引文格式:唐小妹,马鹏程,马春江.一种基于功率可行域的卫星导航欺骗干扰评估方法[J].武汉大学学报(信息科学版),2023,48(7):1160-1169.DOI:10.13203/j.whugis20220643

Citation: TANG Xiaomei, MA Pengcheng, MA Chunjiang. Evaluation Method of Satellite Navigation Spoofing Based on Power Feasible Region[J]. Geomatics and Information Science of Wuhan University, 2023, 48(7): 1160-1169. DOI: 10.13203/j.whugis20220643

一种基于功率可行域的卫星导航欺骗干扰评估方法

唐小妹[1] 马鹏程[1] 马春江[1]

1 国防科技大学电子科学学院,湖南 长沙,410073

摘 要:针对欺骗干扰评估场景复杂、反欺骗策略繁多等所导致的量化评估难度大的问题,建立了欺骗对抗场景到欺骗对抗效果的评估模型和映射过程,并从欺骗对抗场景中的功率空间和欺骗对抗效果中的欺骗有效概率出发,设计了基于欺骗有效功率可行域的评估方法与指标。仿真结果表明,该评估方法可以实现不同反欺骗策略之间性能的量化对比,能够为接收机反欺骗算法选择和优化提供量化评估方法。

关键词:卫星导航;欺骗干扰;功率空间;干扰评估;导航接收机

中图分类号:P228 **文献标识码**:A **收稿日期**:2023-03-10

DOI:10.13203/j.whugis20220643 **文章编号**:1671-8860(2023)07-1160-10

Evaluation Method of Satellite Navigation Spoofing Based on Power Feasible Region

TANG Xiaomei[1] *MA Pengcheng*[1] *MA Chunjiang*[1]

1 College of Electronic Science and Technology, National University of Defense Technology, Changsha 410073, China

Abstract: **Objectives**: In view of the difficulty of quantitative evaluation caused by complex spoofing scenarios and numerous anti-spoofing strategies, it is necessary to form effective indicators and methods for the evaluation of spoofing countermeasures. **Methods**: The evaluation model and mapping process from spoofing scenes to spoofing countermeasure effect are established. Based on the power space in the spoofing scenes and the spoofing effective probability in the spoofing countermeasure effect, the evaluation method and index based on the power feasible region are designed. **Results**: Through simulation, the quantitative evaluation results based on power feasible region of two spoofing countermeasure strategies are given, and the simulation results show that the evaluation method can realize the quantitative comparison of the performance of different anti-spoofing strategies. **Conclusions**: The indicator of the power feasible region can provide a quantitative evaluation method forselection and optimization of the anti-spoofing algorithms in receivers.

Key words: satellite navigation; spoofing; power feasible region; spoofing evaluation; navigation receiver

全球导航卫星系统(global navigation satellite system, GNSS)是当今社会最为重要的基础设施之一,能够给人类带来高精度的导航、定位和授时服务。然而,由于卫星导航信号传播信道开放、到达用户端功率较低等特性,卫星导航接收机极易受欺骗干扰的影响,甚至会输出错误的定位授时结果[1-2]。欺骗干扰评估是提升卫星导航接收机反欺骗能力和安全应用的重要工作。在实施欺骗干扰评估的过程中,必须明确评估指标和评估方法。评估指标即为定义在欺骗对抗

基金项目:国家自然科学基金(U20A0193, 62003354);国家部委资助项目(2019-JCJQ-JJ-190)。

第一作者:唐小妹,博士,研究员,主要从事北斗导航系统、导航应用、导航信号体制等领域的教学科研及工程研制工作。txm_nnc@126.com

通讯作者:马鹏程,博士,助理研究员。mapengcheng1001@163.com

场景所抽象出的对抗模型上的泛函映射，从不同的场景模型和评估需求出发即可得到不同的指标映射[3]。目前，对于欺骗干扰评估的研究主要集中在评估指标、评估方法等方面：评估指标即为评估方法或评估模型的输出；在评估方法方面，主要有理论评估、仿真评估、数据集评估和实际硬件平台评估等。

根据电子战领域常用的信息、功率、效率、时间等准则可以派生出不同的评估指标[3]，目前已有一定的研究基础。清华大学研究团队提出的卫星导航欺骗干扰评估指标[4]，包括欺骗有效概率、压制系数、欺信比、欺骗影响区域、欺骗成功后的破坏性、欺骗起效时延、欺骗风险、成本、复杂度等，并对欺骗有效概率、压制系数和欺骗风险等指标进行了实例计算。然而，由于剩余的其他指标存在理论计算难度，所以建议采用专家系统进行评估。另外，使用单一指标进行评估很难适用于所有场景。比如，欺骗有效概率、欺骗干扰检测概率等概率指标能够说明特定场景下欺骗对抗的概率情况，当欺骗干扰场景发生变化时，其概率值随之发生变化。所以，仅应用概率等指标无法对不同欺骗干扰场景下的对抗性能进行全面评估。在雷达领域多假目标对抗场景下，文献[5]从功率准则出发给出欺骗干扰成功必要的欺信比条件，而未给出充分条件，这是因为欺骗干扰功率指标无法直接用于衡量欺骗干扰有效性。欺信比能够从功率维度说明欺骗干扰功率对卫星导航接收机的影响，但是在欺骗对抗中，功率具有双重属性：既是攻击方实施欺骗干扰的能量保证，又是防守方检测欺骗干扰的重要特征，当欺骗干扰功率越来越大时，欺骗干扰有效性并非越来越高，所以应用欺信比进行欺骗对抗评估为必要条件而非充分条件。

在理论评估方法方面，欺骗干扰检测概率是常用的反欺骗算法的性能评估方法。文献[6]提出了基于博弈论的评估方法，将不同算法和攻击方法放在同一对抗矩阵中进行评估。文献[7]提出了基于灰色关联分析和模糊综合评判的GNSS欺骗干扰效能评估，主要将欺骗干扰评估进行指标分解，形成不同维度和不同层次的欺骗干扰性能评估结果，聚合成欺骗干扰装备性能的评估指标。目前来看，欺骗干扰有效性评估方法已经引起业内广泛关注。然而，这些方法和指标还未在接收机产品设计中得到广泛应用，主要是因为部分指标理论计算困难、不同指标权值确定主观性强、物理概念解释存在难度等。

通过仿真进行评估也是欺骗干扰评估研究的热点，尤其是欺骗干扰对于环路影响的评估。文献[8]提出了基于仿真的欺骗干扰评估方法，分析了不同干扰参数对于环路攻击成功的概率。以欺骗信号和真实信号之间的初始相位误差和多普勒误差作为二维变量，文献[9]提出了面积评估的方法，已经初步形成了基于攻击方参数遍历评估攻击效果的思路。虽然攻击方的初始相位误差和多普勒误差可以用于评估欺骗干扰对于跟踪环路的影响，但是部分欺骗干扰检测算法对这两个参数不敏感，所以很难将其用于欺骗干扰检测算法的评估。文献[10]通过仿真和实验分析了环路带宽和鉴别器对欺骗干扰效能的影响。

