方法各异且相对容易实现，但针对 M 码接收机环路的失锁会困难得多；生成式干扰则要解决发射后信号的失真问题，涉及 L 波段微弱信号的接收、处理、匹配及放大等，需要尽量减少信号失真，提高信噪比，且对于军码等加密信号的对抗方式是无法使用生成式干扰的，这都导致生成式干扰在工程实现上相较于转发式干扰难度更大。

3）单一干扰方式易被识别

目前，授时干扰技术的研究主要局限于理论研究和单一的干扰手段，随着抗干扰技术的发展，现有的单一欺骗干扰手段很难顺利且隐蔽地入侵带有抗欺骗模块的目标接收机。但对于有效性更高的多协同干扰手段，如何成熟运用高级协同欺骗干扰并降低系统复杂度与成本也是亟待解决的问题。

6 总结与展望

干扰与抗干扰是“矛与盾”的博弈过程，但不论 GNSS 如何发展，鉴于其运作环境复杂、信号不完善，总存在脆弱性，以及被欺骗干扰的风险。如何开发低成本、高效能及高精度的 GNSS 授时干扰技术，将是未来授时对抗的发展热点。通过梳理授时干扰效果评估指标，对现有 GNSS 授时安全进行全面评估分析有助于厘清导航战、授时战的负面影响，评估对手干扰手段对我方的威胁层次。本文可为卫星授时抗压制、反欺骗对策研究提供参考，对于未来更好维护国家卫星授时与导航安全具有重大意义。新兴的 GNSS 授时干扰技术应用前景十分广阔，本文对此技术的发展作出以下几点展望。

1）更加逼真的欺骗场景仿真与训练

对于建模仿真需要注意如何优化算法使得仿真结果与实际环境更加匹配。随着数据集与电磁环境建模理论的逐渐完善，未来的欺骗场景重建将更加成熟与逼真，这对于未来 GNSS 智能化博弈的对抗也起到至关重要的作用。

2）多元融合下的授时干扰技术

未来研究将致力于探索多种组合的授时干扰技术，如压制干扰辅助欺骗干扰、多设备和天线联合发送伪造信号等多系统协同下的干扰方式。且由于位置和授时干扰的方法类似，未来的授时干扰策略必然会更注重联合位置干扰一并高效开展。通过结合不同的干扰手段，可以提高干扰的复杂度与鲁棒性，增加对抗防御系统的识别与应对难度。此外，随着智能化技术的不断发展，未来的授时干扰技术会更加智能与自适应化，结合 AI 技术使得干扰机能够根据环境变化和对抗手段的进化实时进行动态调整与优化。

3）大规模复杂网络下的授时干扰技术

针对单节点的授时接收机进行干扰效果的分析是至关重要的，然而对于多节点干扰效果的研究同样具有重要意义。尤其对于组网系统中单节点或少量节点受到授时欺骗后整个系统性能的影响分析，将成为未来研究的重点之一。此外，随着大规模节点与复杂通信网络等各组网系统的不断发

展，其授时安全性和可靠性对于整个网络的稳定运行至关重要。在未来将更加关注多节点系统的安全性和稳定性，为智能化、互联化的网络提供更可靠的授时保障。

4)个性化定制干扰策略

目前，针对授时接收机的欺骗干扰分析主要基于一般性接收机，然而不同类型的授时接收机在抗干扰性能上存在较大差距。虽然它们的结构相似，但对干扰信号的响应能力却不尽相同。因此，未来的研究可以更加深入地针对各种类型的授时接收机进行关键参数分析，并据此预测欺骗干扰效果，这有助于制定针对性的防御策略，提高授时系统的安全性和稳定性。

致谢：感谢信号盲处理全国重点实验室对本文的资助。

参考文献

[1] 杨旭海，李孝辉，华宇，等．卫星授时与时间传递技术进展[J]．导航定位与授时，2021，8(4)：1-10.
YANG Xuhai，LI Xiaohui，HUA Yu，et al. Technical progress of satellite time service and time transfer[J]. Navigation Positioning and Timing，2021，8(4)：1-10(in Chinese).

[2] 华宇，郭伟，燕保荣，等．我国授时服务体系发展现状分析[J]．时间频率学报，2016(3)：193-201.
HUA Yu，GUO Wei，YAN Baorong，et al. Developing status of national time service architecture[J]. Journal of Time and Frequency，2016(3)：193-201(in Chinese).

