doi:10.19306/j.cnki.2095-8110.2024.02.008

绝对同相支路输出的 GNSS 欺骗检测

赵 慎[1]，胡 勇[1]，李世玲[1]，许 伟[2]

（1. 湖南工商大学智能工程与智能制造学院，长沙 410205；
2. 湖南矩阵电子科技有限公司，长沙 413000）

摘 要：针对功率随时间变化，载波同步欺骗场景下，传统检测算法的欺骗检测性能不理想的问题，提出了一种基于绝对同相支路输出求和（SAIBO）的欺骗检测算法，为改善欺骗检测性能，进一步提出了 SAIBO 滑动平均（SAIBO-MA）算法。SAIBO-MA 算法的构建过程使用接收机跟踪环的同相支路的输出结果取绝对值后求和形成 SAIBO 检测量，再做滑动平均处理后得到 SAIBO-MA 检测量。实验使用德克萨斯大学奥斯汀分校的德州欺骗测试电池（TEXBAT）的场景 7（DS7）为数据集，比较并分析所提算法与传统算法的检测概率、欺骗判决数目和稳健性等欺骗检测性能。实验结果表明，SAIBO-MA 具有更高的检测概率和检测精度、更好的即时性和稳健性以及更宽的检测范围。提出的 SAIBO-MA 算法克服了传统算法的缺点，具有更优的欺骗检测性能。

关键词：载波同步；欺骗检测算法；检测概率；欺骗检测；检测性能

中图分类号：TN967.1；V324.2^{+}4 **文献标志码**：A **文章编号**：2095-8110(2024)02-0083-10

GNSS spoofing detection based on absolute in-phase branch output

ZHAO Shen[1], HU Yong[1], LI Shiling[1], XU Wei[2]

(1. School of Intelligent Engineering and Intelligent Manufacturing, Hunan University of Technology and Business, Changsha 410205, China;
2. Hunan Matrix Electronic Technology Co., Ltd., Changsha 413000, China)

Abstract: A spoofing detection algorithm based on sum of absolute in-phase branch outputs (SAIBO) is proposed to address the issue of suboptimal spoofing detection performance of traditional detection algorithms in carrier synchronous spoofing scenarios where power varies over time. To improve spoofing detection performance, the SAIBO-moving average (SAIBO-MA) algorithm is further proposed. The construction process of the SAIBO-MA algorithm uses the output results of the in-phase branch of the receiver's tracking loop to take absolute values and sum them to form the SAIBO detection metric. After performing moving average processing, the SAIBO-MA detection metric is obtained. The experiment uses Data Scenario 7 (DS7) of Texas Spoofing Test Battery (TEXBAT) from the University of Texas at Austin as the dataset, and compares and analyzes the detection probability, number of spoofing decisions, and robustness of the three algorithms for spoofing detection. The experimental results indicate that SAIBO-MA has higher detection proba-

收稿日期：2023-12-11；**修订日期**：2024-01-22

基金项目：国家自然科学基金（61976088）；湖南省教育厅科学研究项目（23A0464）；湖南省研究生科研创新项目（QL20230271）

作者简介：赵慎（1983—），男，博士，讲师，主要从事导航时空信息安全、阵列信号处理等方面的研究。

通信作者：许伟（1988—），男，硕士，工程师，主要从事卫星导航仪器设计方面的研究。

bility and accuracy, better immediacy and robustness, and a wider detection range. The proposed SAIBO-MA algorithm overcomes the shortcomings of traditional algorithms and has better spoofing detection performance.

Key words: Carrier synchronous; Spoofing detection algorithm; Detection probability; Spoofing detection; Detection performance

0 引言

全球卫星导航系统(global navigation satellite system, GNSS)利用卫星广播的伪距、星历和信号发射时间等信息,为地表或近地空间用户提供全天候的定位、测速和授时服务[1],广泛应用在交通、通信、电力及金融等领域。由于能量微弱、信号结构公开和系统对时间敏感等原因,GNSS 易受各种干扰的影响[2]。其中,欺骗干扰的隐蔽性极强且危害性最大[3]。欺骗攻击者通过播发虚假导航信号,将接收机跟踪环牵引至欺骗信号,导致接收机输出错误的定位信息,甚至输出攻击者意图控制的定位结果,是 GNSS 面临的主要安全威胁之一。研究有效的导航欺骗检测技术,保障 GNSS 的时空信息安全,是当前卫星导航研究的热点问题。

按照产生方式的不同,欺骗方式分为转发式欺骗和生成式欺骗[4]。转发式欺骗将收到的真实卫星信号,经过功率放大和一定延迟后发给用户设备。生成式欺骗根据真实信号结构生成欺骗信号,与转发式欺骗相比,其隐蔽性更强,更难被检测到[5]。根据复杂程度,生成式欺骗又分为初级、中级和高级欺骗,其中,中级欺骗的可行性最高,应用范围最广。中级欺骗过程分为欺骗注入、欺骗对齐、欺骗牵引和欺骗分离 4 个阶段[6]。

随着对欺骗检测研究的深入,国内外学者提出了诸多有效的欺骗检测技术,主要包括空间处理[7-11]、测量域[12-14]和基带信号处理[15-17]等。空间处理技术设计复杂,系统成本高;测量域技术在检测量变化不明显时无效,应用受限;基带信号处理技术具有设计简单、无需外加设备辅助和检测性能好等优点,逐渐成为近年来的重点研究领域。

作为基带信号处理技术之一,信号质量监测(signal quality monitoring, SQM)具有设计简单、成本低和效率高等优点。SQM 技术[18]起初用于检测多径干扰,后逐渐应用到欺骗检测领域。经典的 SQM 欺骗检测算法主要包括 Delta 和 Ratio[19],两种算法均利用同相支路超前、即时和滞后相关器的输出结果构建检测量,以衡量相关峰的畸变程度,区别在于 Delta 检测相关峰的对称性,Ratio 检测相关峰的尖锐程度。Delta 和 Ratio 被证实具有较好的欺骗检测性能,但由于缺少正交支路参与,当接收复合信号在同相和正交通道波动时,检测性能变差。ELP(early-late phase)算法[20]使用超前与滞后的相位差作为检测量,在同相支路基础上补充正交支路,可有效检测到欺骗干扰,但当欺骗信号与真实信号的相位差接近 π 的整数倍时,ELP 的检测性能急剧恶化。针对单检测算法的缺陷,孙超等[21]提出了复合 SQM 算法,利用 Ratio,Delta 与 ELP 之间的互补性,通过线性加权方式构建检测量,弥补了 Ratio,Delta 和 ELP 单独使用的缺陷,有效改善了欺骗检测性能。Dehghanian 等[22]提出了基于功率监测的欺骗检测方法,当欺骗信号功率比真实信号功率高时,该方法具有较好的检测性能,而当欺骗信号与真实信号功率相当时,该方法不再适用。为弥补单一 SQM 算法检测性能不理想的问题,王文益等[23]提出了 SQM 方差算法,在功率恒定时,有效提高了检测性能,但在功率随时间变化时,检测性能并不理想。针对单一欺骗检测方法的不足,王璐等[24]提出了功率监测与信号质量监测融合(power combined with SQM, PCS)的欺骗检测方法,其兼顾功率监测与信号质量监测的优点,能有效检测欺骗信号,但在同频同相欺骗场景下,PCS 检测性能并不理想。

