Review of Spoofing Detection Based on Integrated Navigation

Fang Xie[1], Honglei Lin[1], Jing Yu[1], Weihua Mou[1*]

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

drmou@163.com

Abstract: After the completion of the Beidou navigation satellite system(BDS-3), it has been widely used in various industries. However, due to the openness of civil navigation message information and the lack of security authentication mechanism, it faces the threat of information being forged and tampered with, which makes it vulnerable to spoofing attacks. How to detect spoofing signals effectively and make up for the deficiency of satellite navigation system is priority to ensure navigation safety. The spoofing detection algorithm based solely on satellite navigation is limited by the fact that satellite signals are easily affected by the environment, resulting in false alarms or missed detections. Inertial navigation system, as an autonomous and self-contained navigation, has the natural advantage of anti-spoofing. Therefore, spoofing detection algorithms based on integrated navigation have attracted more attention in recent years. Based on the influence of spoofing on the integrated navigation system, this paper analyzes the types of deception and integrated navigation system. Firstly, the current spoofing detection algorithms based on integrated navigation are classified according to the testing statistic, then sorts out and analyzes their algorithm principles, simulation results, detection indexes, application scope and limitations, and finally discusses the possible direction of algorithm improvement. This will pave the way for more advantageous spoofing detection algorithms based on integrated navigation.

Keywords: integrated navigation; Kalman filter; spoofing influence; spoofing detection algorithms

基于组合导航的欺骗检测研究综述

谢芳 [1]，林红磊 [1]，庚靖 [1]，牟卫华 [1*]

1．国防科技大学电子科学学院，长沙，中国，410073

drmou@163.com

【摘要】北斗三号全球卫星导航系统全面建成后，在各行业得到广泛应用。但由于民用导航电文信息公开,缺少安全认证机制,面临信息被伪造和篡改的威胁,容易遭受欺骗攻击。如何有效地对欺骗信号进行检测，弥补卫星导航系统的不足，是保障导航安全的首要任务。单纯基于卫星导航的欺骗检测算法，由于卫星信号易受环境影响而受限，出现虚警或是漏检的情况。惯性导航以不依赖外界、自主导航的特点有着抗欺骗的天然优势，故近些年基于组合导航的欺骗检测算法受到更多关注。本文从欺骗对组合导航系统的影响出发，对欺骗类型和组合导航系统两方面进行分析。以检验统计量为分类依据，首先对目前基于组合导航的欺骗检测算法进行分类，再对其算法原理，仿真结果，检测指标，适用范围以及局限性等进行梳理分析，最后讨论算法可能的改进方向，为后续基于组合导航更具优势的欺骗检测算法的提出作铺垫。

【关键词】组合导航；卡尔曼滤波器；欺骗影响；欺骗检测算法

1 引言

随着我国自主研发的北斗三号全球卫星导航系统的全面建成与发展，区域覆盖范围广，定位精度高且用户端价格低等诸多优点突显出来，使得北斗卫星导航系统在交通，通信，金融，电力等领域的应用愈加广泛[1][2]，为国民提供更加精准的时空信息支撑。但由于民用导航电文结构公开并且在传输过程中缺少安全认证[3]，导航信号就容易受到欺骗攻击，直接面临被篡改和被伪造的风险。用户终端在没有察觉的情况下利用错误信息进行定位，就会被拉偏到欺骗位置，存在着很大的安全隐患。那么提升卫星导航的抗欺骗能力是保障用户导航安全的当务之急。卫星导航的抗欺骗能力涉及导航系统端和接收机终端两方面，考虑到若将安全认证引入到新一代导航系统中，从发射端导航信号的结构到接收端信号的接口设计都要相应地进行改变，需要的研制周期较长，而用户对于导航信号抗欺骗能力的需求又相当迫切，那么从接收机终端提

* 通讯作者简介：牟卫华，drmou@163.com;

升抗欺骗能力就成为首要选择。接收机终端所采取的传统举措是对卫星信号功率，载噪比或相关峰等特性的检测[4][5]，以此判决欺骗的存在，发出欺骗告警，进而不再采用接收的信息进行导航定位。但是由于卫星信号功率较低的特点，使得这类只利用卫星信号的欺骗检测方法极易受到环境的影响，进而检测结果出现虚警或者漏检的情况。惯性导航是建立在物理方程的基础上推算得到用户位置信息的，不需要与外界交互，因而抗干扰能力强，具有完全自主性[6]。GNSS与IMU联合解算以检测欺骗的思想早在1995年就被提出[7]，近几年由于北斗卫星导航系统的广泛应用，欺骗检测问题被重视起来，而基于组合导航的欺骗检测算法也陆续被提出。

