文章编号：2095-4980(2026)01-0027-09

基于IQ支路绝对值求和的GNSS诱导式欺骗检测

夏耀祖，王文益

(中国民航大学 天津市智能信号与图像处理重点实验室，天津 300300)

摘　要：全球卫星导航系统(GNSS)已在大众消费、机械控制、航海航空以及灾害救援等领域得到了广泛应用。但由于导航信号的微弱性以及GNSS系统对用户接口的开放性，GNSS极易受到欺骗攻击。信号质量监测(SQM)技术不仅方法简单，且已被证明可用于检测GNSS欺骗攻击，但传统的SQM算法易受环境等因素影响，很难同时满足检测精确度和检测时效性的基本需求。本文提出一种利用同相(I)和正交(Q)支路的绝对值相加求和的欺骗检测算法，实现逻辑简单，且仅需对GNSS接收机进行少量代码更新。使用美国德克萨斯大学奥斯汀分校的欺骗信号数据集(TEXBAT)进行实验分析，结果表明，与传统的SQM算法相比，本文所提算法检测诱导式欺骗攻击时检测速度更快，欺骗检测性能更优。

关键词：全球卫星导航系统(GNSS)；诱导式欺骗；欺骗检测；信号质量监测；检测概率

中图分类号：TN967.1　　**文献标志码：**A　　**DOI：**10.11805/TKYDA2025009

GNSS induced spoofing detection based on absolute sum of IQ branches

XIA Yaozu，WANG Wenyi

(Tianjin Key Laboratory for Intelligent Signal and Image Processing，Civil Aviation University of China，Tianjin 300300，China)

Abstract: Global Navigation Satellite Systems(GNSS) have been widely applied in mass consumer applications, mechanical control, maritime and aviation navigation, and disaster relief. However, due to the inherent weakness of navigation signals and the open user interface of GNSS, GNSS is highly vulnerable to spoofing attacks. Signal Quality Monitoring(SQM) technology offers a simple yet proven approach for detecting GNSS spoofing attacks. Nevertheless, traditional SQM algorithms are vulnerable to environmental factors, making it difficult to simultaneously satisfy the basic requirements of detection accuracy and timeliness. This paper proposes a spoofing detection algorithm based on the sum of absolute values from the in-phase(I) and quadrature(Q) branches. The implementation logic is simple and requires only minor software modifications to GNSS receivers. Experimental analysis using the spoofing signal dataset from the University of Texas at Austin(TEXBAT) demonstrates that, compared with conventional SQM algorithms, the proposed algorithm achieves faster detection speed and superior performance in detecting spoofing attacks.

Keywords: Global Navigation Satellite System(GNSS); induced spoofing; spoofing detection; signal quality monitoring; detection probability

全球卫星导航系统(GNSS)能够提供全天候、不间断、实时、全球覆盖的高精确度定位授时服务，已广泛用于农林业、金融、电网监控、通信等诸多领域，对国民经济和社会生活的各个方面都产生了深远影响[1-2]。因此，GNSS的安全性问题越来越受到人们的关注[3-4]。GNSS信号因功率低、信号标准公开极易遭受干扰和欺骗攻击[5-6]，其中，欺骗攻击会带来比干扰更大的危险。欺骗攻击可产生与真实信号结构相同的欺骗信号，并诱使目标接收机相信它们是真实信号，逐渐误导目标接收机的跟踪过程，进而导致错误的导航和授时结果[7-8]。因此，

收稿日期：2025-01-08；**修回日期：**2025-02-25

引用格式：夏耀祖,王文益. 基于IQ支路绝对值求和的GNSS诱导式欺骗检测[J]. 太赫兹科学与电子信息学报, 2026,24(1):27-35. DOI:10.11805/TKYDA2025009.

Citation format: XIA Yaozu,WANG Wenyi. GNSS induced spoofing detection based on absolute sum of IQ branches[J]. Journal of Terahertz Science and Electronic Information Technology, 2026,24(1):27-35. DOI:10.11805/TKYDA2025009.

对GNSS欺骗攻击的检测引起了越来越多的重视[9]。根据欺骗信号产生难易程度，欺骗干扰可分为简单欺骗式干扰、中级欺骗式干扰和高级欺骗式干扰3类[10-11]，其中，中级欺骗式干扰高效，便于实施，使其成为一种主要的欺骗技术[12]。中级欺骗式干扰也称为诱导式欺骗干扰，其基于目标接收机的动态性能，通过调整欺骗信号的功率和码速率等参数，在目标接收机尚未察觉的情况下控制其跟踪环路，进而输出错误的时间和位置信息[13]。由于中级欺骗式干扰的隐蔽性强，实现成本低，已成为GNSS欺骗干扰检测研究的重要领域之一。

近年来，信号质量监测技术(SQM)因算法简单、可行性高等优点在欺骗检测领域大量运用[14]。SQM算法使用接收机码跟踪环超前、即时和滞后相关器输出进行测量，然后通过计算得到的检测量识别由欺骗信号引起的异常尖锐、平坦或不对称的相关峰值[15]。为准确识别由欺骗攻击引起的相关函数失真，研究人员已开发出多种简单有效的SQM指标，如，Phelts最早提出了Delta和Ratio两种SQM算法。Delta算法通过相关峰值的不对称性进行欺骗检测，而Ratio算法则通过相关函数峰值处的“死区”(平坦相关峰)的存在进行检测[16]。之后，为改进Delta算法，出现了Double-Delta算法[17]。随后，通过利用超前和滞后码片的相位差检测欺骗信号，验证了ELP (Early Late Phase)算法的有效性[18]。随着欺骗攻击方法的不断更新与进步，传统SQM算法的有效性和鲁棒性变得越来越差。因此文献[19]利用不同SQM算法间的互补特性，开发了一种利用Ratio、Delta和ELP算法的多指标联合检测技术，将各种SQM算法组合成复合SQM算法检测欺骗攻击。文献[20]利用正交通道的异常能量构建指标，提出了Q-channel的欺骗攻击检测方法。此外，文献[21]通过在捕获模块中应用多模态检测技术，并利用采集模块监视被跟踪信号，通过判断超出阈值的峰值数量进行欺骗攻击检测。随后，文献[22]提出利用左右相关峰多个相关器的时域瞬态响应的加权中心二阶矩进行欺骗攻击检测。此后，文献[23]提出了一种新的欺骗攻击检测方法，该方法通过将时域相关器的输出转换到频域，再利用欺骗攻击的特征进行欺骗攻击检测。

