基于KL 散度的紧组合导航欺骗式 干扰检测方法



钟伦珑¹,刘永玉¹,李雪艳² 1.中国民航大学智能信号与图像处理天津市重点实验室,天津 300300 2.中国民航大学,天津 300300

摘 要:蓄意的欺骗式干扰可诱导机载全球导航卫星接收机定位结果偏离真实位置,给民航飞行安全带来极大的风险。针 对欺骗式干扰隐蔽性强、难以被检测的问题,基于机载导航系统体制,本文提出了一种基于KL散度的欺骗式干扰检测方法。 基于机载紧组合导航系统滤波器新息数据,利用卫星受欺骗与否时新息可能存在的两种概率密度分布,构建基于KL散度的 欺骗检测统计量,进行欺骗式干扰检测。仿真结果表明,与传统新息序列卡方检测方法相比,基于KL散度的欺骗式干扰检 测方法提高了算法对缓变式欺骗干扰和微小突变式欺骗干扰的检测能力,降低了欺骗检测的漏警率。

关键词:全球导航卫星系统;欺骗式干扰;紧组合导航系统;新息;Kullback-Leibler散度

中图分类号:TN713

文献标识码:A

全球导航卫星系统(GNSS)为航空领域提供覆盖全球 的高性能导航信息。国际民航组织(ICAO)将其选作新一 代区域导航系统的主用系统,规定使用民用GNSS信号进 行导航。但是,由于民用GNSS信号的码字信息和信号结 构是公开的,GNSS导航容易受到蓄意的欺骗式干扰影 响^[1-2]。及时、有效的欺骗式干扰检测技术对民航飞行安全 至关重要。根据检测数据的来源不同,机载欺骗式干扰检 测技术可分为基于信号处理的检测技术^[3-4]和基于信息解 算^[5-6]的检测技术。与基于信号处理的检测技术相比,基于 信息解算的检测技术无须改变接收机的结构^[7],可融合其 他无干扰的传感器信息,提高算法检测性能,且可嵌入机载 组合导航算法中,便于在区域导航计算机中实现。

典型的基于信息解算的欺骗式干扰检测技术对卫星导航和其他传感器信息进行一致性检测^[8],如基于GNSS和惯性导航系统(INS)紧组合导航的欺骗式干扰检测技术^[9],利用INS不受欺骗式干扰影响的特点,使用卡尔曼滤波等方式融合GNSS测量信息和INS导航信息,再结合适当的检测方法判断GNSS测量信息和INS导航信息的一致性,实现欺骗式干扰检测。传统的新息序列卡方检测方法直接以

DOI: 10.19452/j.issn1007-5453.2022.11.011

组合导航滤波器新息构建卡方检测统计量,但卡方检测容 易扩大检测区域,导致对微小欺骗量检测延时较大,漏警率 较高。为提高算法性能,Bhatti¹⁰⁰提出将新息的变化率作为 检测统计量,张超¹⁰¹提出将抗差估计与新息卡方检测算法 相结合。两种方法重新构建基于新息的欺骗检测统计量, 提高了对欺骗的检测效果,但仍不满足 ICAO 对巡航阶段 的告警时间要求。

KL散度是基于数理统计方法的重要概念之一,能够有 效描述样本数据可能存在的两个概率密度分布之间的差 异。曹玉苹^[11]等提出基于KL散度的无迹卡尔曼滤波的过 程故障检测方法,能够及时检测出故障的发生。基于故障 检测思想^[12],针对GNSS欺骗式干扰威胁民航飞行安全问 题,本文引入KL散度算法,基于紧组合导航滤波过程判断 GNSS是否受到欺骗式干扰。首先使用扩展卡尔曼滤波器 进行GNSS的观测数据和INS的导航数据融合。然后在紧 组合系统滤波器输出新息的概率密度分布基础上,构建基 于KL散度算法的检测统计量,进行GNSS欺骗式干扰检 测。最后进行仿真试验验证本文所提方法的有效性。

收稿日期: 2022-05-26;退修日期: 2022-07-19;录用日期: 2022-09-15 基金项目:航空科学基金(201908067001)

引用格式: Zhong Lunlong, Liu Yongyu, Li Xueyan. Spoofing Interference detection method based on KL divergence for tightly-coupled navigation system[J]. Aeronautical Science & Technology, 2022, 33(11):76-83. 钟伦珑, 刘永玉, 李雪艳. 基于KL 散度的紧组合导航 欺骗式干扰检测方法[J]. 航空科学技术, 2022, 33(11):76-83.