针对 Ratio,PCS 和 ELP 在功率随时间变化、载波同步(同频同相)的欺骗场景下,检测性能不理想的问题,提出了一种基于绝对同相支路输出求和(sum of absolute in-phase branch outputs, SAIBO)的欺骗检测方法。为更清晰地反映在欺骗过程中 SAIBO 的输出波形随时间的变化,减小噪声带来的影响,进一步提出了 SAIBO 滑动平均(SAIBO-moving average, SAIBO-MA)欺骗检测方法。实验中,使用 TEXBAT 中的 DS7 作为数据集,对 Ratio,PCS,ELP 和 SAIBO 及其对应 MA 算法进行欺骗检测实验,并分析其检测性能。

1　信号模型及相关器输出

1.1　接收信号

中级欺骗攻击的过程分为欺骗注入(Ⅰ)、欺骗对齐(Ⅱ)、欺骗牵引(Ⅲ)和欺骗分离(Ⅳ)4 个阶段[24]。第Ⅰ阶段:欺骗信号与真实信号存在一定距离并不断靠近真实信号,接收机跟踪真实信号;第Ⅱ阶段:欺骗信号与真实信号对齐并逐渐提升欺骗信号功率,接收机仍然跟踪真实信号;第Ⅲ阶段:欺骗信号利用功率优势夺取接收机的控制权,接收机被牵引至欺骗信号;第Ⅳ阶段:欺骗信号通过调整自身码速率,缓慢偏离真实信号[24],中级欺骗的完成对接收机造成不可逆的影响。中级欺骗过程如图 1 所示。

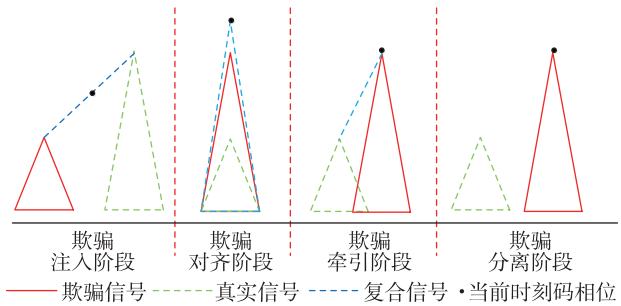


图 1　中级欺骗示意图

Fig. 1　Schematic of intermediate spoofing

存在欺骗干扰时,接收信号由真实信号、欺骗信号和噪声组成

$$x(t)=x^{\mathrm{a}}(t)+x^{\mathrm{s}}(t)+n(t) \tag{1}$$

其中,$x^{\mathrm{a}}(t)$ 为真实信号;$x^{\mathrm{s}}(t)$ 为欺骗信号;$n(t)$ 为零均值的高斯白噪声。

真实信号 $x^{\mathrm{a}}(t)$ 表示为

$$x^{\mathrm{a}}(t)=\sqrt{P^{\mathrm{a}}}C^{\mathrm{a}}(t-\tau^{\mathrm{a}})D^{\mathrm{a}}(t-\tau^{\mathrm{a}})\cos(2\pi(f_0+f_{\mathrm{d}}^{\mathrm{a}})t+\varphi^{\mathrm{a}}) \tag{2}$$

其中,P^{a} 为真实信号功率;C^{a} 为真实信号伪随机扩频码;D^{a} 为 ±1 的真实信号导航数据;τ^{a} 为真实信号码延迟;f_0 为中心频率;$f_{\mathrm{d}}^{\mathrm{a}}$ 为真实信号的多普勒频移;φ^{a} 为真实信号的载波相位。

由于欺骗信号与真实信号具有相同的信号结构,因而欺骗信号为

$$x^{\mathrm{s}}(t)=\sqrt{P^{\mathrm{s}}}C^{\mathrm{s}}(t-\tau^{\mathrm{s}})D^{\mathrm{s}}(t-\tau^{\mathrm{s}})\cos(2\pi(f_0+f_{\mathrm{d}}^{\mathrm{s}})t+\varphi^{\mathrm{s}}) \tag{3}$$

其中,P^{s} 为欺骗信号功率;C^{s} 为欺骗信号伪随机扩频码;D^{s} 为±1的欺骗信号导航数据;τ^{s} 为欺骗信号码延迟;$f_{\mathrm{d}}^{\mathrm{s}}$ 为欺骗信号的多普勒频移;φ^{s} 为欺骗信号的载波相位。

1.2　接收机相关器输出

作为接收机的核心组成部分,相关器的作用是剥离伪码。以全球定位系统(global positioning system, GPS)L1 载波的 C/A 码为例,相关输出为

$$R(t,\tau)=R^{\mathrm{a}}(t,\tau)+R^{\mathrm{s}}(t,\tau)+R^{\mathrm{n}}(t,\tau) \tag{4}$$

其中,$R^{\mathrm{a}}(t,\tau)$ 为真实信号与本地信号的互相关结果;$R^{\mathrm{s}}(t,\tau)$ 为欺骗信号与本地信号的互相关结果;$R^{\mathrm{n}}(t,\tau)$ 为噪声信号与本地信号的互相关结果。由 PRN 码的特性可知

$$R^{\mathrm{a}}(t,\tau)=\begin{cases}1-|\tau|, & |\tau|<1\\ 0, & \text{其他}\end{cases} \tag{5}$$