本文提出了一种新的欺骗检测方法，通过同时利用I、Q支路绝对值输出相加求和，构建新的欺骗检测量。采用美国德克萨斯大学奥斯汀分校TEXBAT数据集分析所提算法性能，并与Ratio、Delta、ELP和Q-channel四种传统SQM算法性能比较。结果显示，所提算法检测概率更高，检测性能更好。

1 诱导式欺骗过程与信号模型

1.1 诱导式欺骗过程

诱导式欺骗攻击凭借改变欺骗信号功率、码相位等参数，慢慢将接收机跟踪的信号从真实信号转变为欺骗信号，最终导致接收机产生错误的时间、位置等信息。诱导式欺骗过程如图1所示，最初，欺骗信号大致地估算真实信号的码相位、载波频率等信息，然后以较低的功率从距离真实信号数个码片的位置缓慢地向真实信号靠近，在靠近过程中逐渐调整其自身码相位与真实信号一致。一旦欺骗信号与真实信号码相位对齐，欺骗信号功率将缓慢增大，最终超过真实信号功率，进而掌控接收机跟踪环路。之后，欺骗信号调节码相位，慢慢远离真实信号，从而诱使接收机跟踪欺骗信号。当欺骗信号相关峰与真实信号相关峰完全分离时，此时接收机的跟踪环路已开始完全跟踪欺骗信号，诱导式欺骗成功。

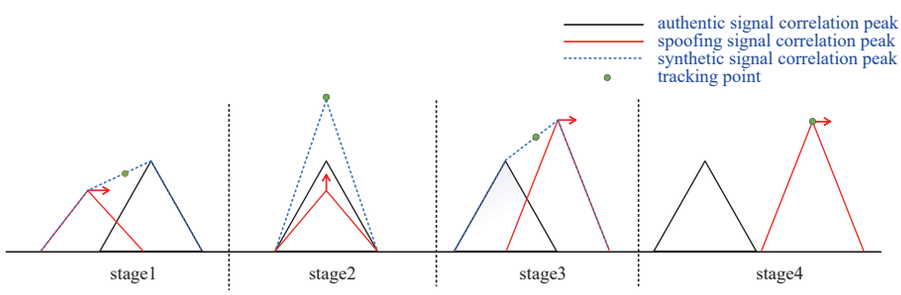

Fig.1 Induced spoofing process
图1 诱导式欺骗过程

1.2 信号模型

遭遇欺骗攻击时，接收机中频信号包括真实信号、欺骗信号及噪声：

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

式中：下标a、s分别表示真实、欺骗；$x_{\mathrm{a}}(t)$为真实信号；$x_{\mathrm{s}}(t)$为欺骗信号；$n(t)$为零均值加性高斯白噪声。

真实信号与欺骗信号可表示为：

$$x_a(t)=\sqrt{P_a(t)}\,D_a(t-\tau_a)C(t-\tau_a)\cos\left(2\pi\left(f_0+f_{d,a}\right)t+\varphi_a\right) \tag{2}$$

$$x_s(t)=\sqrt{P_s(t)}\,D_s(t-\tau_s)C(t-\tau_s)\cos\left(2\pi\left(f_0+f_{d,s}\right)t+\varphi_s\right) \tag{3}$$

式中：P为信号功率；D为数据码；C为伪随机码；τ为信号传播时延；f_0为中心频率；f_d为多普勒频移；φ为载波初相位。

当中频信号经过粗捕获(Coarse Acquisition，C/A)码相关器进行相关计算后，单颗卫星通道I支路和Q支路的超前、即时、滞后相干积分器输出可表示为:

$$I_E(t,\tau)=\sqrt{P_a}\,R_a(t,\tau-d)\mathrm{sinc}\left(\Delta f_{d,a}T\right)\cos\varphi_a+\sqrt{P_s}\,R_s(t,\tau-d)\mathrm{sinc}\left(\Delta f_{d,s}T\right)\cos\varphi_s \tag{4}$$

$$Q_E(t,\tau)=\sqrt{P_a}\,R_a(t,\tau-d)\mathrm{sinc}\left(\Delta f_{d,a}T\right)\sin\varphi_a+\sqrt{P_s}\,R_s(t,\tau-d)\mathrm{sinc}\left(\Delta f_{d,s}T\right)\sin\varphi_s \tag{5}$$

$$I_P(t,\tau)=\sqrt{P_a}\,R_a(t,\tau)\mathrm{sinc}\left(\Delta f_{d,a}T\right)\cos\varphi_a+\sqrt{P_s}\,R_s(t,\tau)\mathrm{sinc}\left(\Delta f_{d,s}T\right)\cos\varphi_s \tag{6}$$

$$Q_P(t,\tau)=\sqrt{P_a}\,R_a(t,\tau)\mathrm{sinc}\left(\Delta f_{d,a}T\right)\sin\varphi_a+\sqrt{P_s}\,R_s(t,\tau)\mathrm{sinc}\left(\Delta f_{d,s}T\right)\sin\varphi_s \tag{7}$$

$$I_L(t,\tau)=\sqrt{P_a}\,R_a(t,\tau+d)\mathrm{sinc}\left(\Delta f_{d,a}T\right)\cos\varphi_a+\sqrt{P_s}\,R_s(t,\tau+d)\mathrm{sinc}\left(\Delta f_{d,s}T\right)\cos\varphi_s \tag{8}$$

$$Q_L(t,\tau)=\sqrt{P_a}\,R_a(t,\tau+d)\mathrm{sinc}\left(\Delta f_{d,a}T\right)\sin\varphi_a+\sqrt{P_s}\,R_s(t,\tau+d)\mathrm{sinc}\left(\Delta f_{d,s}T\right)\sin\varphi_s \tag{9}$$