欺骗的引入最直观的影响即为定位结果的偏差，缓变欺骗单次误差引入小，不会引起接收机欺骗告警，多次时间累积后再比对门限又存在检测时间长[8]的问题。其检测困难大，危害程度高，是大多算法预解决的问题。缓变欺骗检测中，检验统计量的设计和检测准则的选取至关重要。能准确的检测到欺骗以及对欺骗的及时响应是重点考量的两个指标。

本文首先讨论欺骗模型，为下一阶段欺骗检测算法的设计和改进提供理论指向性；再以检验统计量的类别为依据对欺骗检测算法进行分类论述，对其算法原理，仿真结果，检测指标，适用范围以及局限性进行梳理分析；最后从欺骗检测可能改进的方向进行展望。

2 欺骗对组合导航系统的影响

2.1 欺骗类型

欺骗攻击过程可以简化为图1进行理解，欺骗设备通过加入延迟后播发，使得GNSS接收机出现错误定位结果，这种产生方式是转发式欺骗。另外还有生成式欺骗[9]，其产生的欺骗样式更丰富，比如可以生成负延时信号等。但在欺骗检测中更关注欺骗的存在性问题，算法是通过检测欺骗的影响大小来判定的，那么就可以弱化欺骗的产生方式。按照欺骗产生的误差表征分为突变式欺骗和缓变式欺骗[10]。

突变式欺骗通过引入常量延迟，造成位置，速度等组合导航解算结果的阶跃变化，检测难度低，检测技术成熟。缓变式欺骗引入的延迟是随时间连续变化的，在欺骗引入的初始时刻，组合导航输出结果与真实定位值相一致。随着引入延迟的增加，接收机解算结果发生缓慢偏移，单次检测时间内变化量小，不易被接收机察觉。故目前欺骗检测领域的研究聚焦于缓变式欺骗，也作为本文讨论的重点。

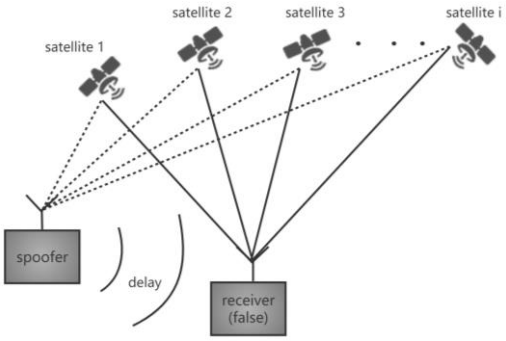

Figure 1. Spoofing attack schematic

图 1.欺骗攻击示意图

延迟可以由码相位时延或多普勒频偏实现，不同控制方式使得欺骗在系统模型上有所表征差异。码相位时延和多普勒频偏分别建模为[10]：

$$\Delta\tau = (t_s + t_p + t_d) - t_a$$

$$\Delta f = (f_s + f_d) - f_a$$

其中，$\Delta\tau$ 和 Δf 分别代表欺骗信号和真实信号之间的码相位时延和多普勒频偏，t_s 和 f_s 分别代表卫星信号到欺骗设备的传播时延和相对多普勒频移量，t_p 代表欺骗设备内部处理时延，t_d 和 f_d 分别代表欺骗设备欲增加时延和多普勒频率变化量，t_a 和 f_a 分别代表卫星信号到接收机传播时延和相对多普勒频移量。而从欺骗产生的特点，便于仿真的角度又可以得到：

$$c\Delta\tau = a_r(t - t_s) + b_r$$

$$\lambda\Delta f = a_v(t - t_s) + b_v$$

至此，通过改变 a_r 和 a_v 的值可以构建不同牵引率的欺骗检测算法验证场景。

2.2 组合导航系统

组合导航系统是以GNSS量测和惯性系统量测差值为滤波器的量测输入，以惯性器件的误差估计为状态输出，再以此为依据对惯性系统不断进行修正，惯性/GNSS组合导航系统结构如图 2所示。组合导航系统在不同参数设置下，所表现出的抗欺骗性能有所差异。