[3] 魏艳艳．2021 年外军定位导航与授时领域发展综述[J]．中国电子科学研究院学报，2022，17(4)：342-346.
WEI Yanyan. Overview of the development of foreign military positioning，navigation and timing in 2021[J]. Journal of CAEIT，2022，17(4)：342-346(in Chinese).

[4] 薛连莉，尹晓桐，沈玉芃，等．美国《国防部定位、导航与授时体系战略》报告解析[J]．飞航导弹，2020(4)：82-89.
XUE Lianli，YIN Xiaotong，SHEN Yupeng，et al. Analysis of the U.S. department of defense positioning，navigation and timing system strategy report[J]. Aerodynamic Missile Journal，2020(4)：82-89(in Chinese).

[5] 葛悦涛，薛连莉．美国导航战与授时战劣势分析[J]．飞航导弹，2020(6)：6-11.
GE Yuetao，XUE Lianli. Analysis of disadvantages of American navigation war and timing war[J]. Aerodynamic Missile Journal，2020(6)：6-11(in Chinese).

[6] ERNIE B. Briefing highlights vulnerability of GPS to adverse space weather[J]. Space Weather，2011，9(8)：1.

[7] JOHANNESSEN R，GALE S J，ASBURY M J A. Potential interference sources to GPS and solutions appropriate for applications to civil aviation[J]. IEEE Aerospace and Electronic Systems Magazine，1990，5(1)：3-9.

[8] BANERJEE P，BOSE A，DASGUPTA A. Effect of scintillation on timing applications of GPS in Indian subcontinent[J]. IEEE Transactions on Instrumentation and Measurement，2007，56(5)：1596-1600.

[9] FABIO D. GNSS Interference threats and countermeasures[M]. London：Artech House，2015.

[10] SHEPARD D P，HUMPHREYS T E，FANSLER A A. Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks[J]. International Journal of Critical Infrastructure Protection，2012，5(3-4)：146-153.

[11] PARESH R，NIKOLAOS G，AHMAD T. Vulnerability analysis of smart grids to GPS spoofing[J]. IEEE Transactions on Smart Grid，2019，10(4)：3535-3548.

[12] 焦海松，杨海强，王博，等．GNSS 授时设备受电磁干扰的影响与分析[C]// 第五届中国卫星导航学术年会．南京：中国学术期刊电子出版社，2014：43-46.
JIAO Haisong，YANG Haiqiang，WANG Bo，et al. Analysis of the influence on GNSS timing equipment by electromagnetic interference[C]// Proceedings of 5th China Satellite Navigation Conference. Nanjing：China Academic Journal Electronic Publishing House，2014：43-46(in Chinese).

[13] 张欣然，李洪，杨春，等．欺骗干扰对 GNSS 矢量跟踪环路的影响[J]．清华大学学报(自然科学版)，2022，62(1)：163-171.
ZHANG Xinran，LI Hong，YANG Chun，et al. Influence of spoofing interference on GNSS vector tracking loops[J]. Journal of Tsinghua University (Science and Technology)，2022，62(1)：163-171(in Chinese).

[14] ZHOU M，LI H，LU M Q. Calculation of the lower limit of the spoofing-signal ratio for a GNSS receiver-spoofer[J]. EURASIP Journal on Wireless Communications & Networking，2018(1)：1-12.

[15] HUMPHREYS T E，LEDVINA B M，PSIAKI M L，et al. Assessing the spoofing threat (cover story)[J]. GPS World，2009，20(1)：28-38.

[16] 傅宁，范金锋，杨芳，等．电力系统 GNSS 授时接收

机抗干扰技术研究[J]. 无线电工程，2020，50(1)：81-84.
FU Ning，FAN Jinfeng，YANG Fang，et al. Study of anti-jamming technology of GNSS timing receiver in electric power system[J]. Radio Engineering，2020，50(1)：81-84(in Chinese).

[17] JIANG X C，ZHANG J M，HARDING B J，et al. Spoofing GPS receiver clock offset of phasor measurement units[J]. IEEE Transactions on Power Systems，2013，28(3)：3253-3262.

[18] HAO W，QING C，YONG X. An integrated beam anti-jamming algorithm for low-orbit navigation augmentation[J]. IEEE Communications Letters，2022，26(4)：877-881.

