doi:10.19306/j. cnki. 2095-8110. 2025. 03. 007

基于同相支路输出与 PCS 融合的 GNSS 欺骗检测方法

覃业梅¹,刘 毅¹,胡 勇¹,黄文娜¹,张肖龙¹,江佳升²

(1. 湖南工商大学智能工程与智能制造学院,长沙 410205;2. 长城电源技术(深圳)有限公司,广东深圳 518100)

摘 要:基于信号质量监测(SQM)的全球卫星导航系统(GNSS)欺骗检测算法具有运算量小、实时 性好等优点,但其对复杂欺骗场景的普适性并不理想。而基于绝对功率监测与 SQM 融合(PCS) 的欺骗检测算法对载波同步的欺骗场景检测效果不理想。为此,提出了一种基于跟踪环同相支路 超前及滞后输出绝对值与 PCS 融合(AELCP)的欺骗检测算法。根据欺骗信号对接收机跟踪环路 相关峰的影响特性,取同相支路超前及滞后输出的绝对值的加权并与 PCS 进行乘积运算,形成 AELCP 检测量。基于偏度和峰度指标,检验 AELCP 检测量的概率分布特性,为选取检测门限及 评估检测概率提供了理论依据。进一步对 AELCP 采用滑动平均处理,形成 AELCP-MA 检测量, 以降低噪声影响。利用美国德州大学的欺骗测试数据集(TEXBAT)中的 DS3,DS4,DS5 和 DS7 等多个场景数据,对比分析了各类算法的检测概率等性能。结果表明,与 PCS-MA,ELP-MA 和 Delta-MA 等 SQM 算法相比,AELCP-MA 算法在多种欺骗场景下均表现出更高的检测概率和稳 健性。

关键词:全球卫星导航系统;欺骗检测;偏度;峰度;滑动平均;检测概率;稳健性 **中图分类号**:TN967.1;V324.2+4 **文献标志码**:A **文章编号**:2095-8110(2025)03-0068-11

Research on GNSS spoofing detection based on fusion of in-phase branch output and PCS

QIN Yemei¹, LIU Yi¹, HU Yong¹, HUANG Wenna¹, ZHANG Xiaolong¹, JIANG Jiasheng²

 School of Intelligent Engineering and Intelligent Manufacturing, Hunan University of Technology and Business, Changsha 410205, China;

2. Great Wall Power Supply Technology (Shenzhen) Co., Ltd., Shenzhen, Guangdong 518100, China)

Abstract: The GNSS spoofing detection algorithm based on signal quality monitoring(SQM) has the advantages of low computational complexity and excellent real-time performance, but its universality for complex spoofing scenarios is not ideal. Since the spoofing detection algorithm based on power combined with SQM (PCS) shows suboptimal detection effectiveness in carrier synchronization spoofing scenarios, a spoofing detection algorithm based on the absolute early and late outputs of the in-phase branch of the tracking loop combined with PCS (AELCP) is proposed. Based on the influence characteristics of the spoofing signal on the correlation peaks of the receiver tracking loop, the absolute values of the early and late outputs of the in-phase branch are weighted

收稿日期: 2024-10-08;修订日期: 2024-11-20

基金项目:国家自然科学基金面上项目(61903049);湖南省自然科学基金(2025JJ9043);湖南省厅科学研究重点项目(21A0381, 23A0464);湖南省研究生科研创新项目(QL20230271)

作者简介:覃业梅(1979-),女,博士,副教授,主要从事智能信息处理、时间序列分析预测方面的研究。

通信作者:胡勇(1997—),男,硕士研究生,主要从事全球卫星导航系统(GNSS)信息安全方面的研究。

and multiplied by the PCS to form the AELCP detection metric. Based on the skewness and kurtosis indexes, the probability distribution characteristics of the AELCP detection metric are examined to provide a theoretical basis for selecting the detection threshold and evaluating the detection probability. A moving average method is also applied to AELCP so that the AELCP-MA detection metric can be formed to reduce the noise effect. Using data from multiple scenarios such as DS3, DS4, DS5, and DS7 in the Texas spoofing test battery (TEXBAT) at the University of Texas, the performance such as detection probability of different algorithms are compared and analyzed. The results show that the AELCP-MA algorithm can be applied to multiple spoofing scenarios and has higher detection probability and robustness in various spoofing scenarios compared to the SQM algorithms such as PCS-MA, ELP-MA, and Delta-MA.