通过实测场景数据集进行评估是另一个研究热点，比如广泛应用的得克萨斯州大学奥斯汀分校发布的欺骗干扰测试数据集（Texas spoofing test battery，TEXBAT）提供了8个欺骗干扰场景[11-12]，而且已有大量文献基于TEXBAT进行欺骗干扰算法的验证[13]。2020年，美国能源部橡树岭国家实验室发布的欺骗干扰测试评估平台（Oak Ridge spoofing and interference test battery，OAKBAT）进一步扩充了TEXBAT测试场景[14]。然而，上述数据集的评估场景参数固定、数目有限，无法全面评估反欺骗算法的场景适应性。实测方式也是评估欺骗干扰和反欺骗算法性能的主流手段，目前已经有国内外导航领域公司和研究机构研发了欺骗干扰评估产品和评估场景，比如国外的司博伦[15]、诺瓦泰[16]、得克萨斯大学奥斯汀分校[11]、欧洲空间局[17]等，国内的国防科技大学[18]、清华大学[19]、北京航空航天大学[20]、奇虎360公司[21]等推出了相应的欺骗干扰实验环境，加速了欺骗干扰评估的发展。

从上述研究现状来看，仿真测试、数据集测试和实际硬件平台测试发展迅速，但是这些测试方法只能评估特定场景下的接收机反欺骗性能，无法给出接收机在复杂欺骗对抗场景下的反欺骗能力量化评估结果。在实际场景中，接收机所面临的欺骗干扰场景是多种多样的，比如转发式、生成式，甚至是多种干扰方式的叠加等。所以，只从特定场景和特定参数出发评估接收机反欺骗能力，并不能说明其在所有可能存在的欺骗干扰场景下的反欺骗性能。

针对目前的欺骗干扰评估方法无法进行场

景遍历、量化评估接收机反欺骗策略难度大的问题,本文基于目前的研究基础继续发展欺骗干扰评估指标与方法:(1)从卫星导航信号特征空间出发,提出了攻击方欺骗干扰模型与防守方处理模型;(2)针对单一指标无法全面量化攻守双方的对抗效果等问题,提出了基于欺骗有效功率可行域的欺骗对抗评估指标和方法;(3)基于典型对抗场景和反欺骗策略,通过仿真验证了本文提出的评估指标的可行性。

1 卫星导航欺骗对抗模型

本文给出了基于卫星导航信号特征空间的对抗模型,然后对欺骗干扰模型、卫星导航接收模型及对抗场景模型进行整合,并给出了卫星导航欺骗干扰评估场景模型,基于该模型提出了基于功率可行域的欺骗干扰评估指标。卫星导航欺骗对抗模型的数学模型基础主要由3部分构成:卫星导航信号特征空间,以及攻守双方的模型:卫星导航欺骗干扰模型和卫星导航接收机处理模型。

1.1 卫星导航信号特征空间

导航卫星发射信号构成的集合可以表示为[22]:

$$\boldsymbol{S}=\left\{s(t,\boldsymbol{a})\left|\int_{-\infty}^{\infty}s^2(t,\boldsymbol{a})\mathrm{d}t\leqslant E,\boldsymbol{a}\in\Lambda\right.\right\} \tag{1}$$

式中,$\boldsymbol{S}$是线性赋范空间,称为信号空间;t表示信号发射时刻;$s(t,\bullet)$表示导航卫星信号表达式,为实函数;E表示信号能量;$\boldsymbol{a}=[a_1\quad a_2\quad\cdots\quad a_N]$为$N$维特征矢量,$a_i$表示独立特征参量;$\Lambda$表示导航卫星发射信号特征参量的完备矢量集,它包含导航卫星辐射的电磁波在空域、时域、频域和极化域等一切特征空间参量,比如信号来向、功率、时延、频率、载波相位等。在某特定时刻$t=t_0$,$\boldsymbol{a}$中元素将取特定值,即$\boldsymbol{a}=\boldsymbol{a}_0=[a_1^0\quad a_2^0\quad\cdots\quad a_N^0]$,发射信号$s(t,\boldsymbol{a}_0)$可表示为$N$维特征空间中的一个点。

在接收机端,卫星发射的导航信号经过发射通道、空间传播信道以及接收通道引入的随机特性影响后,接收机收到的信号$s(t,\boldsymbol{a}')$不再是N维特征空间中的一个点,而是以$\boldsymbol{a}_0$为中心的一个N维区域,其中$\boldsymbol{a}'=[a_1'\quad a_2'\quad\cdots\quad a_N']$。

1.2 攻击方欺骗干扰模型

当存在欺骗干扰信号时,卫星导航接收机接收到的信号$x(t,\tilde{\boldsymbol{a}})$是导航卫星发射的真实信号和欺骗攻击方发射的欺骗信号的叠加,即:

$$x(t,\tilde{\boldsymbol{a}})=s(t,\boldsymbol{a}')+s(t,\boldsymbol{a}_J) \tag{2}$$

式中,欺骗干扰信号$s(t,\boldsymbol{a}_J)$是导航卫星发射信号$s(t,\boldsymbol{a}_0)$的泛函,可以记为$s(t,\boldsymbol{a}_J)=f\left[s(t,\boldsymbol{a}_0)\right]$;$\tilde{\boldsymbol{a}}=[\tilde{a}_1\quad\tilde{a}_2\quad\cdots\quad\tilde{a}_N]$表示接收信号的$N$维特征矢量;$\boldsymbol{a}_J=[a_1^J\quad a_2^J\quad\cdots\quad a_N^J]$表示欺骗干扰信号的$N$维特征矢量。一切可能的泛函映射构成了攻击方的欺骗干扰手段的集合F,$F=\left\{f\left|s(t,\boldsymbol{a}_J)=f\left[s(t,\boldsymbol{a}_0)\right]\right.\right\}$。

从干扰效果维度出发,卫星导航欺骗干扰类型可以分为两类。第一类是拖引式欺骗干扰,若被拖引的是第K维参量,其一般泛函表示为:

$$f\left[s(t,\boldsymbol{a}_0)\right]=\lim_{a_K^0\to a_K^J}s(t,\boldsymbol{a}_0),t\in[t_0,t_1] \tag{3}$$

第二类是重心偏移式欺骗干扰,其一般表达式可以写为:

$$f\left[s(t,\boldsymbol{a}_0)\right]=s(t,\boldsymbol{a}_J)\big|_{a_K^J=a_K^0+\Delta a_K},t\in[t_0,t_1] \tag{4}$$