1 基于伪距测量的欺骗式干扰模型

GNSS 欺骗式干扰的根本目的是对用户接收机造成恶意攻击,使用户接收机捕获到虚假的干扰信号,形成错误的测量伪距,导致接收机定位结果偏离真实的用户目标位置^[13]。根据 GNSS 基本原理^[14],用户接收机 *R* 与第*j* 颗可见卫星的伪距测量值 *ρ*,为

 $<math>
 \rho_j = r_j + \delta t_u - v_\rho$ (1) 式中, r_j 为用户接收机 R 到第 j 颗可见卫星的真实距离; δt_u 为 GNSS 接收机时钟误差的等效距离; v_ρ 是接收机内部噪声与 GNSS 测量噪声总和, $v_\rho \sim N(0, \sigma_G^2)$, σ_G 为伪距测量噪声标 准差。

欺骗式干扰使用户接收机定位结果偏离真实位置的关键是在伪距测量值上引入了附加的伪距欺骗量。当存在欺骗式干扰时,受附加的伪距欺骗量的影响,第*j*颗可见卫星的伪距测量值变为

$$\rho_j = r_j + \delta t_u - v_\rho + \Delta \rho_j \tag{2}$$

式中, $\Delta \rho_j$ 为欺骗式干扰引入的附加伪距。当 $\Delta \rho_j = a(a)$ 常 值)时,存在突变式欺骗干扰;当 $\Delta \rho_j = v(t-t_s)$ 时,存在缓变式 欺骗干扰,v为伪距欺骗速率,t为导航时间, t_s 为欺骗发生 时刻。

2 基于紧组合导航的欺骗检测系统模型

GNSS和INS 紧组合导航是基于伪距、伪距率的组合导航方式^[15]。相对于其他组合导航方式,紧组合导航有更高的精度和更强的抗干扰能力。在GNSS/INS 紧组合导航系统中嵌入欺骗式干扰检测算法,利用卡尔曼滤波器新息的概率密度分布,构建基于KL 散度算法的检测统计量,实现欺骗式干扰检测功能。检测无欺骗时系统校正INS进行组合导航输出,否则系统进行欺骗异常告警。设计的基于紧组合导航的欺骗检测系统模型如图1所示。

2.1 紧组合导航系统状态方程

GNSS/INS 紧组合导航系统的状态量由 INS 的误差状态和 GNSS 的误差状态构成,包括 18 维的 INS 误差状态和 二维的 GNSS 误差状态。由紧组合导航系统理论可知^[16], 系统状态方程为

$$X = FX + GW \tag{3}$$

式中,**F**为状态转移矩阵;**G**为系统噪声矩阵;**W**为系统噪声矢量;**X**为系统状态量。

$$\boldsymbol{X} = [\boldsymbol{\phi}_{E}, \boldsymbol{\phi}_{N}, \boldsymbol{\phi}_{U}, \delta v_{E}, \delta v_{N}, \delta v_{U}, \delta_{L}, \delta_{\lambda}, \delta_{H}, \varepsilon_{bx}, \varepsilon_{by}, \varepsilon_{bz}, \varepsilon_{rx}, \\ \varepsilon_{ry}, \varepsilon_{rz}, \nabla_{x}, \nabla_{y}, \nabla_{z}, \delta t_{u}, \delta t_{ru}]^{\mathrm{T}}$$

(4)

$$g$$
 g g

式中, ϕ 为东北天方向的姿态角误差; δv 为东北天方向的速 度误差; δ 为纬经高方向的位置误差; ϵ 为INS陀螺仪误差; ∇ 为INS加速度计零偏; δt_u 为GNSS接收机时钟误差的等效 距离; δt_n 为GNSS接收机时钟频率误差的等效距离率。

interference detection system

2.2 紧组合导航系统量测方程

GNSS/INS 紧组合导航系统量测的实际观测量由伪距、 伪距率量测值构成。伪距、伪距率量测值为 INS 等效的伪 距、伪距率与 GNSS 接收机观测的伪距、伪距率之差。 INS 等效的伪距、伪距率由 INS 推算的载体位置、速度相应与星 历中卫星的位置、速度计算得到。