Key words: Global navigation satellite system(GNSS); Spoofing detection; Skewness; Kurtosis; Moving average; Detection probability; Robustness

0 引言

全球卫星导航系统(global navigation satellite system, GNSS)可为全球用户提供全天候的定位、导 航和授时服务^[1]。然而,由于 GNSS 信号到达地面能 量弱,且民用 GNSS 的信号结构公开,易受外界干扰。 欺骗干扰是 GNSS 面临的主要威胁之一^[2],其通过发 射与 GNSS 相似的欺骗信号,影响接收机对真实信号 的锁定,使接收机定位解算出错[3]。卫星欺骗干扰可 分为转发式欺骗和生成式欺骗^[4]。与转发式欺骗相 比,生成式欺骗的检测难度更大[5]。生成式欺骗分为 初级、中级和高级欺骗^[6]。初级欺骗通过发射大功率 的压制干扰,使接收机处于失锁状态,隐蔽性差,易被 检测;中级欺骗的欺骗信号功率与真实信号功率接 近,利用诱导式欺骗策略,在不中断接收机跟踪状态 的情况下,将 GNSS 接收机跟踪环诱导至欺骗信号, 夺取 GNSS 接收机的控制权,实现欺骗攻击;高级欺 骗则为多个中级欺骗的叠加,不再是欺骗信号固定的 单欺骗源欺骗,其具有系统成本昂贵、设计复杂及检测 难度大的特点。其中,中级欺骗复杂度适中、可行性高 且隐蔽性好,目前 GNSS 欺骗中主要为中级欺骗。

GNSS 欺骗检测技术主要有空间处理^[7]、测量 域处理^[8]和基带信号处理^[9]等。其中,基带信号处 理技术具有设计简单和检测性能好等优点。作为 基带信号处理技术之一,信号质量监测(signal quality monitoring, SQM)技术最初用于检测多径 干扰^[10],后用于欺骗检测。SQM 技术主要包括 Ratio 检测量和 Delta 检测量^[11],这 2 类检测量均由 同相支路的相关器输出构成,通过检测相关峰的形 变判断是否存在欺骗。早迟相位(early late phase, ELP)检测量则利用正交支路的输出特征变化进行 检测,当存在欺骗时,超前码和滞后码相位不相 等^[12]。而当欺骗信号与真实信号的载波相位差接 近π时,ELP算法失效^[13]。为综合利用多个 SQM 检测量,孙超等^[14]提出了复合 SQM 算法,通过对 Ratio和ELP线性加权构建检测量,检测性能较单 一检测量有了明显提高。王文益等^[15]提出了复合 SQM 方差算法,相较于复合 SQM,具有更高的检测 概率,但对于功率随时间变化的场景检测性能不理 想。王璐等^[16]提出了基于绝对功率监测与 SQM 融 合(power combined with SQM, PCS)的欺骗检测 算法,适用于大功率欺骗场景的检测,但对载波同 步的欺骗场景检测效果不理想。

综上分析,为改善 SQM 类欺骗检测算法的场景 适用性,借鉴复合 SQM 算法的思路,构建了一种基于 同相支路超前及滞后输出绝对值与 PCS 相结合(absolute early and late outputs combined with PCS, AE-LCP)的检测量,并通过概率分布分析确定检测门限。 为降低噪声影响,提出了 AELCP 滑动平均(AELCPmoving average, AELCP-MA)的欺骗检测方法。利 用美国德州大学的欺骗测试数据集(Texas spoofing test battery, TEXBAT)^[17-18]中的静态场景数据集 3 (data sets 3, DS3),DS4,DS7 及动态场景 DS5 进行算 法性能验证。

1 欺骗干扰检测算法

1.1 接收环路相关器输出

接收机跟踪环路相关输出为

 $r(t,\tau) = R^{a}(t,\tau) + R^{s}(t,\tau) + R^{n}(t,\tau)$ (1) 其中:上标 a,s,n 分别代表真实信号、欺骗信号和噪 $R(\bullet)$

声信号; *R*(*t*,τ)为信号与本地码的互相关结果。 真实信号与本地码的互相关结果为

$$R^{a}(t,\tau) = \begin{cases} 1 - |\tau|, & |\tau| < 1\\ 0, & \ddagger \psi \end{cases}$$
(2)

因欺骗信号与真实信号具有相同信号结构,且 功率相近, $R^{*}(t,\tau)$ 可表示为

$$R^{s}(t,\tau) = R^{a}(\tau - \hat{\tau}(t))$$
(3)

其中, $\hat{\tau}(t)$ 为欺骗信号与真实信号的码相位差,是随时间变化的变量。

跟踪环路使用超前、即时及滞后3对相关器。 导航数据码为1时,即时相关器的同相支路输出 *I*_P 和正交支路输出 *Q*_P 分别为

$$I_{\rm P} \approx \frac{\sqrt{2P^{\rm a}}}{2} R(\tau^{\rm c} - \tau^{\rm a}) \cos(\varphi^{\rm a} - \varphi^{\rm c}) +$$

$$\frac{\sqrt{2P^{\rm s}}}{2} R(\tau^{\rm c} - \tau^{\rm s}) \cos(\varphi^{\rm s} - \varphi^{\rm c})$$

$$Q_{\rm P} \approx \frac{\sqrt{2P^{\rm a}}}{2} R(\tau^{\rm c} - \tau^{\rm a}) \sin(\varphi^{\rm a} - \varphi^{\rm c}) +$$

$$\frac{\sqrt{2P^{\rm s}}}{2} R(\tau^{\rm c} - \tau^{\rm a}) \sin(\varphi^{\rm a} - \varphi^{\rm c}) +$$
(5)

$$\frac{1}{2} R(\tau^{e} - \tau^{s}) \sin(\varphi^{s} - \varphi^{e})$$
其中: P 代表信号功率; τ 代表信号的码相位;