[19] SUN Y F，CHEN F Q，LU Z K，et al. Anti-jamming method and implementation for GNSS receiver based on array antenna rotation[J]. Remote Sensing，2022，14(19)：4774.

[20] 姜鹏，边少锋，占乃洲. 基于导航战的 GPS 压制式干扰技术研究[J]. 舰船电子工程，2010，30(8)：66-68.
JIANG Peng，BIAN Shaofeng，ZHAN Naizhou. Research of the GPS suppress jamming technology based on navigation warfare[J]. Ship Electronic Engineering，2010，30(8)：66-68(in Chinese).

[21] 盛莹，李宏宇，周述勇，等. GPS 生成式欺骗干扰方法研究[J]. 国外电子测量技术，2018，37(8)：39-43.
SHENG Ying，LI Hongyu，ZHOU Shuyong，et al. Research of GPS generated spoofing method[J]. Foreign Electronic Measurement Technology，2018，37(8)：39-43(in Chinese).

[22] 柳亚川，寇艳红. 同步式 GPS 欺骗干扰信号生成技术研究与设计[J]. 北京航空航天大学学报，2020，46(4)：814-821.
LIU Yachuan，KOU Yanhong. Research and design of synchronous GPS spoofing signal generation technology[J]. Journal of Beijing University of Aeronautics and Astronautics，2020，46(4)：814-821(in Chinese).

[23] GEBREMICHAEL H R. GPS 欺骗方法研究，GPS-SDR-SIM[D]. 天津：南开大学，2021.
GEBREMICHAEL H R. Research on GPS spoofing method，GPS-SDR-SIM[D]. Tianjin：Nankai University，2021(in Chinese).

[24] 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 21st International Technical Meeting of the Satellite Division of the Institute of Navigation. Savannah：Institute of Navigation，2008：2314-2325.

[25] 朱亮. 北斗卫星导航系统干扰识别与测向技术的研究与实现[D]. 北京：北京交通大学，2019.
ZHU Liang. Research and implementation of interference recognition and direction finding technology in BeiDou navigation satellite system[D]. Beijing：Beijing Jiaotong University，2019(in Chinese).

[26] 杨泽泽. 卫星导航接收机抗干扰算法研究[D]. 成都：电子科技大学，2022.
YANG Zeze. Study on anti-jamming algorithm for satellite navigation receiver[D]. Chengdu：University of Electronic Science and Technology of China，2022(in Chinese).

[27] 张通. 卫星导航系统压制干扰检测与识别技术研究[D]. 济南：山东大学，2023.
ZHANG Tong. Research on jamming detection and recognition techniques of satellite navigation system[D]. Jinan：Shandong University，2023(in Chinese).

[28] 周颖，邹斌，郝冰，等. 一种简易 GPS 压制式高斯白噪声窄带干扰机设计[J]. 航天电子对抗，2005，21(6)：15-18.
ZHOU Ying，ZOU Bin，HAO Bing，et al. Design of a simple GPS jammer using Gaussian white noise[J]. Aerospace Electronic Warfare，2005，21(6)：15-18(in Chinese).

[29] HUANG L，LU Z K，REN C，et al. Research on detection technology of spoofing under the mixed narrowband and spoofing interference[J]. Remote Sensing，2022，14(10)：2506.

[30] MOUSSA M，OSMAN A，TAMAZIN M，et al. Enhanced GPS narrowband jamming detection using high-resolution spectral estimation[J]. GPS Solutions，2017，21(2)：475-485.

[31] 赵新曙，王前. 压制式干扰对 GNSS 接收机的影响及应对策略[J]. 全球定位系统，2014，39(6)：47-51.
ZHAO Xinshu，WANG Qian. The effect and solving strategy on GNSS receiver by suppressing interface[J]. Gnss World of China，2014，39(6)：47-51(in Chinese).

[32] 刘瑞华，周童，刘亮. 压制式干扰对北斗接收机授时性能的影响评估[J]. 无线电工程，2023，53(9)：2125-2134.
LIU Ruihua，ZHOU Tong，LIU Liang. Evaluation of the influence of suppression jamming on Beidou receiver timing accuracy[J]. Radio Engineering，2023，53(9)：2125-2134(in Chinese).

[33] 刘禹圻，胡修林，冉一航，等. 卫星导航信号抗单频干扰性能研究[J]. 电子学报，2011，39(6)：1410-

1416.
LIU Yuqi, HU Xiulin, RAN Yihang, et al. Study on evaluating the impact of CWI on DLL tracking performance for GNSS signals[J]. Acta Electronica Sinica, 2011,39(6): 1410-1416(in Chinese).