式中：下标E、P、L分别表示超前、即时、滞后；d为超前或滞后相关器与即时相关器的间距，通常设为0.5chip；$\Delta f_{d,a}$与$\Delta f_{d,s}$分别为本地信号与真实、欺骗信号载波多普勒频差；T为相干积分时间；$R_a(t,\tau)$与$R_s(t,\tau)$分别为本地信号与真实、欺骗信号互相关函数。

2　检测算法

2.1 传统SQM欺骗检测算法

传统SQM欺骗检测技术通过接收机码跟踪环超前、即时和滞后相关器输出，构建不同的检测量检测跟踪环路中相关函数畸变，进而对诱导式欺骗干扰实施欺骗攻击检测。传统的SQM欺骗检测算法为：Ratio、Delta、ELP和Q-channel算法，分别定义为：

$$H_{\mathrm{Ratio}}(t)=\frac{I_E(t)+I_L(t)}{2I_P(t)} \tag{10}$$

$$H_{\mathrm{Delta}}(t)=\frac{I_E(t)-I_L(t)}{2I_P(t)} \tag{11}$$

$$H_{\mathrm{ELP}}(t)=\arctan\left(\frac{Q_E(t)}{I_E(t)}\right)-\arctan\left(\frac{Q_L(t)}{I_L(t)}\right) \tag{12}$$

$$H_{\mathrm{Q-channel}}(t)=\sqrt{\frac{Q_E^2(t)+Q_L^2(t)}{I_P^2(t)}} \tag{13}$$

Ratio算法通过检测相关函数顶部是否存在平坦区域实现欺骗检测。当不存在欺骗攻击时，相关函数呈现出无平坦区域的尖峰，同时Ratio值在正常值1附近波动；当存在欺骗攻击时，相关函数的峰值会变得平坦，Ratio值偏离正常值，表明出现异常。

Delta算法通过比较超前相关器输出与滞后相关器输出监测相关函数的对称性。当不存在欺骗攻击时，超前相关器输出与滞后相关器输出相等，Delta的正常值为0；当存在欺骗攻击时，超前相关器输出不再等于滞后相关器输出，Delta值偏离正常值。

ELP算法用于识别超前码片和滞后码片之间的载波相位差异。当不存在欺骗攻击时，超前码片相位和滞后码片相位一致，此时ELP输出为正常值0；当存在欺骗攻击时，超前码片和滞后码片的相位不一致，导致ELP值产生非零输出。

Q-channel算法是通过检测Q通道输出的异常能量进行欺骗检测。当不存在欺骗攻击时，Q通道输出通常在0附近波动；当存在欺骗攻击时，Q通道输出会发生显著波动。

2.2 本文所提算法

传统的SQM算法能够对诱导式欺骗干扰进行欺骗检测，但检测精确度低，检测性能差。为此，本文提出一种新的检测算法。

当接收机稳定跟踪真实信号时，I支路输出为信号能量和噪声，Q支路输出仅含噪声。一旦欺骗信号入侵，两信号间的相位差异会使部分能量转移至Q支路。若最后接收机稳定跟踪欺骗信号，由于欺骗信号的功率高于真实信号功率，因此跟踪环路内I支路输出包含的信号能量将会增大。为此，本文同时利用I支路和Q支路输出并取绝对值的方法构建一个新型的SQM检测量，定义为：

$$M(t)=\left|\frac{Q_{\mathrm{E}}(t)}{I_{\mathrm{P}}(t)}\right|+\left|\frac{Q_{\mathrm{L}}(t)}{I_{\mathrm{P}}(t)}\right|+\left|I_{\mathrm{P}}(t)\right| \tag{14}$$

当不存在欺骗攻击时，$Q_{\mathrm{E}}(t)$、$Q_{\mathrm{L}}(t)$和$I_{\mathrm{P}}(t)$均服从高斯分布，$\frac{Q_{\mathrm{E}}(t)}{I_{\mathrm{P}}(t)}$和$\frac{Q_{\mathrm{L}}(t)}{I_{\mathrm{P}}(t)}$为2个高斯分布变量的比值，根据文献[24]的理论推导，上述2个比值也服从高斯分布[25]。高斯分布的线性组合仍服从高斯分布，因此$M(t)$也近似服从高斯分布。在没有欺骗攻击的情况下，新型SQM检测量$M(t)$的直方图如图2所示。由图2可知，新型SQM检测量$M(t)$的理论概率密度函数(Probability Density Function，PDF)曲线与仿真结果几乎相同。

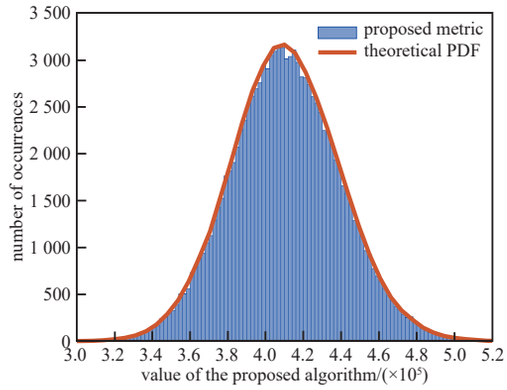

Fig.2 New SQM measurement histogram and theoretical PDF curve

图2 新型SQM检测量直方图与理论概率密度函数曲线

2.3 检测门限及概率分析

对于欺骗攻击的情况，欺骗检测问题可看作是一个二元信号检测问题，此时欺骗攻击的检测可转化为无欺骗攻击存在和有欺骗攻击存在这两种假设情况，分别用H_0和H_1表示。因此，二元信号检测函数可表示为：

$$\phi=\begin{cases}0\sim H_0 & \text{无欺骗攻击存在}\\ 1\sim H_1 & \text{有欺骗攻击存在}\end{cases} \tag{15}$$