欺骗信号与真实信号的信号结构相似、功率相当,则 $R^{\mathrm{s}}(t,\tau)$ 可表示为

$$R^{\mathrm{s}}(t,\tau)=R^{\mathrm{a}}(t-\tau_1) \tag{6}$$

其中,τ_1 为欺骗信号与真实信号之间的码相位差。

跟踪环使用超前、即时和滞后 3 对相关器,相邻相关器间隔为 0.5 个码片,相干积分时间 1 ms。每对相关器由同相支路和正交支路组成,若导航数据码为 1,即时码在同相支路 I_{P} 和正交之路 Q_{P} 的输出分别为

$$I_{\mathrm{P}}\approx\frac{\sqrt{2P^{\mathrm{a}}}}{2}R(\tau^{\mathrm{c}}-\tau^{\mathrm{a}})\cos(\varphi^{\mathrm{a}}-\varphi^{\mathrm{c}})+\frac{\sqrt{2P^{\mathrm{s}}}}{2}R(\tau^{\mathrm{c}}-\tau^{\mathrm{s}})\cos(\varphi^{\mathrm{s}}-\varphi^{\mathrm{c}}) \tag{7}$$

$$Q_{\mathrm{P}}\approx\frac{\sqrt{2P^{\mathrm{a}}}}{2}R(\tau^{\mathrm{c}}-\tau^{\mathrm{a}})\sin(\varphi^{\mathrm{a}}-\varphi^{\mathrm{c}})+\frac{\sqrt{2P^{\mathrm{s}}}}{2}R(\tau^{\mathrm{c}}-\tau^{\mathrm{s}})\sin(\varphi^{\mathrm{s}}-\varphi^{\mathrm{c}}) \tag{8}$$

其中,P^{a},P^{s} 分别为真实信号和欺骗信号的功率;τ^{c} 为本地扩频码相位;τ^{a} 为真实信号码相位;τ^{s} 为欺骗信号码相位;φ^{a} 为真实信号载波相位;φ^{c} 为复制信号载波相位;φ^{s} 欺骗信号载波相位;$R(\cdot)$ 为扩频码的互相关函数。若导航数据码为 −1,则 I_{P},Q_{P} 分别为式(7)、式(8)的相反数。$I_{\mathrm{E}}(Q_{\mathrm{E}})$,$I_{\mathrm{L}}(Q_{\mathrm{L}})$ 为 $I_{\mathrm{P}}(Q_{\mathrm{P}})$ 左右两侧间隔 0.5 个码片的相关输出。

2　算法原理

2.1　传统欺骗检测算法

2.1.1　Ratio 检测量

Ratio 为一种经典的 SQM 欺骗干扰检测算法,利用同相支路上 I_{E},I_{P} 和 I_{L} 输出组合成检测量

$$M_{\text{Ratio}}=\frac{I_{\text{E}}+I_{\text{L}}}{\beta I_{\text{P}}} \tag{9}$$

其中，β 为 C/A 码相关峰斜率，不失一般性，本文取 $\beta=1$。Ratio 检测量的输出服从高斯分布[24]，令 $X=M_{\text{Ratio}}$，X 的概率密度函数为

$$f(x)=\frac{1}{\sqrt{2\pi}\sigma_n}\exp\left(-\frac{(x-u_{\text{r}})^2}{2\sigma_n^2}\right) \tag{10}$$

其中，u_{r} 为无欺骗干扰情况下 Ratio 的均值；σ_n^2 为高斯白噪声的方差。

2.1.2 PCS 检测量

针对中级欺骗的欺骗信号与真实信号功率相近的问题，为弥补绝对功率检测技术的缺陷，PCS 检测量融合绝对功率监测与 SQM

$$M_{\text{PCS}}=E+L-2P \tag{11}$$

其中，E，P，L 分别为超前、即时与滞后相关器的输出，有 $E=\sqrt{I_{\text{E}}^2+Q_{\text{E}}^2}$，$L=\sqrt{I_{\text{L}}^2+Q_{\text{L}}^2}$ 和 $P=\sqrt{I_{\text{P}}^2+Q_{\text{P}}^2}$。令 $Z=P$，据信号检测与估计理论可知，Z 服从莱斯分布[24]，Z 的概率密度分布函数为

$$f(z)=\begin{cases}\dfrac{z}{\sigma_n^2}\exp\left(\dfrac{z^2+u_z^2}{2\sigma_n^2}\right)I_0\left(\dfrac{zu_z}{\sigma_n^2}\right), & z\geqslant 0\\ 0, & \text{其他}\end{cases} \tag{12}$$

其中，σ_n^2 为高斯白噪声的方差；u_z 代表无欺骗情况下 Z 的均值；$I_0(\cdot)$ 为 0 阶修正贝赛尔函数。当信噪比远大于 1 时，E，P 和 L 近似服从高斯分布[15]，由于高斯分布线性组合还是高斯分布[25]，因此 PCS 近似服从高斯分布。

2.1.3 ELP 检测量

ELP 检测量方法使用载波超前和滞后的相位差检测欺骗信号

$$M_{\text{ELP}}=\tan^{-1}\left(\frac{Q_{\text{E}}}{I_{\text{E}}}\right)-\tan^{-1}\left(\frac{Q_{\text{L}}}{I_{\text{L}}}\right) \tag{13}$$

其中，$I_{\text{E}}(Q_{\text{E}})$ 和 $I_{\text{L}}(Q_{\text{L}})$ 分别为同相(正交)支路超前和滞后相关器输出结果。ELP 近似服从高斯分布[22]。

2.2 SAIBO 及其 SAIBO-MA 算法

针对 PCS，Ratio 和 ELP 存在检测性能不理想的问题，通过对同相支路上的超前、即时和滞后相关器取绝对值，再求和构建 SAIBO 检测量

$$M_{\text{SAIBO}}=|I_{\text{E}}|+|I_{\text{P}}|+|I_{\text{L}}| \tag{14}$$

由于 $|I_{\text{E}}|$，$|I_{\text{P}}|$ 和 $|I_{\text{L}}|$ 近似服从高斯分布，因此 SAIBO 同样近似服从高斯分布。其输出结果直方统计如图 2 所示。