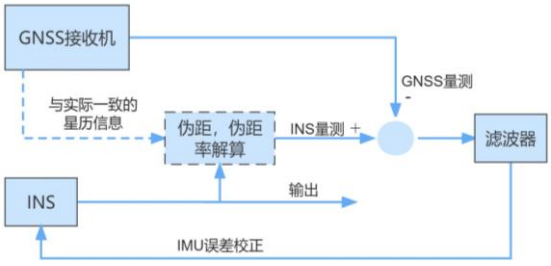

Figure 2. Inertial /GNSS integrated navigation structure diagram

图 2.惯性/GNSS 组合导航结构图

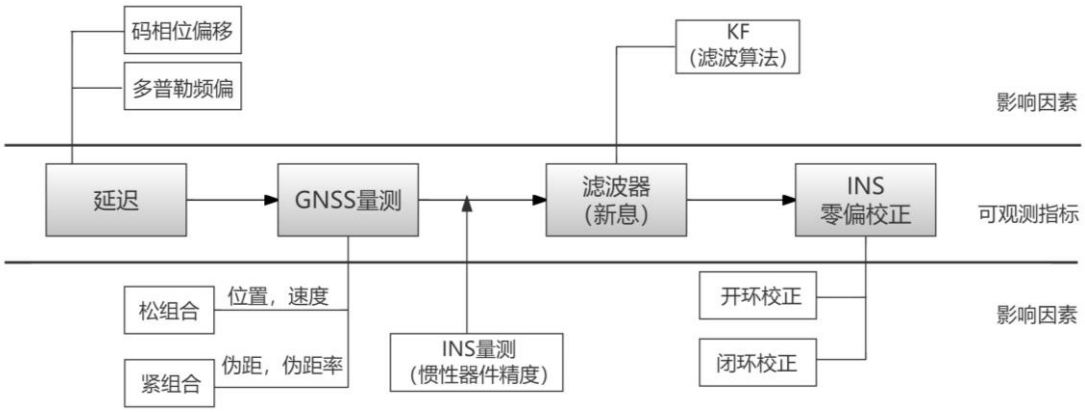

Figure 3. Error influencing factors and observable indexes

图 3.误差影响因素与可观测指标

基于文献[11]针对松组合欺骗攻击下建立的误差传递模型，本文扩充后得到组合导航系统抗欺骗性能的影响因素以及欺骗所产生误差的传递链路，如图3所示。

根据组合导航的信息融合层次可以分为松组合，紧组合以及深组合。深组合在性能方面更具优势，相对应在结构和算法方面均比松、紧组合更加复杂，目前整体研究仍存在很多问题亟待解决，故只讨论松组合和紧组合方式。文献[12]以不同欺骗牵引率对松组合和紧组合系统进行测试，分别得到欺骗攻击下位置，速度和姿态的误差。针对所关注的缓变欺骗场景，紧组合相对于松组合的误差变化率如表1所示：

Table 1. Relative error rate of loose combination and tight combination

表 1.松组合和紧组合的相对误差变化率

延迟控制方式	位置RMSE	速度RMSE	姿态RMSE
码相位延迟	-0.03%	-58.9%	8.7%
多普勒频偏	2.4%	3.97%	-5.63%

负值表示紧组合相较于松组合的误差偏移量更多。虽然紧组合方式相较于松组合方式在定位精度上更具有优势，但据表1数据显示，欺骗攻击下紧组合和松组合的平均定位精度并无明显差异。但需要注意的是，该仿真结果是在欺骗对系统所造成的影响稳定后再统计的各维度误差，那么松组合和紧组合系统对欺骗响应时间的差异是需要进一步研究的。

组合导航是数据融合的手段，其本质是对惯性导航数据和卫星导航数据之间的权重进行选择。惯性系统有不同的精度等级，按照精度从高到低可分为战略级，导航级，战术级和消费级四类[13]。文献[14]和[15]从消费级到导航级对三种不同精度IMU进行无人机欺骗测试，惯性器件精度越高，欺骗的引入速率越慢。对于低精度惯性器件，在不进行欺骗检测的情况下，用户在极短的时间内就会被诱导至欺骗位置。另外，文献[16]对比分析了不同精度IMU和不同精度接收机组合后的误差大小，发现接收机性能相较于惯性器件精度，对误差的影响更大。这是由于欺骗攻击直接作用于卫星导航，使得卫星导航数据占比更多的算法受欺骗影响相应会更大。