在上述假设的基础上，虚警事件和检测事件对判决结果有显著影响。在假设H_0下，如果检测量输出值超出检测门限，则此时即使不存在欺骗攻击，也会错误地认为欺骗攻击存在，这种情况称为虚警事件，其发生概率即虚警概率，表示为P_{fa}。在假设H_1下，如果检测量输出值超出检测门限，且此时确实存在欺骗攻击，则认为欺骗攻击存在，这种情况称为检测事件，其发生概率即检测概率，表示为P_{d}。

理论上，双重门限SQM检测算法虚警概率P_{fa}和检测概率P_{d}计算公式可表示为：

$$P_{\mathrm{fa}}=\int_{-\infty}^{T_{\mathrm{l}}}p\left(z|H_0\right)\mathrm{d}z+\int_{T_{\mathrm{u}}}^{+\infty}p\left(z|H_0\right)\mathrm{d}z \tag{16}$$

$$P_{\mathrm{d}}=\int_{-\infty}^{T_{\mathrm{l}}}p\left(z|H_1\right)\mathrm{d}z+\int_{T_{\mathrm{u}}}^{+\infty}p\left(z|H_1\right)\mathrm{d}z \tag{17}$$

式中：z为SQM检测量的输出值；T_{l}和T_{u}分别为检测下限与检测上限。

当存在欺骗信号时，由于欺骗信号的参数随时间动态变化，使用式(16)~(17)计算所提算法的P_{fa}和P_{d}是不切实际的。因此，使用统计方法[26]计算P_{fa}和P_{d}：

$$P_{\mathrm{fa}}=\frac{\mathrm{num}\left(M(t)<T_{\mathrm{l}}\right)+\mathrm{num}\left(M(t)>T_{\mathrm{u}}\right)}{M} \tag{18}$$

$$P_{\mathrm{d}}=\frac{\mathrm{num}\left(M(t)<T_{\mathrm{l}}\right)+\mathrm{num}\left(M(t)>T_{\mathrm{u}}\right)}{N} \tag{19}$$

式中：$M(t)$为新型SQM检测量的输出值；num(·)表示满足相应条件的数量；M和N分别为在无欺骗攻击存在的情况下和有欺骗攻击存在的情况下的样本总量。

当虚警概率确定时，检测门限可根据以下步骤计算得出：

1) 对不存在欺骗攻击时的数据按照升序和降序分别进行排序，可得到序列s^{u}和s^{d}。然后。根据式(20)~(21)分别得到检测上限指标n_1和检测下限指标n_2：

$$n_1=\left[aMP_{\mathrm{fa}}\right] \tag{20}$$

$$n_2=\left[bMP_{\mathrm{fa}}\right] \tag{21}$$

式中a和b为门限因子，满足$a>0$，$b>0$，$a+b=1$。

2) 检测上限 T_u 和检测下限 T_l 可根据式(22)~(23)计算得到：

$$T_u = s_{n_1}^u \tag{22}$$

$$T_l = s_{n_2}^d \tag{23}$$

式(22)~(23)分别意味着序列 s^u 的第 n_1 个输出值为检测上限 T_u，而序列 s^d 的第 n_2 个输出值为检测下限 T_l。

3) 得到检测上限 T_u 和检测下限 T_l 后，再利用式(19)可得到检测概率。

为减少新型SQM检测量 $M(t)$ 中异常输出值导致的检测虚警概率增高，并有效抑制系统噪声，从而提高检测鲁棒性，对检测量 $M(t)$ 的数据值使用滑动平均处理。先选取一段长度为 W 的固定窗口，并以固定滑动间隔 L 从左至右滑动窗口，依次计算窗口选取不同检测量时的均值。其中第 n 个滑动窗口检测量均值为：

$$M_{avg}(n) = \frac{1}{W}\sum_{i=nL+1}^{nL+W} M(i),\ n = 0, 1, 2, \cdots, N \tag{24}$$

式中：$M(i)$ 为检测量数据值中第 i 个样本的值；N 为滑动窗口的总个数。

3　实验结果与分析

使用TEXBAT数据集对所提算法检测性能进行评估，并与Ratio、Delta、ELP和Q-channel四种传统SQM算法检测性能进行对比分析。

3.1　ds7场景下欺骗检测

利用TEXBAT数据集中第7条欺骗干扰数据进行实验分析和欺骗性能评估。第7条欺骗干扰数据是诱导式欺骗攻击场景，欺骗攻击从110 s开始发起，期间欺骗信号的幅值表现出非线性变化。最开始欺骗信号的码相位滞后真实信号2个码片，随后欺骗信号以相对真实信号1.2 m/s的速度运动。随着时间的变化，欺骗信号逐渐与真实信号重叠，并开始获得对目标接收机跟踪环路的控制权，从而最终使目标接收机产生1.27 μs的时钟偏移。

以第23号卫星为例，所提算法检测结果如图3所示。从图3中可以看出，本文所提检测算法的检测结果输出值存在较大的波动范围，但其随时间的变化过程并不明显，无法从整体上显著地观察到检测结果输出值随时间变化的趋势。采用窗口长度为100 ms的滑动窗对所提检测算法的检测结果输出值进行处理，经过滑动平均处理后，结果如图4所示。对所提算法检测结果输出值滑动平均处理后，检测结果输出值随时间变化的过程变得更加清晰和明显，从而能够更加直观地反映出所提检测算法检测结果输出值随时间变化的反应趋势。