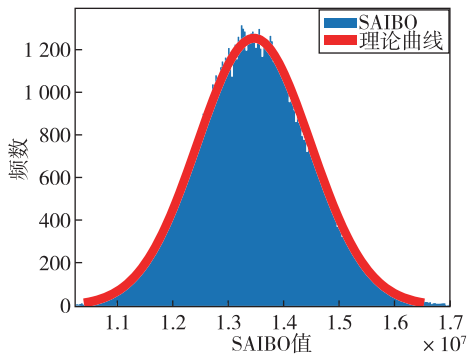


图 2 SAIBO 检测量输出分布

Fig. 2 Distribution of SAIBO detection metric output values

文献[26]对 SCS 检测量进行滑动平均处理，以抑制噪声，提高检测即时性。借鉴其思路，本文以固定长度窗口进行滑动处理，计算 SAIBO 检测量在窗口内的均值，构建 SAIBO-MA 检测量

$$M_{\text{SAIBO-MA}}(n)=\frac{1}{\omega}\sum_{i=nL+1}^{nL+\omega}M_{\text{SAIBO}}(i),\quad n=1,2,\cdots,N \tag{15}$$

其中，ω 表示滑动平均的窗口长度；N 表示滑动窗口个数；L 表示滑动间隔。

通过式(15)再次重构得到检测量 SAIBO-MA。从左到右滑动窗口，得到 N 个数据。SAIBO-MA 的滑动过程如图 3 所示。

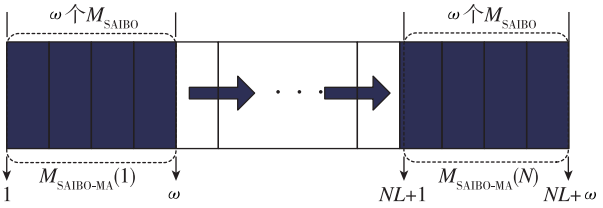


图 3 SAIBO-MA 示意图

Fig. 3 SAIBO-MA schematic

3 判决门限及假设检验

欺骗信号的检测问题可视为一个二元假设检验问题，假设 H_0 表示无欺骗干扰，H_1 表示存在欺骗干扰

$$\begin{cases}H_0:\text{无欺骗}\\ H_1:\text{有欺骗}\end{cases} \tag{16}$$

其中，当检测量输出在门限内时，判为无欺骗；反之，判为有欺骗。判决会产生 4 种结果，其中 $H_1|H_0$ 和 $H_1|H_1$ 分别表示虚警事件和检测事件，对判决结果影响最大。记虚警事件和检测事件对应的概率分别为虚警概率 P_{fa} 和检测概率 P_{d}。

根据文献[26]，对于一个双门限的检测，理论上虚警概率 P_{fa} 和检测概率 P_{d} 可以通过式(17)、式

(18)计算。

$$P_{\mathrm{fa}}=\int_{-\infty}^{\gamma_{\mathrm{Th,l}}} f(z\mid H_0)\mathrm{d}z+\int_{\gamma_{\mathrm{Th,u}}}^{\infty} f(z\mid H_0)\mathrm{d}z \quad (17)$$

$$P_{\mathrm{d}}=\int_{-\infty}^{\gamma_{\mathrm{Th,l}}} f(z\mid H_1)\mathrm{d}z+\int_{\gamma_{\mathrm{Th,u}}}^{\infty} f(z\mid H_1)\mathrm{d}z \quad (18)$$

其中，$\gamma_{\mathrm{Th,l}}$ 和 $\gamma_{\mathrm{Th,u}}$ 分别表示检测上限和检测下限；$f(\cdot)$ 表示概率密度函数。

由于存在欺骗信号时，欺骗信号的参数时变且未知，无法基于式(17)和式(18)得到 P_{fa} 和 P_{d} 的理论结果，一般采用统计方法计算。首先，设定检测门限上下限 $\gamma_{\mathrm{Th,l}}$ 和 $\gamma_{\mathrm{Th,u}}$，当检测量输出超过检测门限时，判为有欺骗；反之，则判为无欺骗。然后统计有欺骗(无欺骗)的样本点数，在无欺骗存在时间段内，P_{fa} 为判为有欺骗的样本数与样本总数的比值，P_{d} 为滑动窗口内判为欺骗的样本点数与滑动窗口内的样本总数的比值。使用统计方法计算虚警概率 P_{fa} 和检测概率 P_{d} 的公式为

$$P_{\mathrm{fa}}=\frac{N(M_{\mathrm{SAIBO}}(n)<\gamma_{\mathrm{Th,l}})+N(M_{\mathrm{SAIBO}}(n)>\gamma_{\mathrm{Th,u}})}{q} \quad (19)$$

$$P_{\mathrm{d}}=\frac{N(M_{\mathrm{SAIBO}}(n)<\gamma_{\mathrm{Th,l}})+N(M_{\mathrm{SAIBO}}(n)>\gamma_{\mathrm{Th,u}})}{p} \quad (20)$$

其中，q 和 p 分别代表无欺骗时的样本总数和滑动窗口中的样本总数；$\gamma_{\mathrm{Th,l}}$ 和 $\gamma_{\mathrm{Th,u}}$ 分别代表检测上下限；$N(\cdot)$ 代表满足条件的数量。

SAIBO 的检测概率 P_{d} 的计算过程为：预先设置虚警概率，将其代入式(19)中，计算检测下限 $\gamma_{\mathrm{Th,l}}$ 和检测上限 $\gamma_{\mathrm{Th,u}}$，进一步将检测门限代入式(20)计算出检测概率，其他检测量的检测概率也可使用该方法计算。为清晰地反映检测概率的变化趋势，采用滑动窗口方法将检测量的输出数据划分为多个子窗口，每个窗口内含有 p 个采样点数据，从左到右地滑动窗口依次计算出每一个子窗口对应的检测概率 P_{d} 并绘制出检测概率曲线。

4　实验及性能分析

4.1　数据集介绍及检测量输出

4.1.1　数据集介绍

采用美国德克萨斯大学奥斯汀分校的 TEXBAT 数据集中的 DS7 进行中级欺骗的检测实验。DS7 是以欺骗类型为时间欺骗、采样频率为 24 MHz、码速率为 1.023 MHz、牵引策略为载波同步、数据长度为 468 s 和数据类型为 I/Q 型的静态欺骗数据集。由于载波同步意味同频同相，因此欺骗的隐蔽性更好。取 TEXBAT 数据集的 DS7 的前 460 s 数据进行中级欺骗的检测实验，110 s 前为干净数据；110～130 s 为欺骗攻击的第Ⅰ阶段，注入欺骗信号；130～150 s 为第Ⅱ阶段，即欺骗对齐阶段；150～400 s 为第Ⅲ阶段，对应欺骗牵引阶段；400～460 s 为欺骗攻击的Ⅳ阶段，对应欺骗分离阶段。第Ⅱ阶段至第Ⅳ阶段，欺骗信号与真实信号的相位差为 π。