为扩频码的互相关函数; τ^{e} 为本地扩频码的码相 位; φ^{e} 为复制信号的载波相位。 $I_{E}(Q_{E})$ 和 $I_{L}(Q_{L})$ 是 $I_{P}(Q_{P})$ 两侧相邻的相关器输出,即时相关器与 它们分别间隔 0.5码片,相干积分为 1 ms。

1.2 传统欺骗检测算法

1.2.1 经典检测量

Delta 检测量是 SQM 欺骗检测算法中的经典 检测量,通过观察相关峰形变进行欺骗检测,利用 相关器的 3 个同相支路输出构建检测量。

$$M_{\rm Delta} = \frac{I_{\rm E} - I_{\rm L}}{\alpha I_{\rm P}} \tag{6}$$

其中: $I_{\rm E}$, $I_{\rm P}$, $I_{\rm L}$ 分别为超前、即时及滞后 3 对相关 器的同相支路输出结果; α 为 C/A 码的相关峰斜 率, 通常 $\alpha = 2$ 。Delta 服从高斯分布^[16]。

ELP 算法同时考虑了同相和正交相关通道输 出值,通过比较相位信息进行欺骗检测,使用超前 码和滞后码的相关器输出构建检测量。

$$M_{\rm ELP} = \tan^{-1} \left(\frac{Q_{\rm E}}{I_{\rm E}} \right) - \tan^{-1} \left(\frac{Q_{\rm L}}{I_{\rm L}} \right)$$
(7)

其中, Q_E, Q_L 分别为超前和滞后相关器的正交输出 结果。ELP 近似服从高斯分布^[19]。 1.2.2 PCS 检测量

PCS 检测量为^[16]

$$M_{\rm PCS} = E + L - 2P \tag{8}$$

其中, *E*, *P*, *L* 分别是超前、即时和滞后相关器的自相关幅值, 满足

$$\begin{cases} E = \sqrt{I_{\rm E}^2 + Q_{\rm E}^2} \\ P = \sqrt{I_{\rm P}^2 + Q_{\rm P}^2} \\ L = \sqrt{I_{\rm L}^2 + Q_{\rm L}^2} \end{cases}$$
(9)

其中,当信噪比远大于1时,*E*,*P*,*L*近似服从高斯分布^[9],故线性组合后的 PCS 检测量近似服从高斯分布^[19]。

1.3 AELCP 及 AELCP-MA 检测量

1.3.1 AELCP 检测量

借鉴复合 SQM 算法的思路, PCS 可消除载波 相位的影响,并基于功率监测,对大功率场景的检 测概率高,但 PCS 输出不含载波相位,载波同步场 景的检测性能并不理想。结合同相支路输出,以兼 顾大功率欺骗场景的检测性能为前提,提升对载波 同步场景的检测效果。因此,取同相支路超前和滞 后输出绝对值的加权,并与 PCS 进行乘积运算,构 建 AELCP 检测量

 $M_{AELCP} = (|I_E| + |I_L|) \times (M_{PCS})$ (10) 其中, $I_E 和 I_L$ 分别为同相支路超前和滞后输出结果。 1.3.2 AELCP-MA 检测量

文献[20]通过对检测量进行滑动平均(moving average, MA)运算,实现了降低噪声影响以提升检测效果的目标。本文亦采用 AELCP 检测量 MA 处理的方式,由此构建 AELCP-MA 检测量

$$M_{\text{AELCP-MA}}(n) = \frac{1}{\omega} \sum_{i=nL+1}^{nL+\omega} M_{\text{AELCP}}(i) \qquad (11)$$

其中: ω 为滑动窗口的长度; $n = 1, 2, \dots, N, N$ 为滑动窗口的个数;L为滑动间隔。

AELCP-MA 检测量滑动窗口处理示意图如图 1 所示。



基于超前、即时及滞后相关器的自相关幅值构 建 PCS 检测量,取同相支路超前和滞后输出的绝对 值,将二者加权与 PCS 进行乘积运算,构建 AELCP 检测量,再经 MA 处理后构建 AELCP-MA 检测量。 构建流程如图 2 所示。



图 2 AELCP-MA 检测量流程图 Fig. 2 AELCP-MA detection metric flowchart

2 正态性检验及判决门限

2.1 AELCP-MA 检测量正态性检验

在欺骗检测算法中,检测门限的合理选取决定 了检测性能。为此,需分析 AELCP 检测量的分布 特性。为便于理论分析,取 $X = |I_E| + |I_L|, Y = M_{PCS}, Z = XY, 则$ AELCP 检测量的概率密度函 数为

$$f(z) = \int_{-\infty}^{+\infty} \frac{1}{|x|} f\left(x, \frac{z}{x}\right) \mathrm{d}x \qquad (12)$$

其中, $f\left(x, \frac{z}{x}\right)$ 为X,Y的联合概率密度函数。

当式(10)满足高斯分布时,给检测门限的选取 及检测性能评估带来了诸多便利。为论证式(10) 是否近似满足高斯分布,取正态性检验中常用的偏 度和峰度指标对其进行度量^[21]。