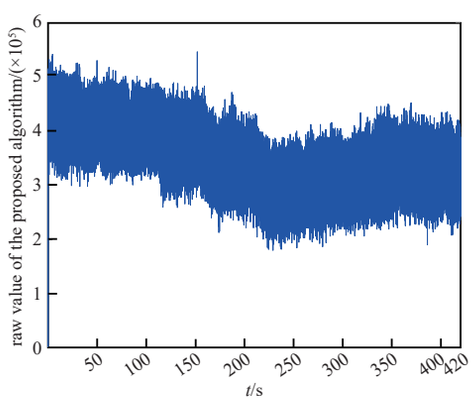

Fig.3 Raw values of detection results of the proposed algorithm
图3　所提算法检测结果原始值

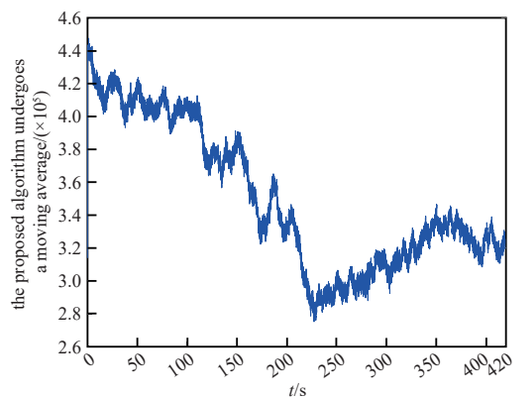

Fig.4 Detection results of the proposed algorithm after sliding mean processing
图4　所提算法检测结果经过滑动均值处理

为比较所提检测算法检测量与Ratio、Delta、ELP和Q-channel四种传统SQM算法检测量随时间变化的过程以及与检测门限的关系，通过预先设定虚警概率为10%，进而计算在此虚警概率下各检测算法的检测门限。Ratio、Delta、ELP、Q-channel和所提检测算法的检测量变化如图5所示。由图5可知，Ratio、Delta、ELP、Q-channel和所提检测算法的检测量均呈现出随时间变化的波动性。但所提检测算法与4种传统SQM算法相比，整体随时间变化的波动更为剧烈，表现出明显的起伏和变化，且所提检测算法的检测量大部分始终保持在检测门限之外，说明所提检测算法对于欺骗攻击的检测具有明显优势。

图6为欺骗过程中不同时刻Ratio、Delta、ELP、Q-channel和所提检测算法的检测概率结果。从图中可以观察到，在150~250 s，4种传统SQM算法的检测率均产生了波动，但所提检测算法的检测概率始终稳定保持在