4.1.2　检测量输出

通过前面分析得到同相支路的输出结果，然后经过取绝对值后再求和得到 SAIBO 检测量，并在滑动平均处理后构建 SAIBO-MA 检测量。SAIBO-MA 算法的流程图如图 4 所示。

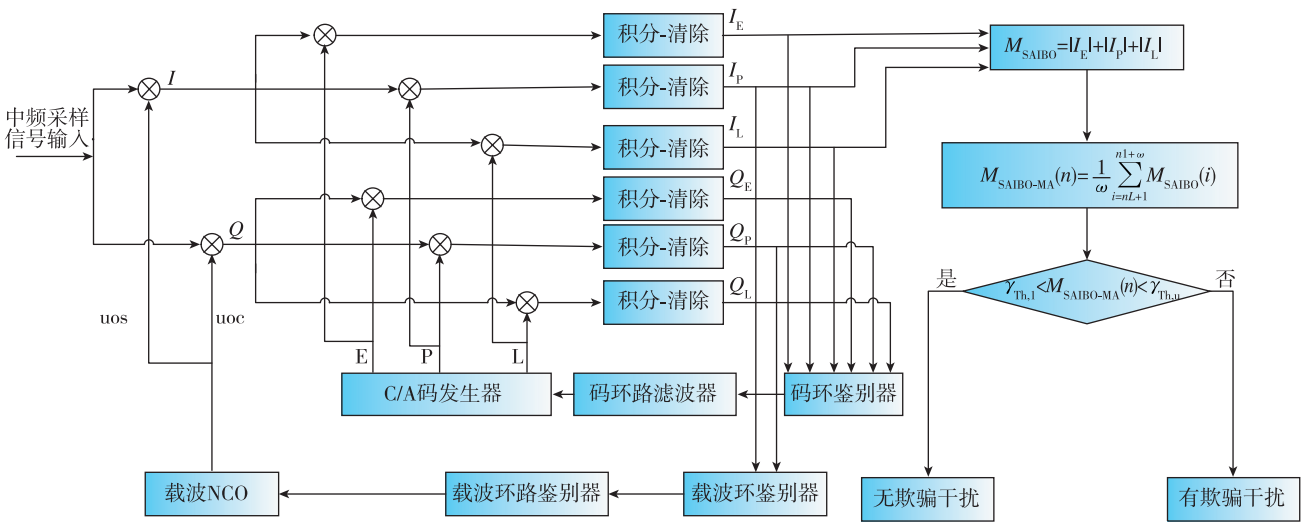


图 4　SAIBO-MA 检测量流程图

Fig. 4　SAIBO-MA detection metric flowchart

对 DS7 中的 PRN23 进行处理，得到 SAIBO 检测量输出波形随时间的变化情况，如图 5 所示。

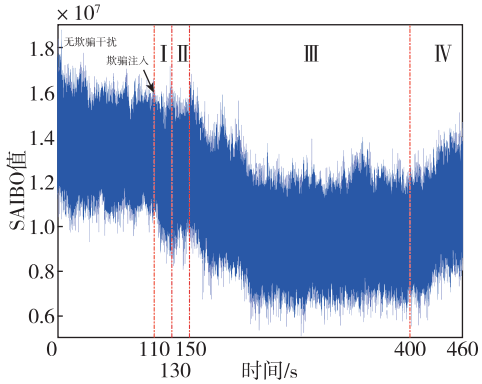


图 5 SAIBO 检测量

Fig. 5 SAIBO detection metric

由图 5 结果可见，SAIBO 检测量输出波形的波动范围大，并在欺骗第Ⅰ阶段到欺骗第Ⅲ阶段初，SAIBO 检测量的波形无明显畸变。采用长度为 100 ms 的滑动窗进行处理，得到 SAIBO-MA 检测量如图 6 所示。

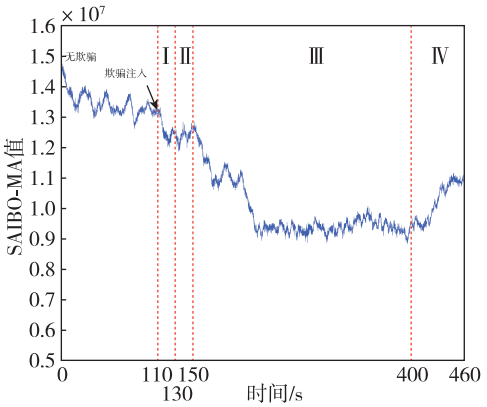


图 6 SAIBO-MA 检测量

Fig. 6 SAIBO-MA detection metric

根据图 6 结果分析可见，前 110 s 无欺骗干扰，SAIBO-MA 的输出为正常波形；在 110～130 s，注入欺骗信号，SAIBO-MA 的输出发生明显畸变；在 130～150 s，波形明显低于正常输出的波形；150～400 s，输出波形再次下降，并逐渐稳定；400 s 后，波形虽有上升，但仍然低于正常波形。

综合图 5 和图 6 的结果，与 SAIBO 检测量相比，SAIBO-MA 检测量的输出波形随时间变化的趋势更加清晰，且 114 s 左右发生畸变后，便持续区别于无欺骗情况下的输出波形。因此基于 MA 处理，一方面可减小检测量的波动范围，同时可清晰反映其随时间的变化趋势。

4.2 检测概率与判决

预先设定虚警概率为 10%，代入式(19)，计算 SAIBO 的检测上限和下限分别为 1.515×10^7 和 $1.117\ 9\times10^7$，再将其代入式(20)中，进一步计算出检测概率。为清楚反映检测概率随时间的变化情况，通过滑动窗口方式计算检测概率。以 PRN23 为例，PCS，Ratio，ELP 与 SAIBO 四类算法的检测概率结果如图 7 所示。