在地心地固坐标系下^[16],GNSS/INS紧组合导航系统量测方程为

$$Z = HX + V \tag{5}$$

式中,H为量测矩阵;V为量测噪声矢量;X为系统状态量;Z 为系统观测量,由n颗可见卫星的伪距、伪距率量测值构成,即

$$Z = [\rho_{1,1} - \rho_{G,1}, \cdots, \rho_{1,n} - \rho_{G,n}, \dot{\rho}_{1,1} - \dot{\rho}_{G,1}, \cdots, \dot{\rho}_{1,n} - \dot{\rho}_{G,n}]^{\mathrm{T}}$$
(6)

式中, $\rho_{L,j}$ 、 $\dot{\rho}_{L,j}$ ($j=1, \dots, n$)为INS 与第j颗可见卫星等效的伪距、伪距率; $\rho_{G'j}$ 、 $\dot{\rho}_{C_j}$ 为GNSS 接收机观测的第j颗可见卫星星历中原始的伪距、伪距率。

3 基于KL 散度的欺骗式干扰检测方法

图1中,卡尔曼滤波器新息为紧组合导航系统实际量 测值与预测值之差。离散化式(3)所示的状态方程和式(5) 所示的观测方程,可得

$$\begin{cases} \boldsymbol{X}_{k} = \boldsymbol{\Phi}_{k} \boldsymbol{X}_{k-1} + \boldsymbol{\Gamma}_{k-1} \boldsymbol{W}_{k-1} \\ \boldsymbol{Z}_{k} = \boldsymbol{H}_{k} \boldsymbol{X}_{k} + \boldsymbol{V}_{k} \end{cases}$$
(7)

式中,k表示当前时刻; Z_k 为系统观测量; X_k 为系统状态量; H_k 为系统观测方程; Φ_k 为状态转移矩阵; Γ_k 为噪声分配矩阵; W_{k-1} 与 V_k 是互不相关的高斯白噪声。

新息定义为

$$\delta \boldsymbol{Z}_{k} = \boldsymbol{Z}_{k} - \boldsymbol{Z}_{k|k-1} = \boldsymbol{Z}_{k} - \boldsymbol{H}_{k} \boldsymbol{X}_{k|k-1}$$

$$\tag{8}$$

式中, δZ_k 为滤波器新息矢量; Z_k 为系统观测量; Z_{kk-1} 为系统预测值; X_{kk-1} 为状态一步预测值; H_k 为系统观测方程。

紧组合导航系统的量测噪声和系统噪声均为互不相关的高斯白噪声,因此卫星未受欺骗时新息服从零均值高斯分布,卫星受欺骗时引入的附加伪距会改变新息值的均值, 但新息值依然服从高斯分布。

3.1 传统的新息序列卡方检测方法

传统的新息序列卡方检测方法利用欺骗式干扰后新息 的变化来检测干扰。若当前时刻 GNSS 受到欺骗式干扰, 则 GNSS 接收机观测的卫星伪距增大,以致滤波器实际量 测值增大。又因滤波器的预测值未受当前时刻欺骗式干扰 的影响,从而滤波器新息值增大并反映出欺骗信息。检测 统计量定义为

$$\boldsymbol{\lambda}_{k} = \sum_{i=1}^{k} \boldsymbol{\delta} \boldsymbol{Z}_{i}^{T} \boldsymbol{S}_{i}^{-i} \boldsymbol{\delta} \boldsymbol{Z}_{i}$$
(9)

式中, $S_t(t = 1, 2, \dots, k)$ 为各滤波时刻新息矢量的协方差 矩阵。

根据卡方分布分位数的计算原理,可由虚警率P_r确定 检测阈值T。

$$P(\lambda_k < T) = \int_0^T f_{\chi^2(nk)}(x) dx = 1 - P_{\rm f}$$
(10)

3.2 基于KL散度的欺骗式干扰检测方法

通过上述分析可知,卫星受欺骗前后新息的概率密度 分布是不同的。利用新息可能存在的两种概率密度分布, 本文基于KL散度构建欺骗检测统计量,将欺骗误差信息反 映为两种概率密度分布之间的"距离"大小。与上述的传统 新息序列卡方检测方法相比,此法可避免卡方检测统计量 容易扩大检测区域,导致对缓变式欺骗和微小的突变式欺 骗检测易发生漏检的问题。

KL 散度是一种衡量样本数据可能存在的两种概率密度分布之间相似度大小的方法,被广泛应用在基于数理统计研究方法的信息论领域^[17]。假设*x*存在两种可能的概率密度函数*p*(*x*)和*q*(*x*),则KL 散度为

$$D[p(x),q(x)] = \int p(x) \ln \frac{p(x)}{q(x)} dx = E\left(\ln \frac{p(x)}{q(x)}\right)$$
(11)