100%，并在之后的时间段内也没有出现任何的下降和波动。因此，对于整个欺骗攻击过程，所提检测算法对欺骗攻击的检测速度和检测性能明显优于4种传统SQM算法。

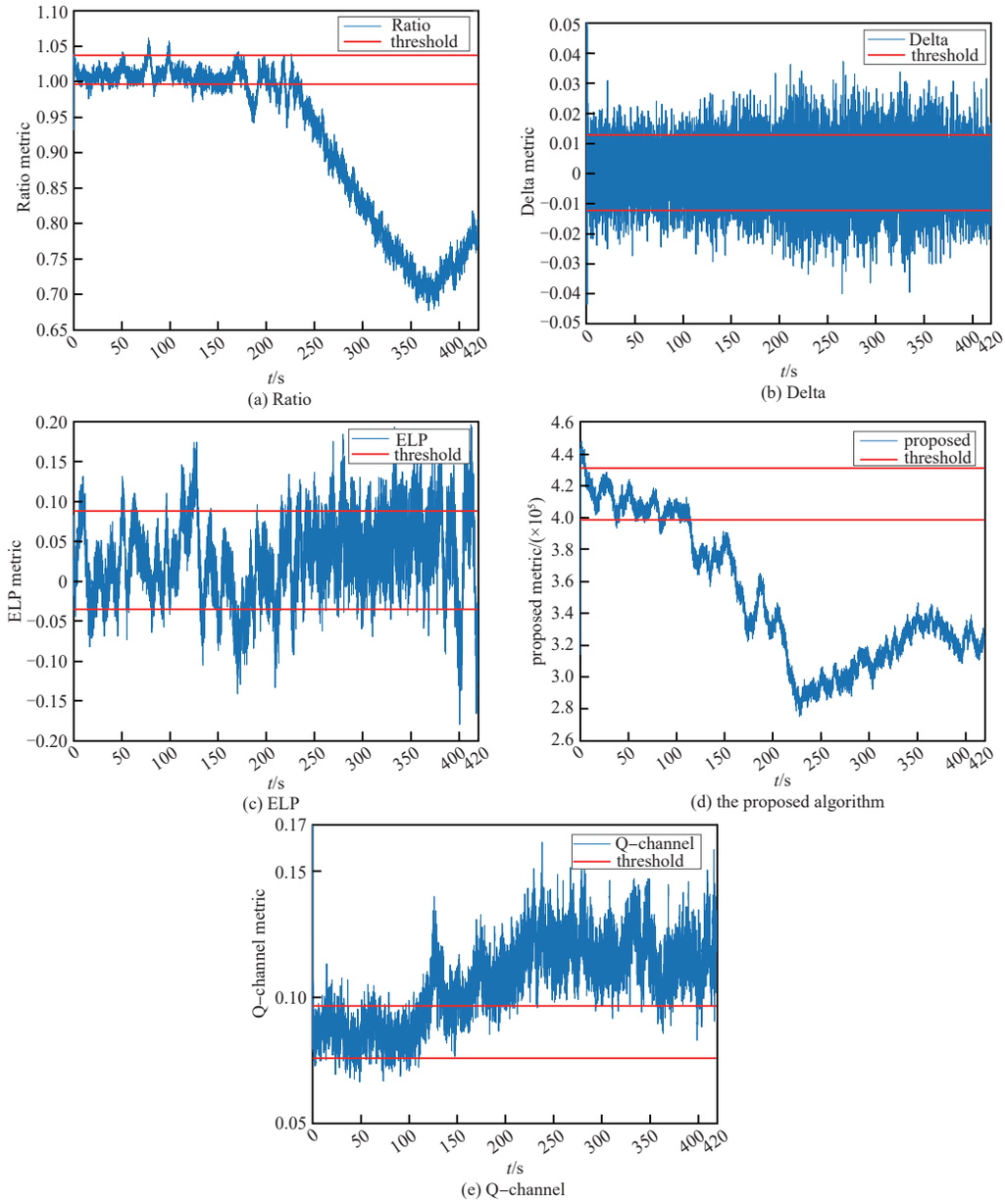

Fig.5 Variation of detection volume of five algorithms
图5 五种算法检测量变化

为综合分析所提算法检测效果，绘制接收机工作特征(Receiver Operating Characteristic，ROC)曲线。图7为5种算法检测概率在不同虚警概率下的变化。从图7中可以看出，当虚警概率为20%时，对于4种传统SQM算法，Q−channel算法的检测概率最高，达到了94%；Ratio算法的检测概率次之，达到80%。相比之下，所提算法的检测概率几乎达到1，远远超出其他2种传统算法的检测概率。在虚警概率相同的条件下，所提算法的检测概率明显高于4种传统SQM算法。

3.2 ds2场景下欺骗检测

利用TEXBAT数据集中第2条欺骗干扰数据进行实验分析和欺骗性能评估。第2条欺骗干扰数据是频率非锁定模式下的大功率优势欺骗干扰场景，欺骗信号与真实信号之间的载波相位偏移总随时间变化。从110~250 s发起欺骗攻击，真实信号与欺骗信号的相对码相位从0 chip到2 chip稳定增大。随着时间的变化，欺骗信号逐渐与真实信号重叠，最终获得对目标接收机跟踪环路的控制。