式中,Δa_K满足使$\left|a_K^J-a_K'\right|\leqslant\delta_K$成立,$\delta_K$表示第$K$维参量特征空间不确定区域的大小;且在其他特征维度上尽可能逼近真实信号,即$\left|a_i^J-a_i'\right|\leqslant\delta_i,i\neq K$($\delta_i(i\neq K)$表示剩余维度信号特征空间不确定区域的大小)。

根据上述分析,考虑到卫星导航接收机的检测能力有限,卫星导航欺骗干扰成功的充要条件是攻击方生成的欺骗干扰信号满足:

$$\left|a_i^J-a_i'\right|\leqslant\delta_i,i=1,2,\cdots,N \tag{5}$$

即欺骗干扰信号$s(t,\boldsymbol{a}_J)$落入真实信号$s(t,\boldsymbol{a}')$的不确定区域。这主要取决于欺骗干扰方逼近真实信号特征空间的能力和不确定区域的测度大小。当欺骗干扰方逼近真实信号特征空间能力较强时,此时欺骗信号和真实信号特征空间距离较近,区分两者难度较大;当欺骗干扰方逼近真实信号空间能力较弱时,此时欺骗信号与真实信号特征空间距离较远,区分两者更加容易。另外,当欺骗信号与真实信号空间距离固定,但是信号空间不确定区域增大时,区分两者的难度也会增加。比如,宽带压制干扰可以对信号空间不确定区域的大小产生显著影响。

1.3 防守方接收处理模型

随着卫星导航应用的不断发展,卫星导航接收机的架构越来越丰富,面向不同应用需求存在不同的架构设计,比如单天线普通导航型接收机、抗干扰阵列天线接收机、高精度测量型接收机、低成本应用型接收机[23]等。不同卫星导航接

收机虽然架构不同,但是都会存在至少一个接收天线、射频模块和基带处理环节。除了接收天线和射频模块以外,基带处理环节按照功能可划分为捕获、跟踪、检测等模块,如图1所示。其中,捕获模块的主要功能是检测信号有无并提供粗同步信息,跟踪模块根据捕获模块输出的粗同步信息进行精准的时空信息测量和输出电文信息,检测模块能够检测接收信号中是否存在欺骗干扰信号甚至鉴别信号真伪等。

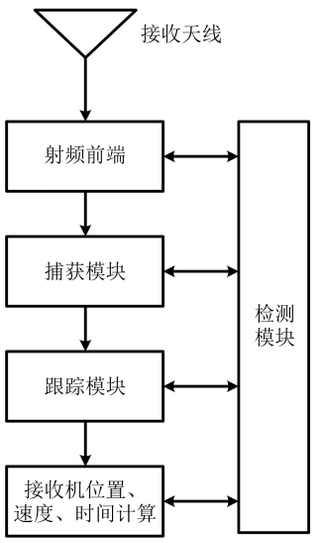

图 1　卫星导航接收机处理架构

Fig. 1　Architecture of Satellite Navigation Receivers

本文重点介绍检测模块。检测模块主要以信号特征空间为输入,设计满足一定指标需求的特征映射函数 T_R,即:

$$T_R\left(x(t,\tilde{\boldsymbol{a}})\right)\sim\begin{cases}f_{H_0}\left(T_R\left(x(t,\tilde{\boldsymbol{a}})\right)\right)\\f_{H_1}\left(T_R\left(x(t,\tilde{\boldsymbol{a}})\right)\right)\end{cases}\tag{6}$$

式中,H_0表示无欺骗干扰存在;H_1表示有欺骗干扰存在;$f_{H_0}\left(T_R\left(x(t,\tilde{\boldsymbol{a}})\right)\right)$表示无欺骗干扰时检测特征量的概率密度函数;$f_{H_1}\left(T_R\left(x(t,\tilde{\boldsymbol{a}})\right)\right)$表示欺骗干扰存在时检测特征量的概率密度函数。

与真实信号检测概率与虚警概率类似,欺骗信号的检测概率和虚警概率也可以由常用的纽曼-皮尔逊检测规则导出,其约束了虚警错误导致的损失,使检测概率达到最大,即:

$$P_D\left(T_R\left(x(t,\tilde{\boldsymbol{a}})\right)\right)=\int_{\lambda_R}^{\infty}p\left(T_R\left(x(t,\tilde{\boldsymbol{a}})\right)\middle|H_1\right)\mathrm{d}\tilde{\boldsymbol{a}}\tag{7}$$

$$P_F\left(T_R\left(x(t,\tilde{\boldsymbol{a}})\right)\right)=\int_{\lambda_R}^{\infty}p\left(T_R\left(x(t,\tilde{\boldsymbol{a}})\right)\middle|H_0\right)\mathrm{d}\tilde{\boldsymbol{a}}\tag{8}$$

式中,λ_R表示欺骗干扰检测阈值;p为欺骗信号检测量的概率密度函数;$P_D\left(T_R\left(x(t,\tilde{\boldsymbol{a}})\right)\right)$表示检测概率;$P_F\left(T_R\left(x(t,\tilde{\boldsymbol{a}})\right)\right)$表示虚警概率。

1.4　欺骗对抗评估模型

欺骗对抗评估模型主要包括真实卫星导航信号、攻击方欺骗攻击信号模型和防守方反欺骗处理模型,以及无线信道引入的信号随机特征等,如图2所示。

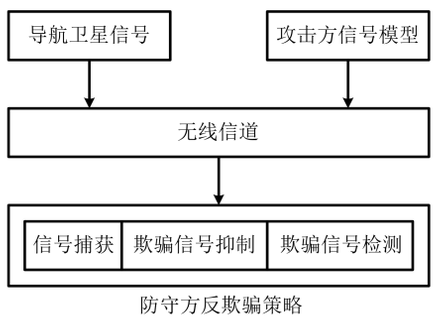

图 2　卫星导航欺骗干扰评估架构

Fig. 2　Evaluation Framework of Satellite Navigation Spoofing

攻击方信号模型和防守方反欺骗策略分别如下所示。

1)攻击方信号模型。由§1.2攻击方欺骗干扰模型可知,攻击方可以通过遍历欺骗干扰信号的功率、时延、入射角度、信号数目等参数,同时播发宽带压制干扰等手段,遍历所有可能的欺骗攻击泛函映射,使欺骗干扰信号空间“落入”真实信号空间的不确定区域内,使目标接收机无法检测和抑制欺骗干扰,达到有效欺骗目标接收机的目的。若攻击方在遍历信号参数空间的过程中,存在某一维度的参数空间无论如何取值,均不能实施有效的欺骗干扰,则此时攻击方很难对目标接收机造成影响。实施有效的欺骗干扰,需要欺骗信号功率、时延、入射角、信号数目等所有参数处于合适的信号空间,使目标接收机能够正常捕获欺骗干扰信号,且无法检测和抑制欺骗干扰信号,才有可能达到有效欺骗目标接收机的目的。