偏度是对随机变量概率分布的对称性进行度 量^[22]:偏度等于0时,随机变量概率分布的对称性 好。由于实际采样信号的点数有限,通常采用样本 统计偏度代替理论偏度^[23]。样本的统计偏度为

$$\hat{S} = \frac{\frac{1}{N_{s}} \sum_{i=1}^{N_{s}} (x(i) - \bar{x})^{3}}{\left(\frac{1}{N_{s}} \sum_{i=1}^{N_{s}} (x(i) - \bar{x})^{2}\right)^{3/2}}$$
(13)

其中,
$$\overline{x} = \frac{1}{N_s} \sum_{i=1}^{N_s} x(i)$$
为信号样本均值, N_s 为样

本点。

峰度反映了随机变量概率尾部的厚度,若峰度 等于3,则该随机变量概率密度函数的拖尾下降速 度与高斯分布近似^[23]。在实际中,通常采用样本统 计峰度代替理论峰度。样本的统计峰度为

$$\hat{K} = \frac{\frac{1}{N_{s}} \sum_{i=1}^{N_{s}} (x(i) - \overline{x})^{4}}{\left(\frac{1}{N_{s}} \sum_{i=1}^{N_{s}} (x(i) - \overline{x})^{2}\right)^{2}}$$
(14)

进一步引入偏度标准误差和峰度标准误差,分别为

$$E_{\rm SE,S} = \frac{6N_{\rm S}(N_{\rm S}-1)}{(N_{\rm S}-2)(N_{\rm S}+1)(N_{\rm S}+3)} \quad (15)$$

$$E_{\rm SE.K} = \frac{4(N_{\rm S}^2 - 1)E_{\rm SE.S}}{(N_{\rm S} - 3)(N_{\rm S} - 5)}$$
(16)

其中,Ns为样本点。

偏度和峰度的 Z 评分分别为^[24]

$$Z_{\rm ZS,\hat{S}} = \frac{\hat{S}}{E_{\rm SE,\hat{S}}} \tag{17}$$

$$Z_{\rm ZS,\hat{K}} = \frac{\hat{K}}{E_{\rm SE,\hat{K}}} \tag{18}$$

基于偏度和峰度指标进行高斯分布检验,在显 著性水平 $\alpha = 0.05$ 的条件下,其 Z 评分的绝对值为 1.96,认为样本服从高斯分布,准确率为95%。

为评估和验证实际导航信号的 AELCP 检测量 是否符合高斯分布,不失一般性,取 DS7 中的 7 颗 星的前 100 s(无欺骗)数据,分别计算 AELCP 的度量指标,结果如表 1 所示。

| Tab. 1 Normanity indicators of AELCP detection metric | | | | | | | | | | |
|---|----------|----------|----------|----------|----------|---------|----------|--|--|--|
| 卫星编号 | PRN3 | PRN6 | PRN7 | PRN13 | PRN16 | PRN19 | PRN23 | | | |
| Ŝ | -0.192 1 | -0.192 9 | -0.261 5 | -0.162 4 | 0.239 2 | 0.231 5 | -0.297 7 | | | |
| Ŕ | 3.063 5 | 3.194 3 | 3.0310 | 2.971 9 | 3.123 5 | 3.094 5 | 3.204 9 | | | |
| $E_{\rm SE, \hat{S}}$ | | | | 0.000 06 | | | | | | |
| $E_{\rm SE,\hat{K}}$ | | | | 0.000 24 | | | | | | |
| Z _{ZS,Ŝ} | -3 202.1 | -3 215.5 | -4 358.8 | -2 707.1 | -3 986.6 | -3858.3 | -4 962.6 | | | |
| $Z_{\rm ZS,K}$ | 12 764 | 13 309 | 12 628 | 12 382 | 13 014 | 12 893 | 13 353 | | | |

表 1 AELCP 检测量的正态性指标 Tab 1 Normality indicators of AELCP detection metric

由表1可知,偏度Ŝ接近于0且峰度 \hat{K} 接近3, 表明AELCP 检测量基本符合高斯分布。显著性水 平 α 为0.02和0.01时对应Z评分的绝对值分别为 2.330和2.575, α =0.01表示99%的正确率。由 数理统计原理可知,显著性水平越小,接受域越宽, Z评分越高。表1中, $Z_{ZS,S}$ 和 $Z_{ZS,R}$ 远大于2.575, 代表显著性水平 $\alpha \approx 0.01$,正确率接近100%。故 AELCP 检测量近似服从高斯分布,其概率密度函 数可表示为

$$f(M_{\text{AELCP}}) = \frac{1}{\sqrt{2\pi\sigma_{\text{AELCP}}^2}} e^{-\frac{(M_{\text{AELCP}} - \mu_{\text{AELCP}})^2}{2\sigma_{\text{AELCP}}^2}} \quad (19)$$

其中, μ_{AELCP} 和 σ^2_{AELCP} 分别为 AELCP 的均值和 方差。

PRN23中,AELCP检测量输出如图3所示。



由图 3 可见, AELCP 检测量输出的均值为 -4.4831×10¹³, 方差为 5.854 0×10¹²。AELCP 输出样本的分布近似服从高斯分布, 与理论分析一 致。因此,MA 处理后的 AELCP-MA 检测量也近 似服从高斯分布。