3 基于组合导航的欺骗检测算法

算法的检测性能与检验统计量和检测准则有着直接关系。检验统计量主要分为组合系统量测值和滤波新息值两大类；而检测准则的选取和所获得先验知识的程度有关，需要根据选取的检验统计量再具体判断。故本文将欺骗检测算法按照检验统计量的类别进行分类，再考虑目前一些基于组合导航的新型欺骗检测算法，共分为三类。

评价欺骗检测算法的性能，主要考虑以下三个指标：

Table 2. Detecting performance indicators

表 2.检测性能指标

性能指标	定义
检测时延	指实际检出欺骗时刻与欺骗引入时刻的差值。可以反映检测算法的灵敏度。
虚警率	指无欺骗攻击下，但却出现欺骗告警的概率。在多通道欺骗场景中，虚警率是衡量存在欺骗的通道对其余正常通道影响情况的重要指标。
检测概率	指欺骗攻击下，正确检测出欺骗的概率。可以反映算法的准确度与可靠性。

3.1 基于量测值的欺骗检测算法

量测值是指位置，速度，姿态，伪距以及伪距率

等导航系统的直接测量信息。德克萨斯州立大学奥斯汀分校Humphreys教授的团队12年在白沙导弹靶场对无人机开展诱骗测试，成功使其位置发生偏移；13年对游艇进行欺骗攻击，造成左向偏移3°的误差[17][18][19]。韩国大田(Daejeon)305-700卫星导航研究小组对欺骗信号影响效果进行分析，实验结果显示欺骗攻击会使伪距发生非线性变化[20]，说明了以量测信息作为欺骗检测依据的可行性。

依据卫星信号传播理论推导得到伪距真实值和欺骗值的表达式，以伪距为检验值，利用最小二乘原理实现欺骗检测[21][22]，但是基于伪距信息的欺骗检测算法对于缓变欺骗的检测效果十分有限。由于较长的检测时间导致惯性器件误差增大，后期即使不存在欺骗信号也会欺骗告警，无法进行欺骗的有效检测。对伪距方程求导得到伪距率真实值和欺骗值间的关系，欺骗会使伪距率产生附加值[23]。文献[23]利用校准后惯性导航的解算数据推算得到的伪距率和卫星导航实际测量的伪距率作差，以此构造检验统计量。假设在无欺骗信号存在时，噪声服从零均值的高斯分布，检测问题转化为高斯噪声中含有未知幅度和方差的电平检测。构造二元假设检验，得到广义似然比检验（GLRT）下的检测门限和检测概率。文献[22]和[24]仿真验证，伪距率相较于伪距检测，对于缓变欺骗更加敏感。但是当采用精度较低的惯导器件时，其本身参数漂移会对量测值的判决产生直接影响，造成漏检或是虚警。

针对以上问题，文献[25]同时利用伪距和伪距率信息，评价时间序列的拟合程度以反映欺骗的存在情况。文献[26]和[27]中分析，欺骗攻击在使伪距和伪距率发生变化的基础上，导航解算接收机的钟差和钟漂会和真实值产生一定的偏差，利用钟差等效距离偏差和其变化率进行一致性检测。以上算法均通过增加比对信息的方法弥补了单一量测检验算法的缺限。

另外，姿态也是一个可以检测的维度。Swaszek P F等人利用载体做俯仰和横滚运动，发现欺骗攻击会使GNSS生成的轨迹和惯性导航输出的轨迹产生差异[28]；而文献[14]基于无人机载体进行实验测试发现，相较于俯仰角和横滚角，欺骗攻击对航向角的影响甚微。一定程度上，也是对文献[28]实验的说明和改进。

综合来看，这类算法具有以下特点：①无论是利用位置还是伪距或是其它数据，基于量测值的欺骗检测算法，其检测性能受限于惯性器件的精度，但是检测量易获取，原理简单，算法易实现。欲直接利用量测信息进行检测，就必须要打破这一瓶颈，目前学者们是通过增加数据比对维度进行改进的；②检测准则的选取固化。GLRT是用最大似然估计取代了未知参数，保证检测概率和虚警率近似最佳。而在欺骗检测问题中，检测时延也是一个重要指标，在选取检测准则时，同样需要考虑。