KL 散度描述了概率密度函数 *p*(*x*)和 *q*(*x*)之间的"距离",满足非负特性和非对称性,当且仅当描述的两个概率 密度函数完全相同时,KL 散度取到最小值0。

对第*j*颗可见星构建基于KL散度算法的欺骗检测统计 量。式(8)中,当前时刻新息矢量 δZ_k 的第*j* 行表示第*j*颗卫 星的新息值。以历史时刻到当前时刻第*j*颗卫星的新息序 列 $\{\delta Z_{i,j} t = 1, 2, \dots, k\}$ 作为KL散度算法检测样本 $x_i (i = 1, 2, \dots, k)$,当前时刻的样本均值 \bar{x}_k 和方差 σ_k^2 定义为

$$\bar{x}_{k} = \frac{1}{k} \sum_{i=1}^{k} x_{i}, \sigma_{k}^{2} = \frac{1}{k} \sum_{i=1}^{k} (x_{i} - \bar{x}_{i})^{2}$$
(12)

基于二元假设检验^[18],定义原假设 H_0 :GNSS未受欺骗, $\bar{x}_k = 0$;备择假设 H_1 :GNSS受欺骗, $\bar{x}_k \neq 0$ 。在二元假设条件下,当前时刻观测样本的概率密度函数可表示为

$$p(x_k|H_0) = \frac{1}{\sqrt{2\pi} \sigma_k} \exp\left(-\frac{x_k^2}{2\sigma_k^2}\right)$$
(13)

$$p(x_k|H_1) = \frac{1}{\sqrt{2\pi} \sigma_k} \exp\left[-\frac{(x_k - \bar{x}_k)^2}{2\sigma_k^2}\right]$$
(14)

对KL散度进行简化^[11],定义检测统计量为

$$D_{k} = \left| \ln \frac{p(x_{k} | H_{1})}{p(x_{k} | H_{0})} \right|$$
(15)

将式(13)、式(14)代入式(15),化简得到检测统计量

$$D_{k} = \left| \frac{2x_{k}\bar{x}_{k} - \bar{x}_{k}^{2}}{2\sigma_{k}^{2}} \right|$$
(16)

式中, $p(x_k|H_0)$ 为当前时刻GNSS未受到欺骗式干扰时新息的概率密度函数; $p(x_k|H_1)$ 为当前时刻GNSS受到欺骗式干扰时新息的概率密度函数; $D_k \ge 0$,当且仅当 $p(x_k|H_1) = p(x_k|H_0)$ 时, $D_k = 0$ 。

在欺骗发生后的告警时间内,若D_k > T_d,则判断第j颗 卫星受到了欺骗式干扰,否则判断第j颗卫星未受到欺骗式 干扰。检测门限T_d由虚警率P_f和漏警率P_m计算得到。

$$T_{\rm d} = 0.03 \ln \left(\frac{1 - P_{\rm m}}{4P_{\rm f}} \right) \tag{17}$$

为方便计算,式(12)中当前时刻的样本均值 \bar{x}_k 和方差 σ_k^2 由上一时刻的样本均值 \bar{x}_{k-1} 和方差 σ_{k-1}^2 递推得到。

$$\begin{cases} \bar{x}_{k} = \frac{k-1}{k} \bar{x}_{k-1} + \frac{1}{k} x_{k} \\ \sigma_{k}^{2} = \sigma_{k-1}^{2} + \frac{k-1}{k} (\bar{x}_{k} - \bar{x}_{k-1})^{2} \end{cases}$$
(18)

4 仿真结果与分析

4.1 试验设置和评价指标

模拟飞机巡航阶段中卫星受到不同的欺骗式干扰,对

比本文KL散度检测方法与传统新息序列卡方检测方法的 检测性能。设置三组仿真试验:试验1验证在突变式欺骗 条件下两种方法的检测时间;试验2验证在缓变式欺骗条 件下两种方法的检测时间;试验3验证在不同的欺骗方式 下两种方法的欺骗检测率。按照ICAO附件10标准规 定^[19],仿真实验相关参数设置见表1。