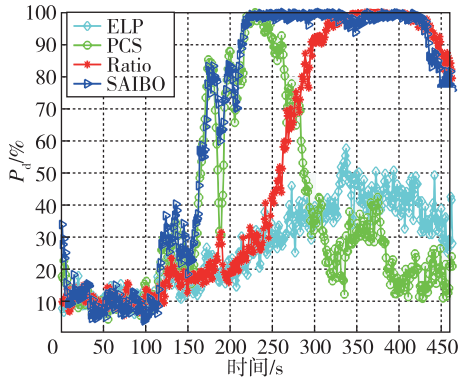


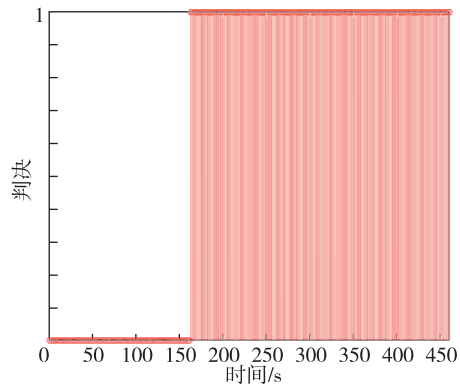
图 7 原始检测量的检测概率对比

Fig. 7 Comparison of detection probabilities of original detection metric

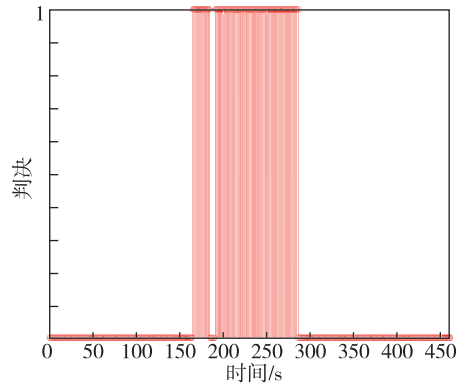
对比四类算法的检测概率，SAIBO 算法的检测概率在 163～460 s 间始终大于 50%；Ratio 的检测概率在 256 s 后始终大于 50%；PCS 算法的检测概率仅在 165～285 s 间有绝大部分大于 50%；ELP 算法的检测概率在绝大多数时间范围内低于 50%。注入欺骗后，与 PCS，Ratio 和 ELP 算法相比，SAIBO 算法拥有最高检测概率和最好的检测即时性，ELP 算法的检测效果最差。

基于二元判决，假设检测概率不小于 50%判为有欺骗干扰，输出 1；反之，判为无欺骗干扰，输出 0，四类算法的二元判决结果如图 8 所示。

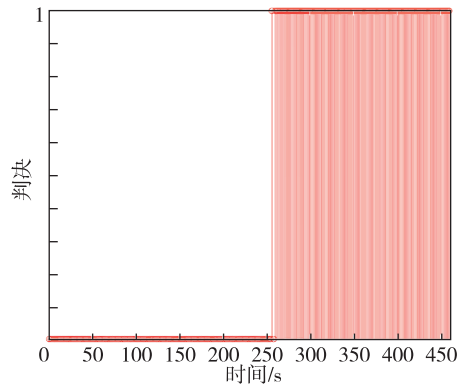
由图 8 结果可见，SAIBO 检测量判决为 1 的数量明显多于 PCS，Ratio 和 ELP 检测量判决为 1 的数量。因此，在欺骗发生时，SAIBO 检测量判决为欺骗的次数明显多于其他检测量。依次滑动窗口，得到 PCS-MA，Ratio-MA，ELP-MA 以及 SAIBO-MA 检测量，计算相应的检测概率并绘制在 460 s 时间段内，ELP 检测量仅有少部分点判决为欺骗干扰的数量，并且 4 种检测量在 150 s 前判决为欺骗的数目为 0，这是由于在图 7 中在 150 s 之前几种算



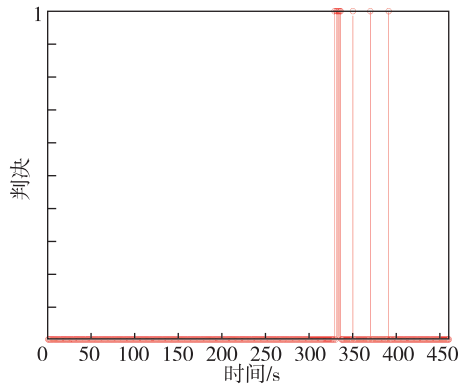
（a）SAIBO 检测量



（b）PCS 检测量



（c）Ratio 检测量



（d）ELP 检测量

图 8　二元判决对比

Fig. 8　Comparison of binary decision

法检测概率均低于 50%。

为进一步分析滑动平均检测量的检测性能，对 PCS，Ratio，ELP 和 SAIBO 检测量均采取滑动平均处理，以 $\omega=100$ ms 为固定的窗口长度，计算窗口内的原始检测量平均值作为新数据点检测概率曲线。以 PRN23 为例，各检测概率曲线如图 9 所示。