3.2 基于滤波新息的欺骗检测算法

卡尔曼滤波中的新息定义为量测的预测误差，而欺骗直接作用于量测值，使得新息会发生明显变化，对新息统计特性持续监测可能会检测出欺骗。

文献[29]分析滤波过程得到结论：欺骗攻击对滤波误差方差阵不产生影响；新息的期望值因欺骗引入随即发生变化。并且仿真表明在欺骗刚发生的一小段时间里，新息变化最为剧烈。因为滤波器的反馈校正机制[30]，新息总是朝着期望为零的方向动态调整变化的。也就是说，欺骗对新息的影响是有作用时间的，后续依据新息特性检测欺骗时需要考虑检测时限的问题。

但是针对缓变式欺骗，仅利用当前时刻的新息作为检验统计量，动态幅度小使得检测效果并不理想。有学者提出“检测窗口”的思想[31]，即对一段时间内的新息进行累积检验。但新息对欺骗的跟踪作用本身会使新息的累积效果减弱，降低了新息对欺骗的敏感性，无法最大程度的对误差进行累积。所以这种改进对缓变欺骗检测效果并不显著，且存在较大的时间延迟问题。另外，有学者进行多路欺骗仿真实验，发现异常观测值也会作用于其它无欺骗通道，产生耦合影响。欺骗对其他通路的影响本质上是因为量测值的异常会引起状态估计的偏差，由于闭环反馈校正方式使得对惯性器件参数的偏移进行修正时引入了误差。

抗差估计是在实际模型与理想模型有很大偏离的情况下，估计值仍能保持较好的指标，并不会受到破坏性影响的一类估计方法[32]。学者们基于抗差估计理论，使用IGG-3等价权函数，设定两个阈值，分为三段处理量测值。对判定异常的量测值降权处理以消除或削弱误差对状态估计的影响，进而避免对其它通路产生污染。文献[33]提出新息优化的抗差估计欺骗检测算法，从测量层面构建欺骗干扰模型优化新息。仿真加入的缓变欺骗，在多路欺骗仿真中，新息抗差估计算法相较于传统新息检测算法，其余正常通道的新息值并未发生偏移，虚警率和漏检率大幅度降低，验证了抗差估计算法使得欺骗攻击对其他正常通道的干扰影响有显著抑制作用，但检测时间并未发生变化。也有学者直接从系统结构出发，采用开环校正方式[34]，再对新息进行累加检验。仿真结果显示，相较于传统闭环校正方式的新息卡方检测法，检测时间明显缩短，时延平均降低了25%。在欺骗检测中，解决缓

变欺骗误差累积慢，检测时延大，多路耦合的问题，此方法确实奏效。但是开环结构对于惯性器件参数漂移无修正作用，长时间使用势必造成滤波器性能的下降。

虽然“检测窗口”的引入使检测性能在一定程度上有所提升，但是窗口长度和检测时间以及检测概率有着直接关系。增加窗口长度会使检测时间相应变长但检测概率提升，所以选择窗口长度时就需要在两个检测性能之间权衡。文献[35]提出基于新息速率的抗差估计算法，采用归一化新息的变化速率作为检验统计量。该算法对新息变化的趋势进行判断，相较于误差累积到一定门限值的传统检测算法，检测时间缩短60%了以上。另外，仿真结果表明抗差效果会随着等价权因子降至0的速率而变化，降得越平缓效果越差。那么可以对等价权函数进行改进，以增强抗差性能。

文献[36]针对传统新息抗差估计检测算法的检测时延问题，建立了一种模式调节准则：在新息需要降权处理也就是量测值可能存在异常时使用滑动窗口检测，其余时刻采用当前时刻新息。通过两个模式的切换，减小过去观测量的计算负担，进而缩短一定的检测时延。并且仿真结果显示，该算法针对间歇性欺骗攻击的检测灵敏度高。相较于传统新息抗差估计检测算法，欺骗消失后系统随即恢复，在下一次欺骗攻击时，响应速度更快。

3.3 基于组合导航的其它欺骗检测算法

多径效应和缓变式欺骗具有相似的特点，有学者考虑借鉴多径检测的方法。多径估计延迟锁定环路(MEDLL)可以同时估计出多径信号和直达信号参数，但却无法加以区分。利用MEDLL算法，估计接收信号的全部参数，若有两个不一致参数产生，则说明有欺骗存在[37][38]。基于MEDLL的GNSS/INS算法，MEDLL估计的信号参数生成两组伪距信息与惯性系统输出数据推算的伪距进行比较，实现欺骗信号的辨识。该算法不仅可以实现欺骗信号的检测，更突出的优势是其还可以对欺骗攻击起到一定的抑制作用。将码相位差平均变化作为欺骗检测量[39][40]，以公开数据集进行测试，结果显示所提出的算法可以将欺骗攻击对位置的误差由600m抑制在10m，并且GNSS接收机失锁90s后，定位结果仍能保持一定的精度[39]。