表1 仿真参数 Table 1 Simulation parameters

参数	数值
GNSS 伪距测量噪声标准差 $\sigma_{\rm G}$	30m
虛警率P _f	1.0×10 ⁻⁵
漏警率P _m	1.0×10 ⁻³

由表1的虚警率和漏警率计算式(10)和式(17)的欺骗 检测阈值。仿真中设置仰角截止角为30°,保持可见星数为 5颗,对单星施加欺骗。

试验1和试验2中分别施加突变欺骗量和缓变欺骗量, 具体的欺骗量设置见表2。

表2 欺骗量设置 Table 2 Settings of spoofing amount

施加时刻/s	突变欺骗量/m	缓变欺骗量/(m/s)
200	10	0.3
200	25	0.5
200	55	1

由于机载组合导航的卡尔曼滤波估计技术是一种最优估计,很小的欺骗量对组合导航结果影响有限,因此设置的最小突变欺骗量为10m,最小缓变欺骗量为0.3m/s。

试验3中不同欺骗方式下对每个伪距欺骗量进行100 次蒙特卡罗试验,计算欺骗检测率P

$$P = \frac{\operatorname{Num}\left[D_k > T_{d}, t_{s} \le t \le t_{s} + \Delta t\right]}{N}$$
(19)

式中, t_s 为欺骗发生时刻; Δt 为欺骗告警时间;Num $[D_t > T_d, t_s < t_s + \Delta t]$ 为成功检测的试验次数;N为蒙特卡罗试验次数。

参照ICAO附件10对巡航阶段的完好性要求,告警时 间Δ*t*取最大值30s,且告警时间内算法欺骗检测的漏警率 不能超过0.001,即在受到欺骗式干扰30s内检测算法的欺 骗检测率需超过99.9%。

4.2 仿真结果分析

(1) 试验1

分别施加10m、25m和55m的突变欺骗量,KL散度检测方法的检测统计量随时间的变化如图2所示。



由图2(a)可以看出,在第200s施加最小10m的突变欺 骗量时,KL散度检测方法的检测统计量在第213.57s超过 检测阈值,满足ICAO对巡航阶段的30s告警时间要求。对 比图2(a)、图2(b)和图2(c)可知,KL散度检测方法的检测 统计量超过检测阈值的时间随着突变欺骗量的增大而逐渐 减小,即算法的检测速度随着突变欺骗量的增大而加快。

对比KL散度检测方法与传统新息序列卡方检测方法 对不同突变欺骗量的检测时间,见表3。

表3 不同突变欺骗量的检测时间对比 Table 3 Comparison between detection time under different abrupt spoofing amounts

伪距欺骗量/m	KL 散度/s	新息序列卡方检测/s
10	13.57	_
25	3.38	22.75
55	0.18	4.10

从表3中可以看出,在相同的突变欺骗量条件下,KL 散度检测方法相较于传统新息序列卡方检测方法有效地缩 短了欺骗检测时间。特别是在10m的微小突变欺骗量情况 下,传统新息序列卡方检测方法不能检测出欺骗干扰,而 KL散度检测方法能以较快的速度检测出来。

(2) 试验2

分别施加 0.3m/s、0.5m/s 和 1m/s 的缓变欺骗量, KL 散 度检测方法的检测统计量随时间的变化如图 3 所示。

由图3(a)可看出,在第200s施加最小0.3m/s的缓变欺 骗量,KL散度检测方法的检测统计量在第225.86s超过检 测阈值。虽然欺骗检测延时较长,但仍满足ICAO对巡航 阶段的30s告警时间要求。对比图3(a)、图3(b)和图3(c), 算法的检测速度随着缓变欺骗速率的增大而加快。

对比KL散度检测方法与新息序列卡方检测方法对不同缓变欺骗量的检测时间,见表4。

从表4中可以看出,在不同的缓变欺骗量条件下,传统 新息序列卡方检测方法的检测时间均不满足ICAO对巡航 阶段的30s告警时间要求。而KL散度检测方法相对提高 了算法对缓变欺骗量的检测敏感度,加快了检测速度。

(3)试验3

根据式(19)计算每个伪距欺骗量下的欺骗检测率。如 图4所示,以5m为间隔施加突变欺骗量,对比KL散度检测 方法和新息序列卡方检测方法的欺骗检测率。新息序列卡 方检测方法的欺骗检测率在突变欺骗量为25m时收敛到 100%。而KL散度检测方法的欺骗检测率在欺骗量为10m



表4 不同缓变欺骗量的检测时间对比 Table 4 Comparison of detection time under different slowly varying amounts of spoofing