2.2 二元判决及检测门限

AELCP-MA 检测量近似满足高斯分布,根据 二元假设检验理论,可通过双门限实施欺骗检测。 记 H。代表无欺骗干扰场景,H1代表存在欺骗干 扰场景,则有

$$\begin{cases} H_{0}: \gamma_{\text{Th},1} \leqslant M_{\text{AELCP-MA}}(n) \leqslant \gamma_{\text{Th},u}, & 无欺骗 \\ H_{1}: \gamma_{\text{Th},1} > M_{\text{AELCP-MA}}(n), M_{\text{AELCP-MA}}(n) > \gamma_{\text{Th},u}, & 有欺骗 \end{cases}$$
(20)

其中: γ_{Th,u} 为检测上限;γ_{Th,l} 为检测下限; *M*_{AELCP-MA}(*n*)表示 AELCP-MA 检测量输出值。

基于上述假设,当检测量位于检测双门限内,则有理由判为无欺骗;反之,则判为有欺骗。在 H。 假设下,若检测量判定结果为有欺骗,则为虚警事件;在 H₁ 假设下,若检测量判定结果为有欺骗,则 为检测事件。虚警事件和检测事件分别对应虚警 概率 P_{1a} 和检测概率 P_d。

理论上2种概率的计算表达式分别为[14]

$$P_{fa} = \int_{-\infty}^{\gamma_{Th,1}} f(z \mid H_0) dz + \int_{\gamma_{Th,u}}^{\infty} f(z \mid H_0) dz \quad (21)$$

$$P_{d} = \int_{-\infty}^{\gamma_{Th,1}} f(z \mid H_1) dz + \int_{\gamma_{Th,u}}^{\infty} f(z \mid H_1) dz \quad (22)$$
其中, $f(\cdot)$ 为概率密度函数。

由于欺骗信号的参数时变且未知,通常采用统 计方法计算检测概率

$$P_{\rm d} = \frac{N(M_{\rm AELCP-MA}(n) < \gamma_{\rm Th,1}) + N(M_{\rm AELCP-MA}(n) > \gamma_{\rm Th,u})}{p}$$

其中:N(•)代表检测量小于检测下限和大于检测 上限的样本点数;p为滑动窗口中的样本总数。

对于高斯分布的检测量,检测上下限 γ_{Th,u} 和 γ_{Th,1} 关于均值对称^[14]

$$\gamma_{\mathrm{Th},\mathrm{u}} = \mu_i + \sqrt{2\sigma_i^2} \operatorname{erfc}^{-1}(P_{\mathrm{fa}}) \qquad (24)$$

$$\gamma_{\text{Th},1} = \mu_i - \sqrt{2\sigma_i^2} \operatorname{erfc}^{-1}(P_{\text{fa}})$$
(25)

其中: μ_i 为检测量均值; σ_i^2 为检测量的方差;erfc⁻¹ 为逆互补误差函数。

3 仿真实验及分析

3.1 数据集介绍及检测量输出

美国德州大学的 TEXBAT 是验证欺骗算法性 能的常用数据集。TEXBAT 含 8 种不同的攻击场 景,分别对应 DS1~DS8。其中,DS1 是真实信号到 欺骗信号的瞬时跳变,对其欺骗检测难度大;DS2 与 DS5 为大功率下的静态/动态场景,检测难度较 小;DS3 为静态小功率的时间欺骗场景;DS4 为静 态功率匹配的位置欺骗场景,且欺骗信号功率接近 真实信号,较难检测;DS6 场景中噪声和多径干扰 影响严重,欺骗攻击与多径干扰区分难度较大;DS7 为载波同步场景,检测难度较大;DS8 与 DS7 类似, 但 DS8 是不断重复袭击的欺骗式干扰,目前技术难 以有效检测。结合本文研究内容,选取 DS3,DS4, DS5 和 DS7 这 4 种欺骗场景进行欺骗检测实验,实 验数据集的具体参数如表 2 所示。

表 2 实验数据集参数 Tab. 2 Experimental dataset parameters

| 数据集 | 场景描述 | 种类 | 功率优势/dB | 锁频状态 | |
|-----|--------|----|---------|------|--|
| DS3 | 静态小功率 | 时间 | 1.3 | 锁定 | |
| DS4 | 静态功率匹配 | 位置 | 0.4 | 锁定 | |
| DS5 | 动态大功率 | 时间 | 9.9 | 失锁 | |
| DS7 | 静态功率匹配 | 时间 | 1.3 | 锁定 | |

实验数据集 DS3,DS4,DS5 的 0~100 s 为无欺 骗干扰,100~110 s 为欺骗注入阶段,110~180 s 为 欺骗对齐阶段,180~280 s 为欺骗牵引阶段,280 s 后为欺骗分离阶段;DS7 则在 110~130 s 注入欺骗 信号,130~150 s 欺骗信号与真实信号对齐,150~ 400 s 接收机被牵引至欺骗信号,400 s 后接收机锁定 欺骗信号,欺骗信号与真实信号开始分离。以 DS7 的 PRN23 为例,AELCP 检测量如图 4 所示。