近些年深度学习的飞速发展，不少学者探索将神经网络用于欺骗检测问题当中。文献[41]针对转发式欺骗，利用概率神经网络（Probabilistic Neural Network, PNN）收敛迅速，分类准确率高的特点，解决载波相位差分检测算法解算整周模糊度时间长的问题[42]。在伪距定位解算过程中，针对缓变式欺骗难以被识别的困难，同样可以考虑以神经网络的方法去解决[43]。需要明晰的是，神经网络前期很重要的是对模型的训练，当出现的欺骗类型与训练序列不一致时，此时的网络很可能不再适用；同时该类算法的计算量相较于其他算法是指数倍的增加。

总的来说，这类算法是将具有突出优势的一些算法与基于组合导航的欺骗检测算法相结合，实现多源融合检测。

4 展望

目前，基于组合导航的欺骗检测已经有了一定程度的研究，但是仍有一些问题值得继续探讨，基于组合导航的欺骗检测呈现出以下发展方向：

1)缩短检测时延。针对缓变欺骗检测，降低组合导航系统中低精度惯导的检测时延，在获取不同先验信息的条件下，可以考虑选取更适合的检测准则；

2)多源融合检测。无论是欺骗检验统计量还是检测方法，单一的信息难以满足缓变欺骗检测的多方性能要求。增加信息层次，丰富检测方法，借鉴与缓变欺骗检测相似的问题研究，在基于组合导航的欺骗检测算法基础上，融合其它技术以获得更多维度的优势；

3)增加算法横向比对。仿真设置的组合导航系统参数有所差异，各个算法所关注的检测性能的侧重点不同，那么对算法之间的检测性能进行全面测试比对是值得进一步研究的。

References (参考文献)

[1] Ke Han, et al. A construction and inspection technology of power emergency communication system based on Beidou[J].Journal of Physics: Conference Series,2022,Vol.2378,012054.

[2] Che Xiaoxi, Lv Zhijie, Xu Haitao, et al. Exploration and thinking on the application of blockchain + Beidou navigation technology in agricultural insurance[J]. Agricultural Outlook, 2021, Vol. 17 (2):86-96.
车晓曦, 吕志界, 徐海涛等. 区块链+北斗导航技术应用在农业保险中的探索与思考[J]. 农业展望, 2021, 第17卷(2):86-96.

[3] Zhang L,Sun C,Zhao H, et al. The Derivation and Evaluation of Algorithm of Anti-spoofing Attack on Loosely/Tightly Coupled GNSS/INS Integration System[C]//China Satellite Navigation Conference(CSNC) 2020 Proceedings:Vol. Ⅲ（pp.691-700）.

[4] Jafarnia-Jahromi A, Broumandan A, Nielsen J, et al. Pre-Despreading Authenticity Verification for GPS L1 C/A Signals[J]. Navigation, 2014, 61(1):1-11.