伪距欺骗量/m	KL散度/s	新息序列卡方检测/s
0.3	25.86	87.74
0.5	23.12	60.53
1.0	10.28	35.35



Fig.4 Detection rates of two methods under the condition of abrupt spoofing amounts

时即可收敛到100%,相对降低了算法对小于25m的微小欺骗量的检测漏警率。

如图 5 所示,以 0.1m/s 为间隔施加缓变欺骗量,对比 KL散度检测方法和新息序列卡方检测方法的欺骗检测率。 在施加 0.3m/s 到 1.4m/s 的缓变欺骗量时,KL 散度欺骗检测 方法的检测率明显优于新息序列卡方检测方法。当缓变欺 骗量达到 0.3m/s时,本文 KL 散度检测方法的欺骗检测率即 可收敛到 100%。而新息序列卡方检测方法的欺骗检测率 在缓变欺骗量达到 1.4m/s时才收敛到 100%。相比之下,本 文方法有效地解决了传统方法对缓变式欺骗干扰检测能力 差的问题。

由以上三组仿真试验可知,本文方法相较于传统方法 对欺骗式干扰的检测敏感度更高,检测性能更好。对于突 变式欺骗干扰,本文方法可实现10m以上的突变欺骗量的 检测。对于缓变式欺骗干扰,本文方法可实现0.3m/s以上 的缓变欺骗量的检测。



Fig.5 Detection rates of the two methods under the condition of slowly varying amounts of spoofing

5 结束语

本文基于航空运输飞机的机载电子系统体制,利用机载 GNSS 和 INS 导航数据,结合 KL 散度理论,提出一种GNSS 欺骗式干扰检测方法。试验结果表明,相较于传统方法,本文方法提高了对缓变式欺骗干扰和微小突变式欺骗干扰的检测能力。同时,本文方法以软件形式集中进行信息处理,在不增加成本的前提下提高了算法的欺骗检测率,降低了检测漏警率。

参考文献

- Rothmaier F, Chen Y H, Lo S, et al. GNSS spoofing detection through spatial processing[J]. Navigation, 2021, 68(2): 243-258.
- [2] 宋庆国.百年未有之大变局下的航空科技发展[J].航空科学 技术, 2021,32(3):1-5.

Song Qingguo. The development of aviation science and technology under changes unseen in a century[J]. Aeronautical Science & Technology, 2021,32(3):1-5. (in Chinese)

- [3] Damian M, Aurelie B, Paul R, et al. Assessment of GPS spoofing detection via radio power and signal quality monitoring for aviation safety operations. [J]. IEEE Intelligent Transportation Systems Magazine, 2020,12(3): 136-146.
- [4] Li Junzhi, Zhu Xiangwei, Ouyang Mingjun, et al. Research on multi-peak detection of small delay spoofing signal[J]. IEEE

Access, 2020,8:151777-151787.

- [5] Gu Nianzu, Xing Fei, You Zheng. GNSS spoofing detection based on coupled visual/inertial/GNSS navigation system[J]. Sensors, 2021,21(20):6769.
- [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):328-333.

Zhang Chao, Lyu Zhiwei, Zhang Lundong, et al. A spoofing detection algorithm for INS/GNSS integrated navigation system based on innovation rate and robust estimation[J]. Journal of Chinese Inertial Technology, 2021, 29(3): 328-333. (in Chinese)

[7] 刘洋,李四海,付强文,等.芯片级原子钟辅助的惯性/卫星组
 合导航系统欺骗检测方法[J].中国惯性技术学报,2019,27
 (5):654-660.

Liu Yang, Li Sihai, Fu Qiangwen, et al. Chip-scale atomic clock aided INS/GNSS integrated navigation system spoofing detection method[J]. Journal of Chinese Inertial Technology, 2019,27(5):654-660. (in Chinese)

[8] 周鹏飞.GNSS/INS组合导航抗欺骗性干扰关键技术研究[D].长沙:国防科学技术大学,2015.

Zhou Pengfei. Research on the key technology of anti-spoofing in GNSS/INS integrated navigation[D]. Changsha: National University of Defense Technology, 2015. (in Chinese)

[9] 黄盼.GPS/INS 深耦合系统抗欺骗式干扰关键技术研究[D]. 成都:电子科技大学,2014.