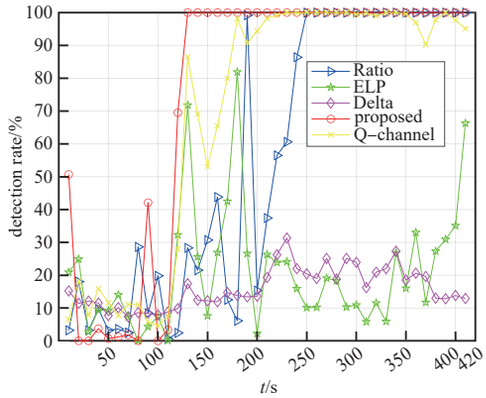

Fig.6 Comparison of detection probability of five algorithms
图6 五种算法检测概率对比

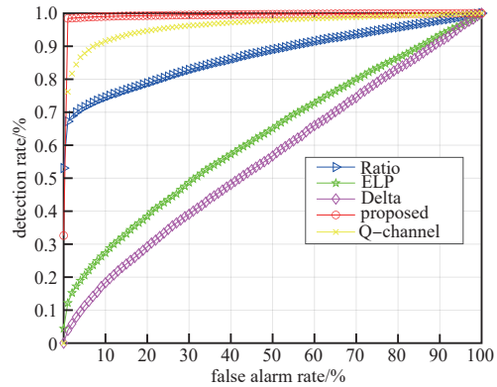

Fig.7 Comparison of ROC curves of five algorithms
图7 五种算法ROC曲线对比

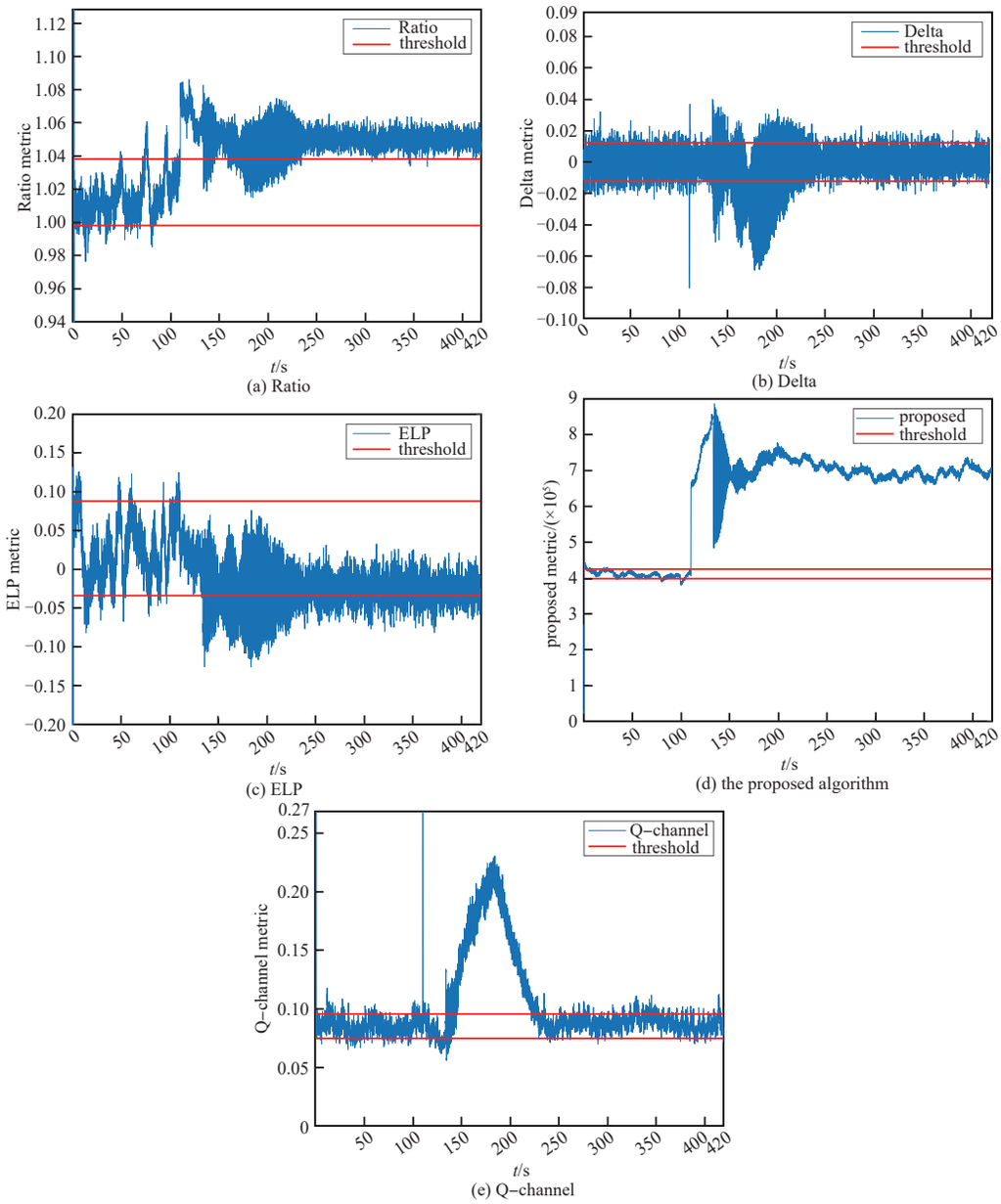

Fig.8 Variation of detection volume of five algorithms
图8 五种算法检测量变化

图 8 为 Ratio、Delta、ELP、Q-channel 和所提检测算法的检测量变化，图中的横线是当虚警概率为 10% 时各检测算法的检测门限。从图 8 可知，Ratio、Delta、ELP、Q-channel 和所提检测算法的检测量均随时间呈现出一定的波动，但所提检测算法的波动性最为明显和剧烈。与其他检测算法相比，所提检测算法的检测量基本都在检测门限之外，说明所提检测算法对于欺骗攻击更灵敏。图 9 为欺骗过程中 Ratio、Delta、ELP、Q-channel 和所提检测算法在不同时刻的检测概率结果。从图中可以看到，从 120 s 开始，所提检测算法的检测概率就已达到 100%，并在之后的时间里始终保持不变，而其他检测算法的检测概率均随时间发生了一定的波动。因此与其他算法相比，所提检测算法具有更好的检测速度和检测性能。图 10 为 Ratio、Delta、ELP、Q-channel 和所提检测算法的 ROC 曲线。从图中可以看出，当虚警概率仅为 0.001 时，所提算法的检测概率就几乎达到 1，且在相同的虚警概率下，所提算法的检测概率显著高于其他检测算法。

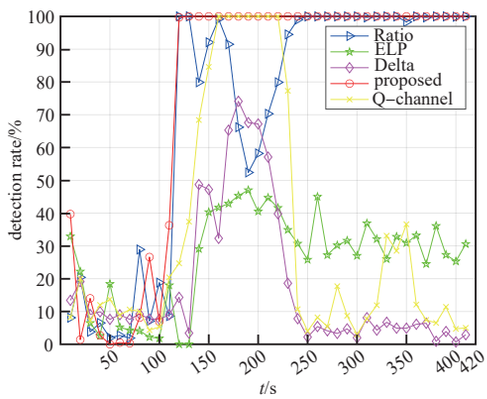

Fig.9 Comparison of detection probability of five algorithms
图 9 五种算法检测概率对比

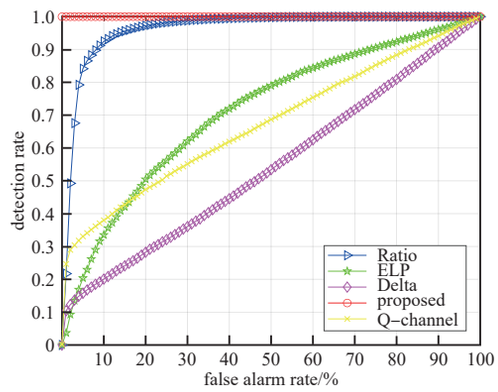

Fig.10 Comparison of ROC curves of five algorithms
图 10 五种算法 ROC 曲线对比

4 结论

针对传统 SQM 算法检测精确度低，检测性能差的问题，本文提出了一种同时利用 I、Q 支路绝对值输出相加求和的新型欺骗检测方法。使用 TEXBAT 数据集评估所提算法性能，结果显示，所提算法能快速识别欺骗攻击，具有更高检测概率、鲁棒性，更好的检测性能。尽管本文所提方法在第 3 章的欺骗场景中取得了较好的效果，但其在应对不同类型的欺骗场景时适用性较为有限，尤其是在欺骗信号功率优势较小时。因此，该方法在面对复杂多样的欺骗场景时，未必能充分发挥其效能，难以满足所有的需求。因此，在今后的研究中将努力关注这方面的应用与研究。

参考文献：

[1] ZHOU Meng,LIU Ying,XIE Lin,et al. Performance analysis of spoofing signal ratio for receiver-spoofer[C]// Proceedings of the 2017 International Technical Meeting of the Institute of Navigation. Monterey,California:ION, 2017:898-911. DOI:10.33012/2017.14956.

[2] BIAN Shaofeng, HU Yanfeng, JI Bing. Research status and prospect of GNSS anti-spoofing technology[J]. Scientia Sinica Informationis, 2017,47(3):275-287. DOI:10.1360/N112016-00073.

[3] QI Weikong,ZHANG Yu,LIU Xiaohui. A GNSS anti-spoofing technology based on Doppler shift in vehicle networking[C]// 2016 International Wireless Communications and Mobile Computing Conference(IWCMC). Paphos,Cyprus:IEEE, 2016:725-729. DOI:10.1109/IWCMC.2016.7577146.

[4] WANG Wenyi, HOU Yinglong. GNSS induced spoofing detection based on dynamic 3-D correlation function[J]. IEEE Transactions on Instrumentation and Measurement, 2024(73):1-18. DOI:10.1109/TIM.2024.3472768.