[5] Phelts R E, Enge, Per K, et al. Multicorrelator Techniques for Robust Mitigation of Threats to GPS Signal Quality[D]. Stanford University. 2001.
[6] Yan G G. Research on Vehicle Self positioning and Orientation System [D]. Northwestern Polytechnical University, 2006.
严恭敏. 车载自主定位定向系统研究[D].西北工业大学,2006.
[7] Key E L. Techniques to Counter GPS Spoofing[R]. MITRE Corporation, 1995.
[8] Liu H， Gang Z， Wang H , et al. Research on integrity monitoring for integrated GNSS/SINS system[C]// The 2010 IEEE International Conference on Information and Automation.
[9] Khan A M， Iqbal N， Khan M F . Synthetic GNSS Intermediate Spoofing Data Generation using Field Recorded Signals[J]. MethodsX, 2018, 5:1272-1280.
[10] Zhang C, Lv Z W, Zhang L D, et al. Influence of deception jamming on positioning performance of GNSS/INS system[J]. Journal of Navigation and Positioning, 2022 (004): 010.
[11] Shi M, Mou J Y, Chen S X. GPS/INS integrated navigation deviation analysis under GPS deception [J].Electro Optics and Control, 2016, 23 (2): 5.
史密, 牟京燕, 陈树新. GPS诱骗下GPS/INS组合导航偏差分析[J]. 电光与控制, 2016, 23(2):5.
[12] Zhang C, Lv Z W, Ke Y, et al Comparison of GNSS/INS loose combination and tight combination under the influence of deception jamming [J]. Journal of Navigation and Positioning, 2022 (005): 010.
[13] Shin E H . Accuracy Improvement of Low Cost INS/GPS for Land Applications[J]. sheimy, 2001.
[14] Guo Y. Research on UAV covert deception method under INS/GNSS integrated navigation mode [D]. National University of Defense Technology, 2019.
郭妍. INS/GNSS 组合导航模式下无人机隐蔽性欺骗方法研究[D]. 国防科学技术大学,2019.
[15] Yang L， Fu Q， Li S , et al. The Effect of IMU Accuracy on Dual-antenna GNSS Spoofing Detection[C]// ION ITM 2016. 2016.
[16] Manickam, Sashidharan, O'Keefe, et al. USING TACTICAL AND MEMS GRADE INS TO PROTECT AGAINST GNSS SPOOFING IN AUTOMOTIVE APPLICATIONS.[J]. Gps World, 2016.
[17] Humphreys T E， Ledvina B M， Psiaki M L , et al. Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer[C]// International Technical Meeting of the Satellite Division of the Institute of Navigation. 2008.
[18] Psiaki M L , O'Hanlon B W , Powell S P , et al. GNSS spoofing detection using two-antenna differential carrier phase[J]. Programme & Abstracts the Volcanological Society of Japan, 2014, 2010(5):342－344.
[19] 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 (ION GNSS+ 2013). 2013.
[20] Jeong S， Lee S， Kim J . [IEEE 2014 14th International Conference on Control, Automation and Systems (ICCAS) - Gyeonggi-do, South Korea (2014.10.22-2014.10.25)] 2014 14th International Conference on Control, Automation and Systems (ICCAS 2014) - Spoofing detection module test of GPS Jamming monitoring system[J]. 2014:1010-1013.
[21] Liu K, Wu W Q, Tang K H, et al. Anti forwarding Deception Jamming Detection Algorithm for GNSS Dual Receivers Based on Pseudo range Information [J]. Systems Engineering and Electronics, 2017, 39 (11): 6.
刘科, 吴文启, 唐康华,等. 基于伪距信息的 GNSS 双接收机抗转发式欺骗干扰检测算法[J]. 系统工程与电子技术, 2017, 39(11):6.
[22] Chu F， Li H， Wen J , et al. Statistical Model and Performance Evaluation of a GNSS Spoofing Detection Method based on the Consistency of Doppler and Pseudorange Positioning Results[J]. The Journal of Navigation, 2019, 72(2):447-466.
[23] Chang H W, Pang C L, Zhang L, et al INS assisted BDS pseudo range rate consistency deception signal detection method [J]. Journal of Air Force Engineering University, 2022 (004): 023.
常浩伟, 庞春雷, 张良,等. INS辅助的BDS伪距率一致性欺骗信号检测方法[J]. 空军工程大学学报, 2022(004):023.
[24] Wu Z J. Research on Inertial Assisted GNSS Induced Deception Detection Algorithm [D]. National University of Defense Technology, 2018.
武智佳. 惯性辅助 GNSS 诱导式欺骗检测算法研究[D].国防科技大学, 2018.
[25] Wu Z J, Wu W Q, Liu K, et al. Research on gradually induced deception detection algorithm based on INS/GNSS tight coupling combination [J]. Navigation, Positioning and Time Service, 2019, 6 (1): 7.
武智佳, 吴文启, 刘科,等. 基于 INS/GNSS 紧耦合组合的逐步诱导式欺骗检测算法研究[J]. 导航定位与授时, 2019, 6(1):7.
[26] Liu Y, Li S H, Fu Q W, et al. Chip level atomic clock assisted deception detection method for inertial/satellite integrated navigation system [J]. China Journal of Inertial Technology, 2019, 27 (5): 7.
[27] Liu K. Research on GNSS Deception Jamming Detection Algorithm and Experimental Verification Method [D]. National University of Defense Technology, 2019.
刘科. GNSS欺骗干扰检测算法与实验验证方法研究[D]. 国防科学技术大学, 2019.