2)防守方反欺骗策略。由§1.3防守方接收处理模型可知,防守方可以通过天线、射频、捕获、跟踪等模块获取信号特征信息,设计相应的欺骗干扰检测策略,进而避免欺骗干扰对接收机的影响,最终输出真实的时空测量信息。不同的反欺骗策略一般只能应对特定的攻击场景,所以需要进行策略组合以增强接收机反欺骗能力。当欺骗攻击方设置合适的攻击参数使欺骗干扰信号“落入”真实信号空间不确定区域,即防守方接收机的欺骗对抗“盲区”时,此时防守方反欺骗策略

失效。防守方反欺骗过程就是通过不同维度的策略组合不断“修补”欺骗对抗“盲区”的过程。

2 基于欺骗有效功率可行域的欺骗干扰评估方法

本节从卫星导航欺骗对抗有效性评估准则出发,给出基于欺骗有效功率可行域的欺骗对抗评估指标与方法,对现有的指标体系进行补充,实现对欺骗对抗的攻防效果进行量化评估。

2.1 欺骗干扰有效性评估准则

目前卫星导航领域并未有文献给出欺骗对抗有效性评估准则,所以本文中参考经典电子战领域的评估准则给出卫星导航欺骗对抗评估准则[3],主要包括信息准则、功率准则、效率准则、时间准则等。

信息准则主要根据信息论计算干扰信号的熵对干扰信号进行评估。对于压制干扰信号,其熵越大则干扰信号品质越好;对于欺骗干扰信号,需要计算真实信号和欺骗信号信息熵之差,其信息熵之差越小,说明欺骗干扰信号逼近真实信号特征空间能力越强,此时防守方区分和检测干扰信号难度越大。然而,信息准则只能在相同功率条件下评估干扰信号本身优劣情况,并未考虑防守方抗干扰和反欺骗措施对干扰效果的影响,所以并不能反映真实的干扰效果。

功率准则主要根据干扰信号功率绝对值及其变化量评估干扰有效性,在理论分析和现场测试等方面较为方便,是目前应用最为广泛的准则。功率准则并非独立准则,其应用通常需要其他指标的约束,才能确定具体的功率评估结果。比如在卫星导航领域评估抗压制干扰能力时,干信比指标的给出需要一定定位精度的约束,当超过此定位精度约束时,即认为压制干扰有效。在应用功率指标评估欺骗干扰有效性时,也需要欺骗干扰检测概率等指标的约束。另外,在欺骗干扰评估当中,应当考虑存在压制干扰的情况,这是因为攻击方为了增加信号空间的不确定度,增加防守方检测难度,通常在发射欺骗干扰的同时发射压制干扰信号。

效率准则又称为概率准则,表示卫星导航接收机在特定条件下完成使命任务的能力,包括信号捕获、信号跟踪以及输出真实时空信息等能力,通常应用各类概率、偏差、标准差等形式量化表达。虽然效率准则评估结果最为客观可靠,但是在实际运用时需要大量实验结果支撑,增加了评估成本。通过对攻击方欺骗信号模型和防守方反欺骗模型进行建模,通过数学仿真实验的方式可以降低成本,提高评估效率。

时间准则可以从攻守双方的角度出发,评估两者达到对抗目标所需的时延。从防守方的角度出发,在欺骗对抗中防守方检测欺骗、输出真实测量结果需要时延;防守方接收机处理时延过大,影响了接收机正常遂行使命任务,则欺骗攻击有效。另外,在卫星导航完好性评估领域也可以发现时间准则指导下的指标,比如完好性告警时间。防守方的处理时延通常通过实测获取。

总之,在欺骗对抗过程中,攻守双方均需要同时满足一定的功率、效率和时间准则。比如,攻击方需要在一定欺骗干扰成功率的约束下,在规定的时间内释放一定功率的欺骗干扰信号达到欺骗攻击目的;若无法满足欺骗成功率,或者欺骗有效时延过久,或者释放欺骗干扰的功率过高,都不能达到有效欺骗干扰的目的,即任意一个有效性评估准则不满足对抗需求,则欺骗攻击失败。同样,防守方进行反欺骗时,也需要满足一定的功率、效率和时间准则,防守方需要在规定时间内以一定的检测概率识别出特定功率欺骗干扰信号,若检测时间过久,或者检测概率过低等,则防守方未达到反欺骗目的。

由于信号功率特征维度几乎影响所有欺骗对抗策略,是所有特征维度的“最大公约数”,而且功率空间能够直接映射到三维空间中的能量分布情况,工程应用广泛且方便,所以基于§1建立的评估模型,将其映射到功率维度上,提出了基于欺骗有效功率可行域的评估方法与指标。

2.2 欺骗干扰有效性评估方法与指标

欺骗对抗评估即建立欺骗对抗场景到欺骗对抗效果的映射过程。欺骗对抗有效性评估方法和指标函数可以表示为:

$$A=f(P_S,P_J,N_S,N_J,\theta_S,\theta_J,\tau,T) \tag{9}$$

式中,A表示欺骗对抗有效性评估指标集;f表示欺骗对抗有效评估方法映射函数;P_S表示欺骗信号等效全向辐射功率(equivalent isotropically radiated power, EIRP);P_J表示压制干扰EIRP;θ_S表示欺骗信号入射方向;θ_J表示压制干扰入射方向;N_S表示欺骗信号数目;N_J表示压制干扰数目;τ表示欺骗信号相对真实信号延迟;T表示接收机反欺骗策略集合。欺骗对抗有效性评估为欺骗对抗场景参数到欺骗对抗效果的映射。

基于§1.4中的卫星导航欺骗对抗评估模型和

§2.1 中提出的卫星导航欺骗干扰有效性评估准则，考虑到卫星导航领域信号功率低于噪声功率的特殊性，结合对抗模型中攻击方的功率空间和对抗效果中的概率准则，给出基于欺骗有效功率可行域的评估指标和方法，具体如下所示。

参考文献[3]中的传统电子战对抗评估中的表示方式，卫星导航领域的欺骗有效概率 P_j 可以表示为：

$$P_j = P_{js}P_D(1-P_{r_1})(1-P_{r_2})(1-P_{r_3}) \tag{10}$$

式中，P_D 表示欺骗信号捕获概率；P_{js} 表示欺骗干扰攻击方模拟真实信号相似程度的概率；卫星导航接收机利用空间特征检测欺骗干扰的概率为 P_{r_1}；利用时频域特征检测欺骗干扰的概率为 P_{r_2}；卫星导航接收机有效抗欺骗干扰的概率，即欺骗干扰抑制概率为 P_{r_3}。