图 4 中,在无欺骗阶段和第Ⅰ,Ⅱ阶段,AELCP 的 波形均无明显变化;在第Ⅲ阶段,AELCP 产生一定变





化,波动范围较大;在第Ⅳ阶段,AELCP逐渐下降,变 化程度降低。为更加直观地分析 AELCP 的变化趋势,以 100 ms窗口对 AELCP 进行 MA 处理,构建得 到的 AELCP-MA 检测量如图 5 所示。



由图 5 可见,在 110 s 左右 AELCP-MA 的波形 存在明显变化;在 110~150 s,波形较平稳,但其量 值大于无欺骗时的量值;在 150~400 s,AELCP-MA 表现为先升高后降低的趋势,且其量值大于无 欺骗时的量值;在 400 s 后,AELCP-MA 持续下降。 综合可见,存在欺骗时,AELCP-MA 的量值大于无 欺骗时的量值。

对比图 4 和图 5 可见,与 AELCP 相比,AELCP-MA 检测量的变化趋势特征更明显。在欺骗注入阶段,可观察到 AELCP-MA 的变化;在欺骗对齐和牵引阶段,AELCP-MA 的量值明显区别于无欺骗时量值。

3.2 检测概率及判决

设定虚警概率为 10%,根据式(22)和式(23), 计算 AELCP-MA 的检测上限和下限,分别为 2.190×10¹²和-4.467×10¹³。取滑动窗口宽度为 100 ms,每1 s计算得到一个检测概率值。对比 AELCP-MA,AELCP,PCS,Delta和ELP这5种检 测量的检测概率,结果如图6所示。



Fig. 6 Comparison of detection probability

图 6 中,在 130~150 s,AELCP-MA 检测量的 检测概率存在较大变化,最大值达 70%左右,其他 4 种检测量的检测概率均低于 50%。在 160 s 以后, AELCP-MA 检测量的检测概率增高至 90%, 但在 400 s 后明显下降; PCS 检测量的检测概率增 高至 90%左右,但在 250 s 左右开始快速降低;而 Delta 和 ELP 检测量的检测概率一直低于 50%。 结合以上结果分析可见,与其他检测量相比, AELCP-MA 检测量表现出较高的检测概率,且检 测即时性较好。

基于二元判决,当检测概率大于或等于 50% 时,判定为存在欺骗,以输出结果为 1 表示;检测概 率小于 50%则认定为无欺骗,以输出结果为 0 表 示。AELCP-MA,AELCP,PCS,Delta 和 ELP 的判 决结果如图 7 所示。



在图 7 中, AELCP-MA 检测量判决为欺骗干扰的数目最多, ELP 和 Delta 检测量判决为欺骗的数目为 0。在第 Ⅱ 阶段, 仅 AELCP-MA 存在判决为欺骗干扰的结果; 在第 Ⅲ 阶段, AELCP-MA 和 AELCP 判决为欺骗的数目相当, PCS 判决数目较少。与其他检测量相比, AELCP-MA 检测量判决为欺骗的次数更多, 且检测范围更宽。

为进一步分析 MA 检测量的检测性能,对 PCS, Delta 和 ELP 这 3 种检测量进行滑动窗口为 100 ms 的 MA 处理,绘制 PCS-MA, Delta-MA, ELP-MA 和 AELCP-MA 的检测概率曲线,如图 8 所示。



Fig. 8 Detection probability curves for detected metrics after MA processing

如图 8 可见,在 130 s后,AELCP-MA 检测量 的检测概率保持在 100%左右;在 170~300 s,PCS-MA 的检测概率保持在 100%左右,400 s后低于 50%;ELP-MA 和 Delta-MA 的检测概率低于 50%。由结果分析可知,在 150 s后 AELCP-MA 检 测量的检测概率始终保持在 100%,且 130 s后即可 检测到欺骗;与 PCS-MA,ELP-MA 和 Delta-MA 检 测量相比,AELCP-MA 检测量表现出较高的检测 概率。

为分析 AELCP-MA 检测量受 ω 的影响情况, 选取 ω 为 25 ms,50 ms,100 ms 绘制检测概率曲 线,如图 9 所示。

图 9 中,当 ω 取 25 ms 和 50 ms 时,在无欺骗 干扰阶段初期,AELCP-MA 检测概率为 100%,误 判存在欺骗干扰。随着 ω 的增大,AELCP-MA 的 检测概率曲线波动趋势变小,且无欺骗阶段初期的 检测概率降低,欺骗检测准确性提高。综合分析可 知,选取合适的窗口长度可提高无欺骗阶段的欺骗 检测准确性。





3.3 接收机工作特性曲线

采用常见的接收机工作特征(receiver operating characteristic, ROC)曲线分析不同虚警率下的检测概率性能。在 ROC 曲线中,横轴为虚警概率,纵轴 为欺骗第 II 阶段初至第 III 阶段末的平均检测概率。ROC 曲线离左上角越近,则算法的检测准确性越高^[25]。以 DS7 的 PRN7, PRN19 和 PRN23 为例, 计算各检测算法的 ROC 曲线,结果如图 10 所示。