[34] JAEGYU J, MATTEO P, BERND E. CW interference effects on tracking performance of GNSS receivers[J]. IEEE Transactions on Aerospace and Electronic Systems, 2012, 48(1): 243-258.

[35] ISLAM S, BHUIYAN M Z H, THOMBRE S, et al. Combating single-frequency jamming through a multi-frequency, multi-constellation software receiver: a case study for maritime navigation in the gulf of finland[J]. Sensors, 2022, 22(6): 2294.

[36] 瞿智，杨俊，杨建伟．大误差条件下单频干扰引起的伪码跟踪误差研究[J]．电子与信息学报，2016，38(1)：222-228.
QU Zhi, YANG Jun, YANG Jianwei. Effects of continuous wave interference on pseudorandom code tracking error under large error conditions[J]. Journal of Electronics & Information Technology, 2016, 38(1): 222-228(in Chinese).

[37] 毛虎，吴德伟，卢虎．对 GPS 接收机多音干扰参数优化设置及效能分析[J]．系统工程与电子技术，2019，41(8)：1699-1704.
MAO Hu, WU Dewei, LU Hu. Parameters configuration and effectiveness analysis of multiple-tone jamming to GPS receiver[J]. Systems Engineering and Electronics, 2019, 41(8): 1699-1704(in Chinese).

[38] 毛虎，吴德伟，卢虎，等．对 GPS 接收机的一种新宽带压制干扰样式分析[J]．电子与信息学报，2014，36(12)：2929-2934.
MAO Hu, WU Dewei, LU Hu, et al. Analysis of a new wideband blanket jamming type to GPS receiver[J]. Journal of Electronics & Information Technology, 2014, 36(12): 2929-2934(in Chinese).

[39] 张鑫鑫．GPSⅢ卫星导航干扰方案和干扰源优化部署方法设计[D]．成都：电子科技大学，2017.
ZHANG Xinxin. GPSⅢ satellite navigation interference scheme and interference source optimization deployment method design[D]. Chengdu: University of Electronic Science and Technology of China, 2017(in Chinese).

[40] 张帆．压制式干扰对卫星导航信号的误比特率影响研究[D]．西安：中国科学院研究生院(国家授时中心)，2013.
ZHANG Fan. Research on effect of blanket jamming on BER of satellite navigation signals[D]. Xi'an: National Time Service Center, Chinese Academy of Sciences, 2013(in Chinese).

[41] 苏煜．对 MUOS 卫星通信系统的压制式干扰仿真与分析[D]．哈尔滨：哈尔滨工业大学，2016.
SU Yu. Simulation and analysis of blanket jamming to MUOS satellite communication system[D]. Harbin: Harbin Institute of Technology, 2016(in Chinese).

[42] 郭海玉，刘小汇，鲁祖坤，等．脉冲和窄带混合干扰对卫星导航终端抗干扰的影响分析[J]．信号处理，2022，38(6)：1284-1292.
GUO Haiyu, LIU Xiaohui, LU Zukun, et al. Analysis of the influence of pulse and narrowband mixed interference on the anti-jamming of satellite navigation terminal[J]. Journal of Signal Processing, 2022, 38(6): 1284-1292(in Chinese).

[43] ZHAO X, HUANG X M, TANG X M, et al. Chirp pseudo-noise signal and its receiving scheme for LEO enhanced GNSS[J]. IET Radar Sonar and Navigation, 2022, 16(1): 34-50.

[44] QIN W J, DOVIS F. Situational awareness of chirp jamming threats to GNSS based on supervised machine learning[J]. IEEE Transactions on Aerospace and Electronic Systems, 2022, 58(3): 1707-1720.

[45] LI B Y, QIAO J, LU Z K, et al. Influence of sweep interference on satellite navigation time-domain anti-jamming[J]. Frontiers in Physics, 2023, 10: 1063474.

[46] 王角，苏中，张月霞．GPS 最优压制式干扰信号研究[J]．计算机测量与控制，2016,24(4)：257-260，267.
WANG Jiao, SU Zhong, ZHANG Yuexia. Study on optimal jamming signal of GPS system[J]. Computer Measurement & Control, 2016,24(4): 257-260, 267(in Chinese).