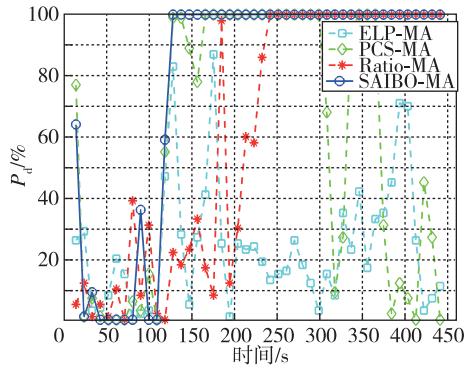


图 9　滑动平均检测量的检测概率对比

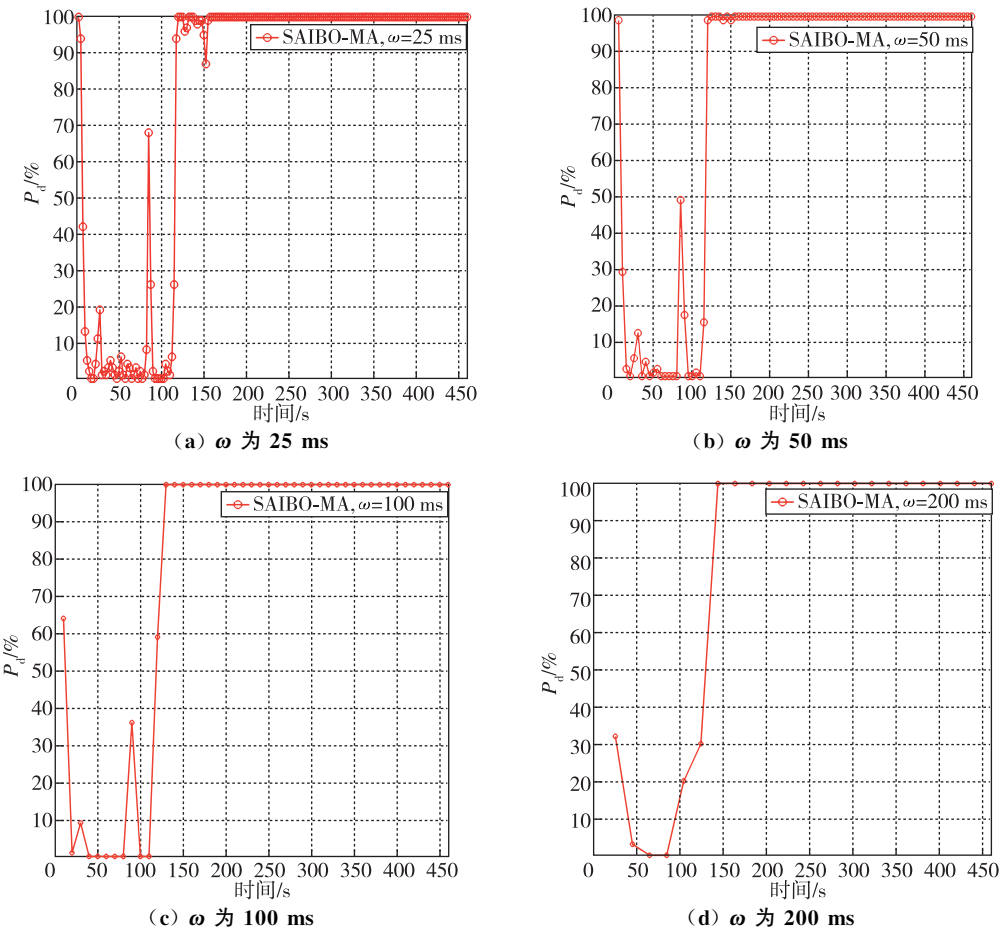
Fig. 9　Comparison of detection probability of moving average detection metric

对比分析可知，110～460 s 间，SAIBO-MA 检测量的检测概率从第 120 s 开始大于 50%，并从第 130 s 之后始终保持在 100%。在 110 s 注入欺骗后，PCS-MA 检测概率同样开始大于 50%，但在 330～340 s 和 390～460 s 两个时段内检测概率明显低于 50%；在欺骗信号存在的情况下，Ratio-MA 检测量的检测概率在第 190 s 大于 50%，但在 110～180 s 和第 200～210 s 间，检测概率低于 50%；ELP-MA 仅有极少部分检测概率大于 50%。

综合以上分析，PCS，Ratio，ELP，SAIBO 四类算法均在 160 s 以后才检测到欺骗存在，且与其他三类算法相比，SAIBO 算法拥有更高的检测概率；SAIBO-MA 算法在 120 s 即可检测到欺骗存在，且 120 s 之后检测概率始终保持在 100%，与 SAIBO 算法相比，SAIBO-MA 算法拥有更好的检测即时性和更高的检测概率。

分别取 ω 为 25 ms，50 ms，100 ms 和 200 ms，为评估 SAIBO-MA 的检测概率受 ω 的影响情况，欺骗检测概率结果如图 10 所示。

对比仿真结果可知，随着滑动窗口长度的增加，SAIBO-MA 检测概率波动趋势减小；且随着 ω 的增加，SAIBO-MA 算法的即时性变差。在 SAIBO-MA 算法中，选择合适的窗口长度可以提高欺骗检测的即时性。



（a）ω 为 25 ms （b）ω 为 50 ms

（c）ω 为 100 ms （d）ω 为 200 ms

图 10 SAIBO-MA 的检测概率随 ω 的变化曲线对比

Fig. 10 Comparison of the curve of SAIBO-MAdetection probability with ω

4.3 接收机工作特性曲线

为进一步分析检测量在任意虚警概率下的欺骗检测性能，引入接收机工作特性（receiver operating characteristic，ROC）曲线。图中横轴为虚警概率，纵轴为欺骗第Ⅱ阶段初与第Ⅳ阶段末之间的平均检测概率。以 PRN23 为例，SAIBO，PCS，Ratio 和 PCSR 以及对应 MA 的 ROC 曲线如图 11 所示。在 ROC 图中，离左上角越近，检测越准确。

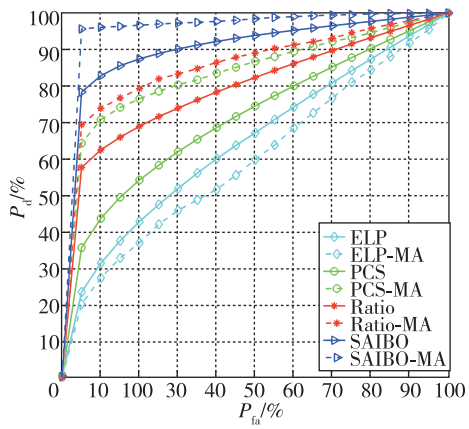


图 11 ROC 曲线对比

Fig. 11 Comparison of ROC curve

由图 11 可见，当虚警概率为 10%时，SAIBO 与 SAIBO-MA 的检测概率分别为 82.77%和 96.08%。在任意虚警概率下，SAIBO 和 SAIBO-MA 的检测概率始终高于其他传统算法的检测概率。虚警概率越小，SAIBO-MA 的检测概率越接近 ROC 图中的左上角，检测精度最高。

为进一步分析 SAIBO-MA 检测量的稳健性，选取 PRN3，PRN7 和 PRN23，比较分析 ELP-MA，PCS-MA，Ratio-MA 以及 SAIBO-MA 的检测概率随虚警概率变化，如图 12 所示。

根据图 12，在选取的 3 颗卫星中，PRN23 检测效果最好，其次是 PRN7，最后为 PRN3。与 ELP-MA，PCS-MA 和 Ratio-MA 相比，SAIBO-MA 算法的检测概率在虚警概率越低的情况下离 ROC 图的左上角越近，任意虚警概率下 SAIBO-MA 算法的检测概率始终高于另外 3 种平均算法的检测概率，因此 SAIBO-MA 算法具有更高的检测精度和更好的稳健性。

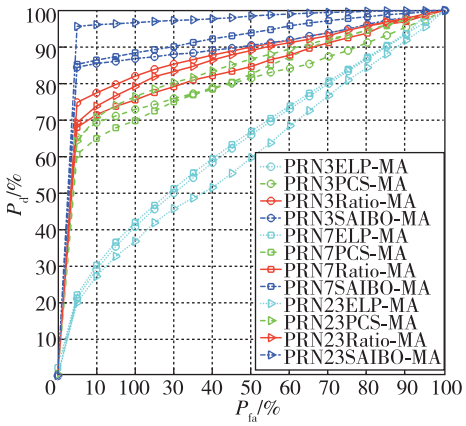


图 12　检测概率随虚警概率的变化曲线对比

Fig. 12　Comparison of the curve of detection probability with the probability of false alarm