图 10 DS7 场景下 ROC 曲线对比 Fig. 10 Comparison of ROC curve in DS7 scenario

在图 10 中,对于任意同一颗卫星,在给定的虚 警概率下,AELCP-MA 的 ROC 曲线始终高于其他 检测量。以 PRN23、虚警率为 10%为例,AELCP-MA,PCS-MA,ELP-MA 和 Delta-MA 的检测概率 分别为 99.89%,84.32%,24.43%和 9.37%。在选 取的 3 颗卫星中,AELCP-MA 检测量的检测概率 均达到 80%以上,PCS-MA 检测量的检测概率均低 于 70%,Delta-MA 和 ELP-MA 检测量的检测概率 均低于 30%。综合分析可知,与 PCS-MA,Delta-MA 和 ELP-MA 相比,AELCP-MA 具有更高的检 测概率和欺骗检测灵敏度。

3.4 多种场景下 ROC 曲线对比

为进一步分析算法的普适性,选取多种欺骗场 景进行欺骗检测实验。不失一般性,选择 DS3, DS4,DS5 和 DS7 这 4 种欺骗场景中的某一颗星为 例,计算 AELCP-MA,PCS-MA,Delta-MA 和 ELP-MA 4 种检测量的 ROC 曲线,结果如图 11 所示。

由图 11(a)(b)(d)可见,AELCP-MA 检测量的 检测概率达80%以上,PCS-MA的检测概率为70%



以上;在图 11(c)中,AELCP-MA 和 PCS-MA 的检 测概率相当,均达到 100%。在 4 种欺骗场景下, Delta-MA 和 ELP-MA 的检测概率均较低。结合以 上结果分析可知,与 PCS-MA 相比,在兼顾大功率 欺骗场景检测性能的前提下,AELCP-MA 的检测 概率至少提升 10%,并具有更高的普适性。

同时,在4种欺骗环境下,选取3颗不同卫星进 行欺骗检测分析,并对不同检测量进行多星 ROC 曲 线对比。因 DS5 动态场景与其他3个静态场景捕获 卫星不同,故 DS5 选取 PRN18,PRN21 和 PRN22,其 他3种静态欺骗场景选取 PRN7,PRN19 和 PRN23, 不同场景下多星 ROC 曲线如图 12 所示。





图 12 不同场景下多星 ROC 曲线对比 Fig. 12 Comparison of multi-satellite ROC curves in different scenarios

由图 12(a)(b)(d)可见,相较于其他检测量, AELCP-MA 检测量的检测概率更高。在图 12(c) 中,AELCP-MA 与 PCS-MA 的检测概率相当,均在 90%以上。由实验结果分析可知,在多种欺骗场景 下进行欺骗检测实验,AELCP-MA 检测量展现出 更高的检测概率和稳健性。

4 结论

针对传统 SQM 类欺骗检测算法在复杂欺骗场 景下普适性不理想的问题,构建了一种基于同相支路 输出与 PCS 相结合的 AELCP 检测量。为抑制噪声, 进一步提出了 AELCP-MA 欺骗检测算法。采用 TEXBAT 的 DS3, DS4, DS5 和 DS7 作为数据集进行 欺骗检测实验,分析 AELCP-MA 算法的检测性能。 实验结果表明:

1)当虚警概率为 10%时,AELCP-MA 的检测 概率保持在 80%以上,且与另外几种传统 SQM 算 法相比,AELCP-MA 算法拥有更高的检测概率、更 好的检测即时性及更宽的检测范围。

2)任意虚警概率下,相较于另外几种 SQM 算法,AELCP-MA 算法具有更高的检测准确度、更好的稳健性及更广的适用场景。

3) AELCP-MA 算法可有效检测中级欺骗,将 来可与机器学习和神经网络融合使用,进一步提升 检测准确率和稳健性,以应对日益复杂的导航时空 安全威胁。

参考文献

[1] WUZ, ZHANGY, YANGY, et al. Spoofing and anti-

spoofing technologies of global navigation satellite system: a survey [J]. IEEE Access, 2020, 8: 165444-165496.

- [2] XIAO L, XIE C, MIN M, et al. User-centric view of unmanned aerial vehicle transmission against smart attacks[J]. IEEE Transactions on Vehicular Technology, 2018, 67(4): 3420-3430.
- [3] GU N, FEI X, YOU Z. GNSS spoofing detection based on coupled visual/inertial/GNSS navigation system[J]. Sensors, 2021, 21(20): 6769.
- [4] 卢丹,殷亚强.基于 CS-C-SVM 的多参数 GNSS 欺骗干扰检测[J].信号处理,2022,38(6):1325-1332.

LU Dan, YIN Yaqiang. Multi-parameter GNSS spoofing interference detection based on CS-C-SVM[J]. Journal of Signal Processing, 2022, 38(6): 1325-1332(in Chinese).