[47] 叶旅洋，樊战友，张瀚青，等．高斯干扰下 GNSS 信号码跟踪精度分析[J]．计算机科学，2020，47(1)：245-251.
YE Lyuyang, FAN Zhanyou, ZHANG Hanqing, et al. Analysis of GNSS signal code tracking accuracy under Gauss interference[J]. Computer Science, 2020, 47(1): 245-251(in Chinese).

[48] 戎建刚，孙卫民．GPS 接收机的相干干扰[J]．航天电子对抗，2005,21(6)：11-14，39.
RONG Jiangang, SUN Weimin. Coherent jamming for GPS receiver[J]. Aerospace Electronic Warfare, 2005,21(6): 11-14, 39(in Chinese).

[49] 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 re-radiating spoofing technique to GNSS timing receiver[J]. Journal of National University of Defense Technology, 2013,35(4): 93-96(in Chinese).

[50] PSIAKI M L, HUMPHREYS T E. GNSS spoofing and detection[J]. Proceedings of the IEEE, 2016, 104(6): 1258-1270.

[51] IOANNIDES R T, PANY T, GIBBONS G. Known vulnerabilities of global navigation satellite systems, status, and potential mitigation techniques[J]. Proceedings of the IEEE, 2016, 104(6): 1-21.

[52] BIAN S F, HU Y F, CHEN C, et al. Research on GNSS repeater spoofing technique for fake position, fake time & fake velocity[C]// Proceedings of 2017 IEEE International Conference on Advanced Intelligent Mechatronics (AIM). Munich: IEEE, 2017: 1430-1434.

[53] GAO Y J, LI G Y. Three time spoofing algorithms for GNSS timing receivers and performance evaluation [J]. GPS Solutions, 2022, 26(3): 87.

[54] 许益乔，曾芳玲，胡燕燕．一种对 GPS 授时干扰的新方法[J]. 电子测试，2013(3)：99-102.
XU Yiqiao, ZENG Fangling, HU Yanyan. New method of GPS time interference[J]. Electronic Test, 2013(3): 99-102(in Chinese).

[55] 高扬骏，吕志伟．TEXBAT 场景的 GPS 接收机授时欺骗影响分析[J]. 测绘科学技术学报，2019，36(2)：127-132，138.
GAO Yangjun, LYU Zhiwei. Impact analysis of GPS time spoofing based on TEXBAT scenes[J]. Journal of Geomatics Science and Technology, 2019, 36(2): 127-132, 138(in Chinese).

[56] GAO Y, LI H, LU M, et al. Intermediate spoofing strategies and countermeasures[J]. Tsinghua Science and Technology, 2013, 18(6): 599-605.

[57] YANG Q, ZHANG Y, TANG C K. A novel GPS spoofing algorithm based on modifying navigation message [J]. Communications and Networking, 2018, 236: 46-53.

[58] MEHMET Ö D, GÜNEŞ K K, ALI E P. On the limitations of GPS time-spoofing attacks[C]// Proceedings of 2020 43rd International Conference on Telecommunications and Signal Processing (TSP). Milan: IEEE, 2020: 313-316.

[59] 陈建平，王旭旭，罗欣宇，等．北斗欺骗干扰对电力授时的影响与对策分析[J]. 浙江电力，2020，39(11)：34-39.
CHEN Jianping, WANG Xuxu, LUO Xinyu, et al. Study on the influence of Beidou deception jamming on power time service and the countermeasures[J]. Zhejiang Electric Power, 2020, 39(11): 34-39(in Chinese).

[60] GAO Y J, LI G Y. Two time spoofing algorithms on GNSS receiver instrumentation of modifying satellite clock correction parameters in navigation message[J]. IEEE Transactions on Instrumentation and Measurement, 2023, 72: 1-11.

[61] 李武涛，黄智刚，肖宏．干扰对卫星导航接收机跟踪性能的影响分析[J]. 电子设计工程，2019，27(8)：119-123.
LI Wutao, HUANG Zhigang, XIAO Hong. Research on the impact of jamming on tracking performance for global navigation satellite system receivers [J]. Electronic Design Engineering 2019, 27(8): 119-123(in Chinese).

[62] 张波，王庆，阳媛，等．基于 AD9361 的北斗接收机终端性能评估方法研究[J]. 传感技术学报，2023，36(4)：583-589.
ZHANG Bo, WANG Qing, YANG Yuan, et al. Design and performance evaluation of Beidou receiver based on AD9361[J]. Chinese Journal of Sensors and Actuators, 2023, 36(4): 583-589(in Chinese).