根据上述欺骗对抗有效性评估方法和欺骗有效概率表达式，本文提出了基于欺骗有效功率可行域的欺骗对抗有效性评估指标，其表达式为：

$$\begin{aligned}&\left\{(\alpha,\beta)\middle| P_j(\alpha,\beta)=\right.\\&\left.P_{js}P_D(1-P_{r_1})(1-P_{r_2})(1-P_{r_3})\geqslant\eta\right\}\\&\text{s.t.}\begin{cases}\alpha_{\min}<\alpha\leqslant\alpha_{\max}\\ \beta_{\min}<\beta\leqslant\beta_{\max}\end{cases}\end{aligned} \tag{11}$$

式中，α 表示欺骗信号功率与真实信号功率比值，即欺信比；$\alpha_{\min}$ 和 $\alpha_{\max}$ 分别表示欺骗有效功率可行域分析欺信比的最小值和最大值，此值可以根据工程实现能力进行取值；β 表示压制干扰信号功率与真实信号功率比值，即干信比；$\beta_{\min}$ 和 $\beta_{\max}$ 分别表示欺骗有效功率可行域分析干信比的最小值和最大值；η 表示攻击方或者防守方所需的欺骗有效概率指标。总的评估功率范围可以表示为：

$$D_\Omega=\left\{(\alpha,\beta)\middle|\alpha_{\min}<\alpha\leqslant\alpha_{\max},\beta_{\min}<\beta\leqslant\beta_{\max}\right\} \tag{12}$$

欺骗有效性评估所需的功率范围的面积为：

$$A_\Omega=\iint_{D_\Omega}\mathrm{d}\alpha\mathrm{d}\beta \tag{13}$$

从欺骗有效功率可行域可以解读的信息有：

1）当 $\alpha=\alpha_{\min}$ 时，此时欺骗干扰功率较小，很难发挥欺骗干扰作用，主要起攻击作用的为压制干扰信号，此时近似为压制干扰场景；

2）当 $\beta=\beta_{\min}$ 时，此时压制干扰功率较小，主要起攻击作用的为欺骗干扰信号，此时近似为生成式欺骗干扰场景；

3）当 $\alpha=k\beta, k\neq 0$ 时，此时欺骗干扰功率与压制干扰功率等比例变化，此时近似为转发式欺骗场景，或者压制干扰与欺骗干扰同时存在的强对抗场景。

所以，通过欺骗干扰可行域可以直观分析出特定欺骗条件下生成式、转发式等典型对抗场景的欺骗有效概率。在本文当中，从防守方的角度出发，在最严苛的条件下评估欺骗对抗有效性，假设欺骗攻击方在空域特征空间能够完全复制真实信号空域特征，欺骗信号与真实信号仅存在时延和功率特征上的差异，且攻击方降低对误码率、跟踪精度的需求，则欺骗有效功率可行域评估方程可以化简为：

$$\begin{aligned}&\left\{(\alpha,\beta)\middle| P_j=P_D(1-P_{r_2})(1-P_{r_3})\geqslant\right.\\&\left.\eta,(\alpha,\beta)\subset D_\Omega\right\}\end{aligned} \tag{14}$$

在根据欺骗有效功率可行域进行欺骗对抗评估之前，需要明确欺骗风险区域划分。在本文中，不同风险区域对应的欺骗有效概率如表 1 所示。

表 1　欺骗干扰风险区域划分

Tab. 1　Area Division of Spoofing Risk

风险区域	有效概率
高风险 η_H	$\geqslant$0.9
中风险 η_M	(0.1,0.9)
低风险 η_L	$\leqslant$0.1

当攻击方能够以 90% 及以上的概率欺骗目标接收机时，此时对应的功率区域是目标接收机的高风险区域；当攻击方以不足 10% 的概率欺骗目标接收机时，此时对应的功率区域是目标接收机的低风险区域；剩余概率区间为中风险区域。高风险区域 D_H 求解方程为：

$$D_H=\left\{(\alpha,\beta)\middle| P_j(\alpha,\beta)\geqslant\eta_H,(\alpha,\beta)\subset D_\Omega\right\} \tag{15}$$

高风险区域对应的功率可行域面积 A_H 可以表示为：

$$A_H=\iint_{D_H}\mathrm{d}\alpha\mathrm{d}\beta \tag{16}$$

同理可得低风险区域 D_L 求解方程为：

$$D_L=\left\{(\alpha,\beta)\middle| P_j(\alpha,\beta)\leqslant\eta_L,(\alpha,\beta)\subset D_\Omega\right\} \tag{17}$$

低风险区域对应功率可行域面积 A_L 可以表示为：

$$A_L=\iint_{D_L}\mathrm{d}\alpha\mathrm{d}\beta \tag{18}$$

不同风险区域对总评估区域面积归一化可以表示为：

$$A'_H=\frac{A_H}{A_\Omega},A'_M=\frac{A_M}{A_\Omega},A'_L=\frac{A_L}{A_\Omega} \tag{19}$$

根据欺骗有效功率可行域和欺骗有效概率划分的欺骗干扰风险区域体现了欺骗对抗双方的目标需求。攻击方期望高风险区域D_H及其面积A_H越大越好,此时攻击方实施欺骗攻击的功率余量较大;防守方希望高风险区域D_H越小越好,低风险区域D_L及其面积A_L越大越好,此时攻击方的欺骗有效功率可行域较小,欺骗攻击实施难度较大,防守方接收机安全性较高。此时,欺骗对抗其他场景参数(欺骗干扰时延、数目、入射角等)固定,攻击方不断"扩张"欺骗有效功率可行域中高风险区域,防守方不断压缩欺骗有效功率可行域中的高风险区域,并"防守"低风险区域不被"蚕食"。根据欺骗干扰风险区域划分,则可以对不同对抗场景中的风险区域大小进行对比,实现不同欺骗对抗场景和反欺骗策略的量化性能对比。

3 仿真校验

首先需要明确仿真场景,对攻击方和防守方的模型和信号空间进行限定,然后对比理论数值计算和实际接收机策略仿真形成的欺骗有效功率可行域范围,验证其有效性。

3.1 仿真场景

本文欺骗干扰仿真场景参数设置如下:欺骗信号路数为1,欺骗信号时延为5码片,欺骗信号来向与真实信号一致,欺骗发射天线为单天线,压制干扰信号为白噪声。导航信号以L1CA为例,目标接收机采用两种策略:最大峰值捕获策略和固定载噪比检测策略。最大峰值捕获策略采用最大峰与次大峰比值作为捕获阈值,其阈值设置为典型值2.5,相干积分时间1 ms,非相干累积次数为10次,搜索步进0.5码片[24]。实际上,此时接收机并未采取任何反欺骗策略。基于固定载噪比检测欺骗信号的策略,直接对信号的载噪比估计值进行监测,若高于固定阈值则判定其为欺骗干扰信号。应用载噪比进行欺骗检测的方法是判断测量的载噪比是否超过真实信号载噪比测量值上限,所以只需真实信号功率上限的先验信息即可,而在实际环境中卫星导航信号的功率上限通常是明确的,可以根据接收机所处的实际环境进行设置。根据文献[25]的结论,在正常功率条件下本文选取载噪比固定阈值为53 dB-Hz,真实信号载噪比假设为40 dBHz。仿真实验设计示意见图3。在仿真实验中,通过遍历攻击方的功率维度,计算不同功率值下的欺骗成功概率,根据欺骗成功概率对应的功率范围计算出欺骗有效功率可行域。