Huang Pan. Research on key technologies of anti-spoofing in GNSS/INS deep integrated system[D]. Chengdu: University of Electronic Science and Technology of China, 2014. (in Chinese)

- [10] Umar I B, Washington Y O, Feng S, et al. Performance of rate detector algorithms for an integrated GPS/INS system in the presence of slowly growing error[J]. GPS Solutions, 2012, 16 (3): 293-301.
- [11] 曹玉苹,田学民.基于信息散度的过程故障检测与诊断[J].浙 江大学学报:工学版,2010(7):1315-1320.

Cao Yuping, Tian Xuemin. Information divergence based Process fault detection and diagnosis[J]. Journal of Zhejiang University: Engineering Science,2010(7): 1315-1320. (in Chinese) [12] 史萌,连晓棠,王汉平,等.惯导智能故障诊断系统设计[J].航 空科学技术,2020,31(10):51-56.

Shi Meng, Lian Xiaotang, Wang Hanping, et al. Design of intelligent fault diagnosis for inertial navigation system[J]. Aeronautical Science & Technology, 2020, 31(10): 51-56. (in Chinese)

- [13] 王文益,王沛菡.基于捕获结果的GNSS欺骗式干扰检测[J]. 信号处理,2021,37(8):1460-1469.
 Wang Wenyi, Wang Peihan. GNSS spoofing interference detection based on acquisition results[J]. Signal Processing, 2021,37(8):1460-1469. (in Chinese)
- [14] 谢钢. GPS 原理与接收机设计[M]. 北京:电子工业出版社, 2009.

Xie Gang. GPS principle and receiver design [M]. Beijing: Electronic Industry Press, 2009. (in Chinese)

- [15] Ceccato M, Formaggio F, Laurenti N, et al. Generalized likelihood ratio test for GNSS spoofing detection in devices with IMU[J]. IEEE Transactions on Information Forensics and Security, 2021, 16: 3496-3509.
- [16] 武智佳.惯性辅助GNSS诱导式欺骗检测算法研究[D].长沙: 国防科技大学,2018.

Wu Zhijia. Research on inertial assisted detection algorithm for induced GNSS deception[D]. Changsha: National University of Defense Technology, 2018. (in Chinese)

- [17] 周伟,潘海鹏,吴平,等.基于DPCA和KL散度的微小故障检测方法[J].传感器与微系统,2020(3):135-138.
 Zhou Wei, Pan Haipeng, Wu Ping, et al. Tiny fault detection method based on DPCA and KL divergence[J]. Sensors and Microsystems,2020(3):135-138. (in Chinese)
- [18] 刘振华,王骥宇,吴福伟,等.信号检测中的似然比不变性及 其证明[J].现代雷达,2019,41(12):40-43.
 Liu Zhenhua, Wang Jiyu, Wu Fuwei, et al. Proof of the invariance property of Likelihood ratio for signal detection[J].
 Modern Radar, 2019, 41(12):40-43. (in Chinese)
- [19] Eugene B, Carl M, Christophe M. Cross-correlation effect of ARAIM test statistic on false alarm risk[J]. GPS Solutions: The Journal of Global Navigation Satellite Systems, 2020, 24(4): 713-732.

Spoofing Interference Detection Method Based on KL Divergence for Tightly-Coupled Navigation System

Zhong Lunlong¹, Liu Yongyu¹, Li Xueyan²

1. Tianjin Key Laboratory for Advanced Signal Processing, Civil Aviation University of China, Tianjin 300300, China

2. Civil Aviation University of China, Tianjin 300300, China

Abstract: Deliberate spoofing interference can induce the positioning results of the airborne GNSS receiver to deviate from the true position, which brings great risks to the flight safety of civil aviation. Aiming at the problem that spoofing interference is highly concealed and difficult to detect, based on the airborne navigation system, a spoofing interference detection method based on Kullback-Leibler divergence is proposed. Based on the filter innovation data of the airborne tightly-coupled navigation system, using the two probability density distributions that the innovation may exist under the condition of whether the satellite is deceived or not, a spoofing interference detection statistic based on KL divergence is constructed to detect interference. The simulation results show that, compared with the traditional chi-square detection method of innovative sequences, the spoofing interference detection method based on KL divergence improves the detection ability of the algorithm for slow-varying spoofing interference and small abrupt spoofing interference, and reduces the missed detection rate of spoofing interference.

Key Words: global navigation satellite system; spoofing interference detection; tightly-coupled navigation system; innovation; Kullback-Leibler divergence