[63] 张坤，曾芳玲，欧阳晓凤，等．基于接收机捕获性能的 GPS 压制干扰效果分析[J]. 舰船电子对抗，2018，41(6)：1-4，10.
ZHANG Kun, ZENG Fangling, OUYANG Xiaofeng, et al. Analysis of GPS blanket jamming effect based on receiver capture performance [J]. Shipboard Electronic Countermeasure, 2018, 41(6): 1-4, 10(in Chinese).

[64] 刘延斌，苏五星，闫抒升．转发式欺骗信号干扰 GPS 接收机的效能分析[J]. 空军雷达学院学报，2004，18(4)：4-6.
LIU Yanbin, SU Wuxing, YAN Shusheng. Efficiency analysis of repeater deception jamming GPS repeater[J]. Journal of Air Force Radar Academy, 2004, 18(4): 4-6 (in Chinese).

[65] 张坤．GPS 对抗干扰效能分析与评估[D]. 长沙：国防科技大学，2018.
ZHANG Kun. Analysis and evaluation of GPS confrontation jamming effectiveness[D]. Changsha: National University of Defense Technology, 2018 (in Chinese).

[66] 郭海玉，鲁祖坤，陈飞强，等．窄带与脉冲干扰对卫星导航信号载噪比的影响[J]. 全球定位系统，2021，46(1)：50-56.
GUO Haiyu, LU Zukun, CHEN Feiqiang, et al. Effects of narrowband and pulse interference on the

carrier-to-noise ratio of satellite navigation signals[J]. GNSS World of China, 2021, 46(1): 50-56(in Chinese).

[67] 窦杰. 卫星导航接收机跟踪环设计及性能评估[D]. 南京: 南京理工大学, 2021.
DOU Jie. Design and performance evaluation of tracking loop for satellite navigation receiver[D]. Nanjing: Nanjing University of Science and Technology, 2021(in Chinese).

[68] 张坤, 曾芳玲, 欧阳晓凤, 等. GPS 压制干扰效果分析[J]. 通信技术, 2018, 51(11): 2544-2548.
ZHANG Kun, ZENG Fangling, OUYANG Xiaofeng, et al. Analysis of GPS blanket jamming effects[J]. Communications Technology, 2018, 51(11): 2544-2548(in Chinese).

[69] 王倩营. 基于 3D-IRT 的 GPS 压制干扰影响范围的计算研究[J]. 兵器装备工程学报, 2023, 44(s01): 322-327, 397.
WANG Qianying. Research on the influence range of GPS suppressing interference based on 3D-IRT[J]. Journal of Ordnance Equipment Engineering, 2023, 44(s01): 322-327, 397(in Chinese).

[70] 倪少杰, 韦世鹏, 肖伟, 等. 面向抗干扰接收机的多干扰优化部署方法[J]. 导航定位学报, 2023, 11(3): 147-155.
NI Shaojie, WEI Shipeng, XIAO Wei, et al. Multi-jammer optimal deployment method for anti-jamming receivers[J]. Journal of Navigation and Positioning, 2023, 11(3): 147-155(in Chinese).

[71] THOMAS R, HARALD H, ANDERS R. Over-the-air jamming and spoofing tests of GNSS timing devices[C]// Proceedings of 2023 Joint Conference of the European Frequency and Time Forum and IEEE International Frequency Control Symposium (EFTF/IFCS). Toyama: IEEE, 2023: 1-3.

[72] 刁卓朋, 伍国英, 李文祥, 等. GPS 欺骗信号对变电站时间同步装置的干扰分析与测试[J]. 南方电网技术, 2024, 18(4): 88-95.
DIAO Zhuopeng, WU Guoying, LI Wenxiang, et al. Analysis and test of the interference of GPS deception signal on time synchronization device in substation[J]. Southern Power System Technology, 2024, 18(4): 88-95(in Chinese).

[73] 钱斌, 蔡梓文, 肖勇, 等. 电力系统时间同步攻击研究综述[J]. 电网技术, 2020, 44(10): 4035-4045.
QIAN Bin, CAI Ziwen, XIAO Yong, et al. Review on time synchronization attack in power system[J]. Power Grid Technology, 2020, 44(10): 4035-4045(in Chinese).

(编辑:孟彬)