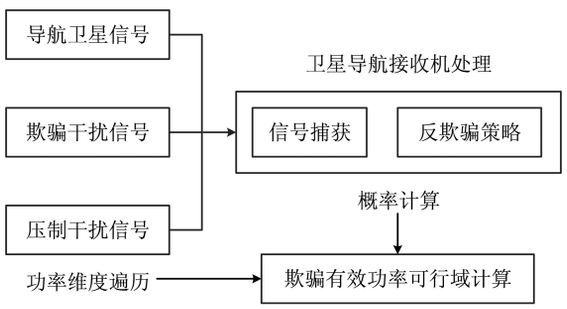

图3 仿真实验设计示意图

Fig. 3 Schematic Diagram of Simulation Experiment Design

3.2 最大峰值捕获策略

下面介绍最大峰值捕获策略欺骗对抗评估性能的理论数值计算结果和实际策略仿真结果。仿真次数为1 000次。最大峰值捕获策略欺骗有效功率可行域的理论计算公式为:

$$\left\{(\alpha,\beta)\middle|P_j=P_D(1-P_{MP})\geqslant\eta,(\alpha,\beta)\subset D_\Omega\right\} \tag{20}$$

式中,P_D为欺骗信号捕获概率;P_{MP}为经过捕获模块处理后未被欺骗的概率,即欺骗信号捕获峰值与次大峰比值未超过阈值2.5时的概率。

图4给出了最大峰值捕获策略欺骗有效功率可行域的实际策略仿真流程图。

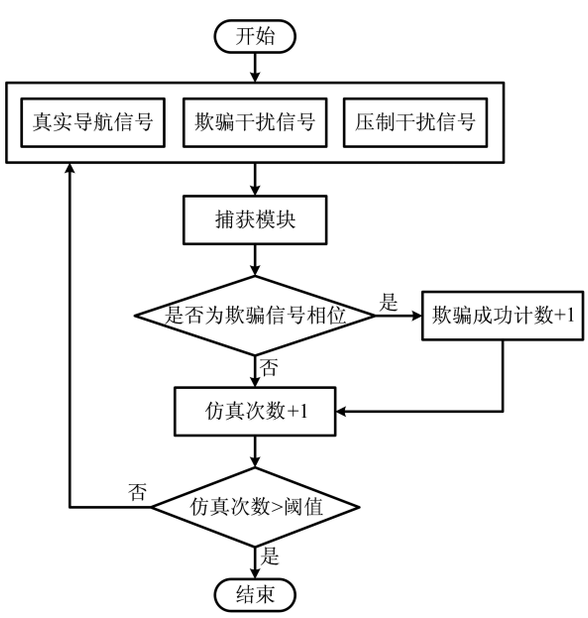

图4 最大峰值捕获策略仿真流程图

Fig. 4 Simulation Flowchart of Maximum Peak Strategy

图 5(a)为最大峰值捕获策略欺骗有效功率可行域的理论数值计算结果,实际策略仿真结果如图 5(b)所示。可以看出,当接收机采取最大峰值捕获策略时,欺骗有效概率较高的范围较大,当欺信比大于 5 dB 以上时,即可实施较高成功率的欺骗干扰。由实际策略仿真结果和理论数值计算结果对比可以看出,两者区域范围和边界特征基本吻合,验证了欺骗有效功率可行域指标的有效性。

图 5(a)右下角存在一定的欺骗有效概率较低的区域,这是因为此时压制干扰功率过高,欺骗信号也无法正常捕获。

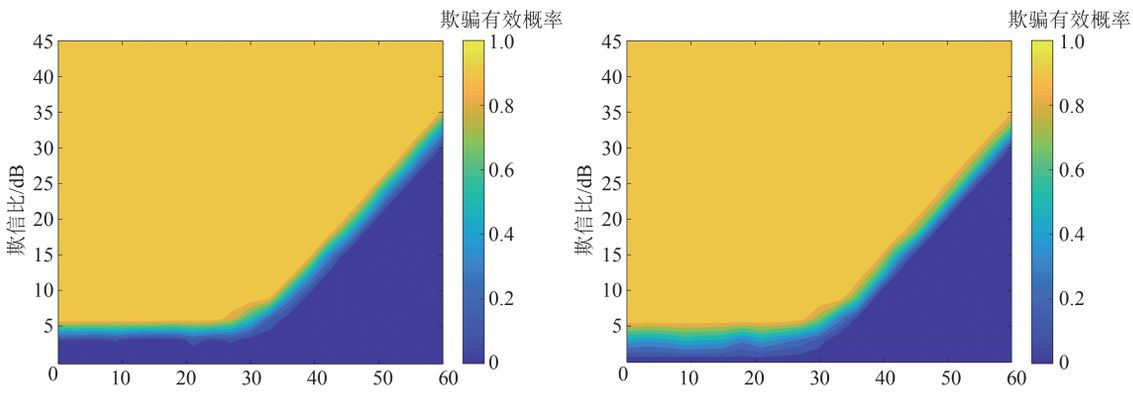

图 5　最大峰值捕获策略的欺骗有效功率可行域结果

Fig. 5　Results of Spoofing Effective Power Feasible Region of Maximum Peak Acquisition Strategy

3.3　固定载噪比策略

固定载噪比检测欺骗策略的欺骗有效功率可行域的理论计算表达式为:

$$\left\{(\alpha,\beta)\middle|P_j=P_D(1-P_{MP})(1-P_{R_1})\geqslant \eta,(\alpha,\beta)\subset D_\Omega\right\} \tag{21}$$

式中,P_{R_1}表示欺骗信号载噪比估计值超过固定阈值的概率,对应的欺骗有效功率可行域的仿真流程如图 6 所示。

固定载噪比阈值检测策略欺骗有效功率可行域的理论计算结果如图 7(a)所示,实际策略仿真结果如图 7(b)所示。可以看出,当接收机采取固定载噪比检测策略时,欺骗有效概率较高的范围相对最大峰值捕获策略有所减小;左上区域对应的欺骗有效概率较低,因为以此区域的欺骗功率配置很容易超过目标接收机的载噪比检测阈值,被目标接收机识别为欺骗干扰,所以难以有效实施欺骗干扰;右下区域对应的欺骗有效概率同样较低,这是因为此时压制干扰功率较高,欺骗信号无法正常捕获,所以欺骗干扰很难奏效。