- [5] 马克,孙迅,聂裕平.GPS生成式欺骗干扰关键技术
 [J].航天电子对抗,2014,30(6):24-26+34.
 MA Ke, SUN Xun, NIE Yuping. Research on key technologies of GPS generated spoofing[J]. Aerospace Electronic Warfare, 2014, 30(6):24-26+34(in Chinese).
- [6] SHEPARD P D, HUMPHREYS E T, 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.
- [7] ROTHMAIER F, CHEN Y, LO S, et al. GNSS spoofing detection through spatial processing [J]. Navigation, 2021, 68(2): 243-258.
- [8] LI J, ZHU X, OUYANG M, et al. GNSS spoofing detection technology based on Doppler frequency shift difference correlation [J]. Measurement Science and Technology, 2022, 33(9): 095109.
- [9] MANFREDINI E G, DOVIS F, MOTELLA B. Validation of a signal quality monitoring technique over a set of spoofed scenarios[C]// Proceedings of 2014 7th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC). Noordwijk: IEEE, 2014: 1-7.
- SCHMIDT E, AKOPIAN D, PACK D J. Development of a real-time software-defined GPS receiver in a LabVIEW-based instrumentation environment [J].
 IEEE Transactions on Instrumentation and Measurement, 2018, 67(9): 2082-2096.
- [11] PHELTS R E. Multicorrelator techniques for robust mitigation of threats to GPS signal quality[D]. Cali-

fornia: Stanford University, 2001.

- [12] SUN C, CHEONG W J, DEMPSTER G A, et al. Moving variance-based signal quality monitoring method for spoofing detection[J]. GPS Solutions, 2018, 22(3): 1-13.
- [13] GENG Z, NIE J, XIAO Z, et al. A GNSS spoofing detection technique based on signal spatial correlation[C]// Proceedings of 2017 China Satellite Navigation Conference (CSNC), Volume I. Singapore: Springer, 2017: 959-969.
- [14] SUN C, CHEONG J W, DEMPSTER A G, et al. GNSS spoofing detection by means of signal quality monitoring (SQM) metric combinations [J]. IEEE Access, 2018, 6: 66428-66441.
- [15] 王文益,龚婧. 基于复合 SQM 方差的 GNSS 欺骗式 干扰检测算法[J]. 中国民航大学学报, 2020, 38(4): 7-12.
 WANG Wenyi, GONG Jing. GNSS spoofing detection algorithm based on composite SQM variance[J]. Journal of Civil Aviation University of China, 2020, 38(4): 7-12 (in Chinese).
- [16] 王璐,张林杰,吴仁彪.功率监测与 SQM 融合的 GNSS 欺骗干扰检测[J]. 信号处理, 2023, 39(3): 505-515.

WANG Lu, ZHANG Linjie, WU Renbiao. GNSS spoofing detection based on power monitoring combined with SQM[J]. Journal of Signal Processing, 2023, 39(3): 505-515(in Chinese).

- [17] HUMPHREYS T E, BHATTI J A, SHEPARD D, et al. The Texas spoofing test battery: toward a standard for evaluating GPS signal authentication techniques [C]// Proceedings of 25th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2012). Nashville: ION, 2012: 3569-3583.
- [18] HUMPHREYS T. TEXBAT data sets 7 and 8[EB/ OL]. (2016-03-16)[2024-10-08]. The University of

Texas at Austin, https://rnl-data.ae.utexas.edu/ datastore/texbat/texbat_ds7_and_ds8.pdf.

- [19] QIAN C, FENG F, WEN L, et al. Conceptualized and contextualized Gaussian embedding[C]// Proceedings of 35th AAAI Conference on Artificial Intelligence (AAAI-21). AAAI, 2021, 35(15): 13683-13691.
- [20] 朱瑞晨,王文益.基于 SCS 的多星联合诱导式欺骗 检测算法[J].现代电子技术,2023,46(11):1-8.
 ZHU Ruichen, WANG Wenyi. SCS-based multi-star joint induced spoofing detection algorithm [J].
 Modern Electronics Technique, 2023,46(11):1-8(in Chinese).
- [21] ASGHAR G, SALEH Z. Normality tests for statistical analysis: a guide for non-statisticians[J]. International Journal of Endocrinology and Metabolism, 2012, 10(2): 486-489.
- [22] 盛骤,谢式千,潘承毅. 概率论与数理统计[M]. 第四版.北京:高等教育出版社,2008:206-208.
 SHENG Zhou, XIE Shiqian, PAN Chengyi. Probability theory and mathematical statistics[M]. 4th edition. Beijing: Higher Education Press, 2008: 206-208(in Chinese).
- [23] 谭哲雯, 雷可君, 杨喜, 等. 一种基于偏度和峰度联合检测的频谱感知算法[J]. 吉首大学学报(自然科学版), 2023, 44(6): 14-19.
 TAN Zhewen, LEI Kejun, YANG Xi, et al. Spectrum sensing algorithm based on joint detection of skewness and kurtosis[J]. Journal of Jishou University (Natural Sciences Edition), 2023, 44(6): 14-19(in Chinese).
- [24] MISHRA P, PANDEY C M, SINGH U, et al. Descriptive statistics and normality tests for statistical data[J]. Annals of Cardiac Anaesthesia, 2019, 22 (1): 67-72.
- [25] NAHM S F. Receiver operating characteristic curve: overview and practical use for clinicians[J]. Korean Journal of Anesthesiology, 2022, 75(1): 25-36.

(编辑:黄利华)