[28] Swaszek P F， Pratz S A， Arocho B N，et al. GNSS Spoof Detection Using Shipboard IMU Measurements[C]// 2014:745-758.
[29] Liu Y, Li S, Fu Q, Liu Z. Impact Assessment of GNSS Spoofing Attacks on INS/GNSS Integrated Navigation System[J]. Sensors. 2018; 18(5):1433.
[30] Zhong L， Liu J， Li R，et al. Approach for Detecting Soft Faults in GPS/INS Integrated Navigation based on LS-SVM and AIME[J]. Journal of Navigation, 2017, 70(3):1-19.
[31] Zhang C， Zhao X， Pang C，et al. Improved Fault Detection Method Based on Robust Estimation and Sliding Window Test for INS/GNSS Integration[J]. Journal of Navigation, 2020, 73(4):1-21.
[32] Yang Y X. Robust estimation theory and its application [M]. August First Press, 1993.
杨元喜. 抗差估计理论及其应用[M]. 八一出版社, 1993.
[33] Ke Y, Lv Z W, Zhou W L, et al Deception detection algorithm of innovation optimized robust estimation of GNSS/INS compact combination [J] Chinese Journal of Inertial Technology, 2022 (002): 030.
柯晔, 吕志伟, 周玟龙,等. GNSS/INS 紧组合的新息优化抗差估计欺骗检测算法[J]. 中国惯性技术学报, 2022(002):030.
[34] Zhong L L, Liu J P. Research on Deceptive Jamming Detection Technology Based on Tight Integrated Navigation [C]//. Proceedings of the Fifth China Aviation Science and Technology Conference, 2021:426-431.
钟伦珑,刘炅坡. 基于紧组合导航的欺骗式干扰检测技术研究[C]//.第五届中国航空科学技术大会论文集.,2021:426-431.
[35] Zhang C, Lv Z W, Zhang L D, et al. Deception detection algorithm of INS/GNSS integrated navigation system based on robust estimation of innovation rate [J]. Chinese Journal of Inertial Technology, 2021,29 (3): 6.
张超, 吕志伟, 张伦东,等. 基于新息速率抗差估计的 INS/GNSS 组合导航系统欺骗检测算法[J]. 中国惯性技术学报, 2021, 29(3):6.
[36] Ren L J, Zhao X B, Pang C L, etc Improved GNSS/INS integrated navigation integrity monitoring method based on robust estimation [J] Aerospace Control, 2021 (039-005).
任利简, 赵修斌, 庞春雷,等. 基于抗差估计改进的GNSS/INS组合导航完好性监测方法[J]. 航天控制, 2021(039-005).
[37] Meng Z， Ma T， Hong L，et al. The Method of Receiver-Spoofer Signal Mitigation Based on Multi-correlator[C]// ION 2017 Pacific PNT Meeting. 2017.
[38] Xu R, Ding M Y, Meng Q, etc MEDLL assisted identification method for deception signal of GNSS/INS system [J] China Journal of Inertial Technology, 2018, 26 (2): 8.
许睿, 丁梦羽, 孟骞,等. MEDLL辅助的GNSS/INS系统欺骗信号辨识方法[J]. 中国惯性技术学报, 2018, 26(2):8.
[39] Shang X Y, Sun F P, Zhang L D, et al INS assisted GNSS deception jamming identification and suppression method [J] Chinese Journal of Inertial Technology, 2022 (002): 030.
商向永, 孙付平, 张伦东,等. INS辅助的GNSS欺骗干扰辨识与抑制方法[J]. 中国惯性技术学报, 2022(002):030.
[40] Shang X， Sun F， Zhang L，et al. Detection and mitigation of GNSS spoofing via the pseudorange difference between epochs in a multicorrelator receiver[J]. GPS Solutions, 2022, 26(2):1-14.
[41] Pang Chunlei, Guo Zehui, Lv Minmin, et al. Beidou Forward Spoofing Signal Detection Method based on PNN[J]. Chinese Journal of Inertial Technology, 2021,29(04):554-560.
庞春雷,郭泽辉,吕敏敏,等.基于PNN的北斗转发式欺骗干扰信号检测方法[J].中国惯性技术学报，2021,29(04):554-560.
[42] Y. Zhang, C. Shen, J. Tang and J. Liu, "Hybrid Algorithm Based on MDF-CKF and RF for GPS/INS System During GPS Outages (April 2018)," in IEEE Access, vol. 6, pp. 35343-35354, 2018.
[43] Rui, Cheng, Qi, et al. A Novel Online Data-Driven Algorithm for Detecting UAV Navigation Sensor Faults[J].Sensors, 2017,Vol. 17, Pages 2243.