另外,随着欺骗信号功率和压制干扰信号功率同时增加,欺骗有效概率较高的区域呈带状向右上方延伸,这是因为只要欺骗信号与压制干扰信号功率同时增大,欺骗信号载噪比估计值维持稳定,所以此时欺骗信号载噪比并未超过固定检测阈值。简单转发式欺骗干扰即为此类场景,此时攻击方将转发器射频通道热噪声和欺骗信号一同转发,导致目标接收机处估计的载噪比与正常情况下差别较小。由实际策略仿真结果和理论数值计算结果对比可以看出,两者区域范围和边界特征基本吻合,进一步验证了欺骗有效功率可行域指标的有效性。

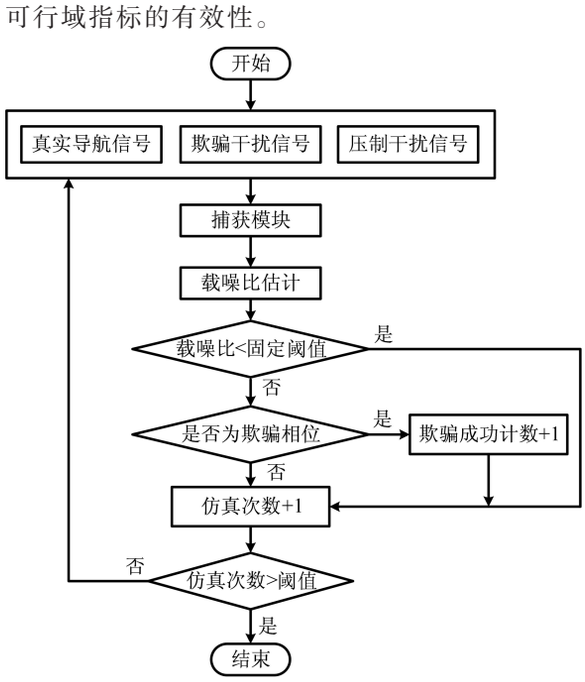

图 6　固定载噪比策略仿真流程图

Fig. 6　Simulation of Fixed Carrier-to-Noise Ratio Strategy

为了更加清晰地对比最大峰值捕获策略和固定载噪比检测策略两者的反欺骗能力,通过仿

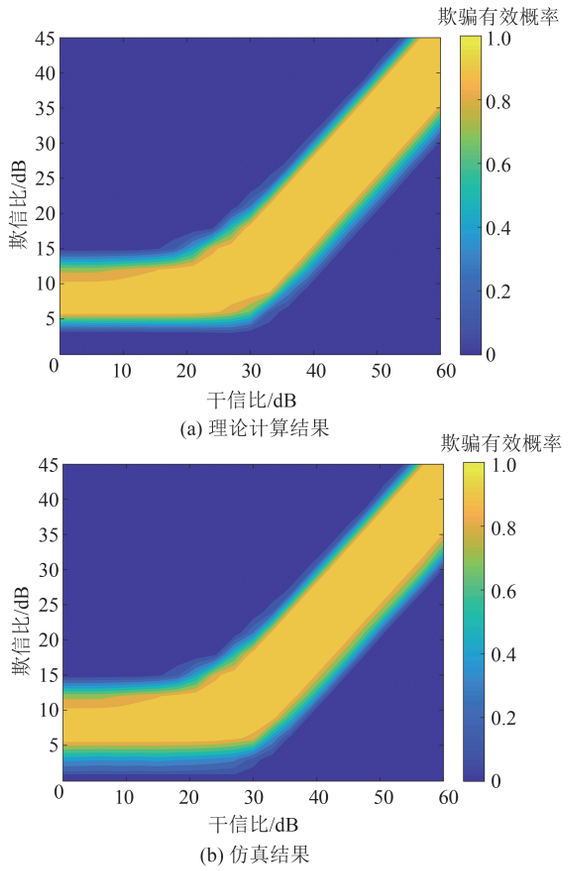

图7 固定载噪比策略的欺骗有效功率可行域结果

Fig. 7 Results of Spoofing Effective Power Feasible Region of Fixed Carrier-to-Noise Ratio Strategy

真计算两者的归一化欺骗有效功率可行域大小，其结果如图8所示。从图8可以看出，相对于最大峰值捕获策略，当接收机采取固定载噪比策略后，低风险区域增加了39.50%，高风险区域降低了44.82%。由此可以看出，当接收机采取载噪比判决时，可有效提升接收机的反欺骗能力，降低其被欺骗干扰影响的风险。

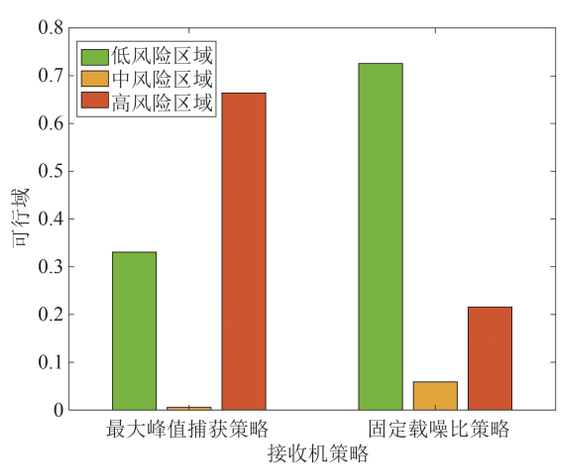

图8 欺骗有效功率可行域对比

Fig. 8 Comparison of the Spoofing Effective Power Feasible Region of Different Strategies

4 结 语

为了进一步完善卫星导航领域欺骗干扰评估方法，本文从卫星导航信号特征空间出发，将特定参数空间下的评估拓展到通过遍历信号特征空间、评估特征空间投影大小，量化评估欺骗干扰有效性和接收机反欺骗策略有效性，并在功率空间上进行了投影。根据欺骗对抗有效性评估准则和对抗场景提出了欺骗有效功率可行域的评估指标，并通过常用的欺骗干扰检测策略对其进行了仿真验证，说明了本文提出的欺骗功率可行域分析方法的有效性。同时，给出了典型对抗场景下的欺骗对抗效果量化结果。根据本文提出的评估方法，很容易将其拓展到各类欺骗干扰对抗效果的量化评估，为接收机设计反欺骗策略提供量化评估手段。

本文的评估假设欺骗攻击场景和目标接收机参数模型完全已知，但是实际对抗场景是实时动态的，部分参数未知，此时需要进行更深入的研究，提出能够应用于非完全信息下的欺骗干扰有效性评估方法。另外，在接下来研究当中，从防守方的角度出发，可以通过遍历接收机自身参数评估不同参数设计下的反欺骗性能。

参 考 文 献

[1] Huang Long, Tang Xiaomei, Wang Feixue. Anti-spoofing Techniques for GNSS Receiver[J]. *Geomatics and Information Science of Wuhan University*, 2011, 36(11): 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[J]. 武汉大学学报(信息科学版)，2011，36(11)：1344-1347.)