5　结论

针对在功率随时间变化，载波同步欺骗场景下，传统欺骗检测算法的检测性能不理想的问题，提出了 SAIBO 检测算法。为更清晰地反映输出波形随时间变化情况，减小噪声影响，改善检测即时性，进一步对 SAIBO 做 MA 处理。使用 TEXBAT 数据集的 DS7 做中级欺骗的检测实验，比较分析 SAIBO，PCS，ELP 和 Ratio 及其对应的 MA 算法的检测性能，实验显示：

1）存在欺骗信号时，与 PCS，ELP 和 Ratio 相比，SAIBO 拥有更高的检测概率、更多判决为欺骗的数目以及更宽的检测范围。

2）在功率随时间变化，载波同步的欺骗场景下，SAIBO-MA 欺骗算法具有更好的检测即时性和稳健性以及更高的精度。

3）在不增加算法复杂度的情况下，SAIBO-MA 算法极大提高了检测性能，且不需要外加设备的辅助便能完成对欺骗信号的检测。

参考文献

[1] 张鑫，丁宸聪，陈书恒．利用旋转双天线载波相位双差的欺骗干扰检测技术[J]．导航定位与授时，2023，10(2)：32-38.
ZHANG Xin，DING Chencong，CHENG Shuheng. Spoofing detection technology using carrier phase double difference of spin dual-antenna[J]. Navigation Positioning and Timing，2023，10(2)：32-38(in Chinese).

[2] 刘清秀，程玉，王国栋，等．北斗卫星导航欺骗与抗欺骗技术现状探讨[J]．导航与控制，2021，20(4)：24-32.
LIU Qingxiu，CHENG Yu，WANG Guodong，et al，Discussion on deception and anti-deception technology of Beidou satellite navigation[J]. Navigation and Control，2021，20(4)：24-32(in Chinese).

[3] 刘丁浩，吕晶，马蕊，等．卫星导航系统欺骗与抗欺骗技术研究与展望[J]．通信技术，2017，50(5)：837-843.
LIU Dinghao，LYU Jing，MA Rui，et al. The research and prospect of spoofing and anti-spoofing technology in the satellite navigation system[J]. Communications Technology，2017，50(5)：837-843(in Chinese).

[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] 钟伦珑，刘炅坡，刘永玉．基于误差估值累加开环校正的诱导式欺骗检测方法[J]．电信科学，2022，38(9)：116-128.
ZHONG Lunlong，LIU Jiongpo，LIU Yongyu. Induced spoofing detection method based on error valuation cumulative open-loop correction[J]. Telecommunications Science，2022，38(9)：116-128(in Chinese).

[6] 王文益，龚婧，王金铭．基于 SCB 方差的 GNSS 欺骗式干扰检测算法[J]．系统工程与电子技术，2021，43(8)：2254-2262.
WANG Wenyi，GONG Jing，WANG Jinming. GNSS spoofing interference detection based on variance of SCB[J]. Systems Engineering and Electronics，2021，43(8)：2254-2262(in Chinese).

[7] ROTHMAIER F，CHEN Y-H，LO S，et al. GNSS spoofing detection through spatial processing[J]. Navigation，2021，68(2)：234-258.

[8] NIELSEN J，BROUMANDAN A，LACHAPELLE G. GNSS spoofing detection for single antenna handheld receivers[J]. Navigation，2011，58(4)：335-344.

[9] CHEN J，XU Y，YUAN H，et al. A new GNSS spoofing detection method using two antennas[J]. IEEE Access，2020，8：110738-110747.

[10] MAGIERA J. A multi-antenna scheme for early detection and mitigation of intermediate GNSS spoofing[J]. Sensors，2019，19(10)：2411.

[11] DOBRYAKOVA A L，LEMIESZEWSKI S L，OCHIN F E. GNSS spoofing detection using static or rotating single-antenna of a static or moving victim[J]. IEEE Access，2018，6：79074-79081.

[12] GU N, XING F, YOU Z. GNSS spoofing detection based on coupled visual/inertial/GNSS navigation system [J]. Sensors, 2021, 21(20): 6769.

[13] TAO H, WU H, LI H, et al. GNSS spoofing detection based on consistency check of velocities[J]. Chinese Journal of Electronics, 2019, 28(2): 437-444.

[14] 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): 732-741.

[15] 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.

[16] ZHANG X, LI H, YANG C, et al. Signal quality monitoring-based spoofing detection method for global navigation satellite system vector tracking structure[J]. IET Radar, Sonar & Navigation, 2020, 14(6): 944-953.

[17] WANG W, LI N, WU R, et al. Detection of induced GNSS spoofing using S-curve-bias[J]. Sensors (Basel,Switzerland), 2019, 19(4): 922.

[18] SUN C, CHEONG J W, DEMPSTER G A, et al. Robust spoofing detection for GNSS instrumentation using Q-channel signal quality monitoring metric[J]. IEEE Transactions on Instrumentation and Measurement, 2021, 70: 1-15.

[19] PHELTS R E. Multicorrelator techniques for robust mitigation of threats to GPS signal quality[D]. California: Stanford University, 2001.

[20] MUBARAK O M, DEMPSTER A G. Analysis of early late phase in single-and dual-frequency GPS receivers for multipath detection[J]. GPS Solutions, 2010, 14(4): 381-388.

[21] SUN C, CHEONG J W, DEMPSTER G A, et al. GNSS spoofing detection by means of signal quality monitoring (SQM) metric combinations[J]. IEEE Access, 2018, 6: 66428-66441.

[22] DEHGHANIAN V, NIELSEN J, LACHAPELLE G. GNSS spoofing detection based on signal power measurements: statistical analysis[J]. International Journal of Navigation and Observation, 2012(7): 313527.

[23] 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).

[24] 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).

[25] 龚婧．基于 SQM 方差的单天线 GNSS 欺骗式干扰检测算法的研究[D]．天津：中国民航大学，2020.
GONG Jing. Single antenna GNSS spoofing detection based on moving variance of SQM[D]. Tianjin: Civil Aviation University of China, 2020(in Chinese).

[26] 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 algorith[J]. Modern Electronics Technique, 2023, 46(11): 1-8(in Chinese).

（编辑：黄利华）