[5] SCHOENBROD S, NIESTROJ M, BRACHVOGEL M, et al. Ultra tightly coupled position and attitude determination with mitigation of temporally correlated signals using an antenna-array[C]// Proceedings of the 2022 International Technical Meeting of the Institute of Navigation. Long Beach,California:ION, 2022:215-228. DOI:10.33012/2022.18185.

[6] PENG Chenxi,LI Hong,WEN Jian,et al. Research of intermediate spoofing without precise target information[C]// China Satellite Navigation Conference(CSNC) 2019 Proceedings. Singapore:Springer, 2019:615-624. DOI:10.1007/978-981-13-7759-4_54.

[7] JEONG S,SIN C S. GNSS interference signal generation scenario for GNSS interference verification platform[C]// 2015 the 15th International Conference on Control, Automation and Systems(ICCAS). Busan, Korea: IEEE, 2015: 1363-1365. DOI: 10.1109/ICCAS.2015.7364851.

[8] BROUMANDAN A,JAFARNIA J A,DANESHMAND S,et al. Effect of tracking parameters on GNSS receivers vulnerability to spoofing attack[C]// Proceedings of the 29th International Technical Meeting of the Satellite Division of the Institute of Navigation. Oregon:Oregon Convention Center, 2016:3033-3043. DOI:10.33012/2016.14782.

[9] 张欣然,梁涛涛,陈懋霖. 牵引式欺骗对矢量跟踪环路的影响[J]. 太赫兹科学与电子信息学报, 2024,22(5):476-484. (ZHANG Xinran,LIANG Taotao,CHEN Maolin. Influence of traction spoofing on vector tracking loop[J]. Journal of Terahertz Science and Electronic Information Technology, 2025,22(5):476-484.) DOI:10.11805/TKYDA2024006.

[10] HUMPHREYS T E,LEDVINA B M,PSIAKI M L,et al. Assessing the spoofing threat:development of a portable GPS civilian spoofer[C]// Proceedings of the 21st International Technical Meeting of the Satellite Division of the Institute of Navigation. Savannah,GA:ION, 2008:2314-2325.

[11] GAO Yangjun, LYU Zhiwei, ZHANG Lundong. Asynchronous lift-off spoofing on satellite navigation receivers in the signal tracking stage[J]. IEEE Sensors Journal, 2020,20(15):8604-8613. DOI:10.1109/JSEN.2020.2984525.

[12] GAO Yang, LI Hong, LU Mingquan, et al. Intermediate spoofing strategies and countermeasures[J]. Tsinghua Science and Technology, 2013,18(6):599-605. DOI:10.1109/TST.2013.6678905.

[13] MAGIERA J. A multi-antenna scheme for early detection and mitigation of intermediate GNSS spoofing[J]. Sensors, 2019,19(10):2411. DOI:10.3390/s19102411.

[14] SUN C,CHEONG J W,DEMPSTER A,et al. Performance assessment of multi-metric joint detection technique for anti-spoofing[C]// IGNSS Conference 2018. Sydney,Australia:IGNSS, 2018:1-15.

[15] KHAN A M,IQBAL N,KHAN A A,et al. Detection of intermediate spoofing attack on global navigation satellite system receiver through slope based metrics[J]. The Journal of Navigation, 2020,73(5):1052-1068. DOI:10.1017/S0373463320000168.

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

[17] PHELTS R E,WALTER T,ENGE P. Toward real-time SQM for WAAS: improved detection techniques[C]// Proceedings of the 16th International Technical Meeting of the Satellite Division of the Institute of Navigation. Portland, OR, USA: Oregon Convention Center, 2003:2739-2749.

[18] 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. DOI:10.1007/s10291-010-0162-z.

[19] 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. DOI:10.1109/ACCESS.2018.2875948.

[20] SUN C,CHEONG J W,DEMPSTER A G,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. DOI:10.1109/TIM.2021.3102753.

[21] LI Jing, ZHANG Jiantong, CHANG Shoufeng, et al. Performance evaluation of multimodal detection method for GNSS intermediate spoofing[J]. IEEE Access, 2016(4):9459-9468. DOI:10.1109/ACCESS.2016.2587322.

[22] ZHOU Wenlong,LYU Zhiwei,DENG Xu,et al. A new induced GNSS spoofing detection method based on weighted second-order central moment[J]. IEEE Sensors Journal, 2022,22(12):12064-12078. DOI:10.1109/JSEN.2022.3174019.

[23] LI Song,TANG Xiaomei,LIN Honglei,et al. GNSS spoofing detection based on frequency domain processing[J]. Measurement, 2025(242):115872. DOI:10.1016/j.measurement.2024.115872.

[24] OLIVEIRA A, OLIVEIRA T, MACÍAS S, et al. Distribution function for the ratio of two normal random variables[J]. AIP Conference Proceedings, 2015,1648(1):840005.

[25] 赵慎,胡勇,李世玲,等. 绝对同相支路输出的GNSS欺骗检测[J]. 导航定位与授时, 2024,11(2):83-92. (ZHAO Shen,HU Yong, LI Shiling, et al. GNSS spoofing detection based on absolute in-phase branch output[J]. Navigation Positioning and Timing, 2024,11(2):83-92.) DOI:10.19306/j.cnki.2095-8110.2024.02.008.

[26] MANFREDINI E G,DOVIS F,MOTELLA B. Validation of a signal quality monitoring technique over a set of spoofed scenarios[C]// 2014 the 7th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC). Noordwijk,Netherlands:IEEE, 2014:1-7. DOI:10.1109/NAVITEC.2014.7045136.

作者简介：

夏耀祖(2000-)，男，在读硕士研究生，主要研究方向为卫星导航.email:yaozu_xia@163.com.

王文益(1980-)，男，博士，教授，主要研究方向为自适应信号处理、卫星导航、无线电通信.