[2] Morton J, van Diggelen F, Spilker J, et al. Position, Navigation, and Timing Technologies in the 21st Century[M]. NewJersey: John Wiley and Sons, 2021.

[3] Wang Xuesong, Xiao Shunping, Feng Dejun. Modeling and Simulation of Modern Radar and Electronic Warfare Systems[M]. Beijing: Publishing House of Electronics Industry, 2010. (王雪松，肖顺平，冯德军. 现代雷达电子战系统建模与仿真[M]. 北京：电子工业出版社，2010.)

[4] Zhou M, Li H, Lu M Q. The Modeling and Analysis for the Assessment of GNSS Spoofing Technology[C]//China Satellite Navigation Conference, Wuhan, China, 2013.

[5] Cui Bingfu. Evaluation of Radar Anti-jamming Effectiveness[M]. Beijing: Publishing House of Electronics Industry, 2017. (崔炳福. 雷达对抗干扰有效性评估[M]. 北京：电子工业出版社，2017.)

[6] Humphreys T E. Detection Strategy for Cryptographic GNSS Anti-spoofing[J]. *IEEE Transactions on Aerospace and Electronic Systems*, 2013, 49(2): 1073-1090.

[7] Wang Yue, Hao Jinming, Liu Weiping. GNSS Spoofing Effectiveness Evaluation Based on Grey Relational Analysis and Fuzzy Comprehensive Assessment[J]. *Acta Electronica Sinica*, 2020, 48(12): 2352-2359.(王月, 郝金明, 刘伟平. 基于灰色关联分析和模糊综合评判的GNSS欺骗干扰效能评估[J]. 电子学报, 2020, 48(12): 2352-2359.)

[8] 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.

[9] Bamberg T, Appel M M, Meurer M. Which GNSS Tracking Loop Configuration Is Most Robust Against Spoofing? [C]//The 31st International Technical Meeting of the Satellite Division of the Institute of Navigation, Miami, Florida, USA, 2018.

[10] Peng C X, Li H, Lu M Q. Research on the Responses of GNSS Tracking Loop to Intermediate Spoofing [C]//The 32nd International Technical Meeting of the Satellite Division of the Institute of Navigation, Miami, Florida, USA, 2019.

[11] Humphreys T, Bhatti J, Shepard D P, et al. The Texas Spoofing Test Battery: Toward a Standard for Evaluating GPS Signal Authentication Techniques[C]//2012 ION GNSS Conference, Nashville, TN, USA, 2012.

[12] Lemmenes A, Corbell P, Gunawardena S. Detailed Analysis of the TEXBAT Datasets Using a High Fidelity Software GPS Receiver[C]//The 29th International Technical Meeting of the ION Satellite Division, Portland, Oregon, USA, 2016.

[13] Gamba M T, Truong M D, Motella B, et al. Hypothesis Testing Methods to Detect Spoofing Attacks: A Test Against the TEXBAT Datasets[J]. *GPS Solutions*, 2017, 21(2): 577-589.

[14] Albright A, Powers S, Bonior J, et al. A Tool for Furthering GNSS Security Research: The Oak Ridge Spoofing and Interference Test Battery (OAKBAT) [C]//The 33rd International Technical Meeting of the Satellite Division of the Institute of Navigation, USA, 2020.

[15] Hunter M, Fillipi F, Buesnel G. An Assessment of GNSS Receiver Behaviour in Laboratory Conditions when Subject to GPS Meaconing or Spoofing Scenarios [C]//The 33rd International Technical Meeting of the Satellite Division of the Institute of Navigation, USA, 2020.

[16] Broumandan A, Taylor T, Anklovitch D, et al. Robust Dual-Antenna Receiver: Jamming/Spoofing Detection and Mitigation[C]//The 33rd International Technical Meeting of the Satellite Division of the Institute of Navigation, USA, 2020.

[17] Pozzobon O, Sarto C, Chiara A D, et al. Status of Signal Authentication Activities Within the GNSS Authentication and User Protection System Simulator (GAUPSS) Project[C]//The 25th International Technical Meeting of the Satellite Division, Nashville, TN, USA, 2012.

[18] Huang Long, Lü Zhicheng, Wang Feixue. Spoofing Pattern Research on GNSS Receivers[J]. *Journal of Astronautics*, 2012, 33(7): 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[J]. 宇航学报, 2012, 33(7): 884-890.)

[19] Zhang X R, Li H, Yang C, et al. The Development of Real-Time Vector Receiver on Hardware Platform and the Assessment of Anti-spoofing Capability [C]//China Satellite Navigation Conference, Harbin, China, 2018.

[20] Li M H, Kou Y H, Xu Y, et al. Design and Field Test of a GPS Spoofer for UAV Trajectory Manipulation[C]//China Satellite Navigation Conference, Harbin, China, 2018.

[21] Huang L, Yang Q. GPS Spoofing Low-Cost GPS Simulator[C]//DEF Conference, Las Vegas, USA, 2015.

[22] Bao Zheng, Xie Weixin, Zhu Bin. ECCM Evaluation for Radar Systems Against Deception[J]. *Acta Electronica Sinica*, 1989, 17(6): 13-20.(保铮, 谢维信, 朱宾. 雷达系统抗欺骗型干扰性能的测度[J]. 电子学报, 1989, 17(6): 13-20.)

[23] Zhang Xiaohong, Tao Xianlu, Wang Yingzhe, et al. MEMS-Enhanced Smartphone GNSS High-Precision Positioning for Vehicular Navigation in Urban Conditions [J]. *Geomatics and Information Science of Wuhan University*, 2022, 47(10): 1740-1749.(张小红, 陶贤露, 王颖喆, 等. 城市场景智能手机GNSS/MEMS融合车载高精度定位[J]. 武汉大学学报(信息科学版), 2022, 47(10): 1740-1749.)

[24] Borre K, Akos D M. Bertelsen N, et al. Software-Defined GPS and Galileo Receiver[M]. Beijing: National Defense Industry Press, 2009.(Borre K, Akos D M, Bertelsen N, 等. 软件定义的GPS和伽利略接收机[M]. 北京: 国防工业出版社, 2009.)

[25] Dehghanian V, Nielsen J, Lachapelle G. GNSS Spoofing Detection Based on Receiver CN0[C]//ION GNSS Conference, Nashville, TN, 2012.