

基于新型SQM的GNSS欺骗式干扰检测技术

邓 敏, 廖欣璐, 郭莹莹, 姚志强

A novel GNSS spoofing interference detection technology based on SQM

DENG Min, LIAO Xinlu, GUO Yingying, and YAO Zhiqiang

引用本文:

邓敏, 廖欣璐, 郭莹莹, 等. 基于新型SQM的GNSS欺骗式干扰检测技术[J]. 全球定位系统, 2024, 49(4): 56–65. DOI: [10.12265/j.gnss.2024017](https://doi.org/10.12265/j.gnss.2024017)
DENG Min, LIAO Xinlu, GUO Yingying, et al. A novel GNSS spoofing interference detection technology based on SQM[J]. Gnss World of China, 2024, 49(4): 56–65. DOI: [10.12265/j.gnss.2024017](https://doi.org/10.12265/j.gnss.2024017)

在线阅读 View online: <https://doi.org/10.12265/j.gnss.2024017>

您可能感兴趣的其他文章

Articles you may be interested in

基于功率变化的移动终端欺骗干扰检测方法

Detection method of spoofing in mobile terminal based on power variation

全球定位系统. 2020, 45(1): 66–70

基于导航接收机的GNSS弱干扰检测识别技术

The technology of GNSS interference detection and identification based on navigation receiver

全球定位系统. 2022, 47(6): 91–95

基于多通道SQM指标联合的矢量接收机多径干扰检测方法

Multipath interference detection method for vector receivers based on joint multi-channel SQM metrics

全球定位系统. 2023, 48(3): 110–119

信号采集回放仪检测全球导航卫星系统接收机RTK性能

Using signal recording and playback instrument detect the RTK performance of GNSS receiver

全球定位系统. 2024, 49(1): 114–119

无人机GPS欺骗干扰攻击对策

Countermeasure of UAV GPS spoofing jamming attack

全球定位系统. 2023, 48(4): 91–98

基于六旋翼无人机平台的GNSS干扰源测向与定位系统设计与实现

GNSS interference source detection and location technology based on unmanned aerial vehicle

全球定位系统. 2021, 46(5): 79–83



关注微信公众号, 获得更多资讯信息

基于新型 SQM 的 GNSS 欺骗式干扰检测技术

邓敏^{1,2}, 廖欣璐¹, 郭莹莹¹, 姚志强¹

(1. 湘潭大学自动化与电子信息学院 智能可导航与定位湖南省重点实验室, 湖南 湘潭 411105;

2. 湖南国家应用数学中心, 湖南 湘潭 411105)

摘 要: GNSS 在基础设施应用的定位、导航、授时领域具有重要的战略意义。鉴于 GNSS 信号落地功率极低、民码结构透明等特点, 民用卫星信号极易受到干扰和欺骗攻击, 使得 GNSS 在获得广泛应用的同时也受到严重的干扰问题。本文针对传统信号质量监测 (signal quality monitoring, SQM) 检测量检测概率低和可靠性差的问题, 提出一种无需使用跟踪支路载波相位信息的新 SQM 检测量, 将检测数据值进行滑动平均处理, 减少异常波动值造成检测虚警率增高的情况, 并推导了检测量的统计分布特性, 设置在无先验信息下的计算门限与测量门限, 能够避免出现在欺骗与真实导航卫星信号相对载波相位为 π 的整数倍时, 检测失效的情况。在美国德克萨斯大学奥斯汀分校的公共数据库 TEXBAT (texas spoofing test battery) 的实采信号上进行的对比实验结果表明, 所提基于 I、Q 支路能量变化的双重门限 SQM 检测算法在不同实采信号场景下均能够在较短的时间内以较优的准确度检测出欺骗攻击。研究成果对未来抗欺骗通信设备开发具有一定的参考价值, 不仅能够有效提高检测性能, 且无需对接收机硬件结构进行大规模的改变, 进行大规模的改变。

关键词: 全球导航卫星系统 (GNSS); 干扰检测; 欺骗攻击; SQM 检测量; 测量门限

中图分类号: P228; TN972.3

文献标志码: A

文章编号: 1008-9268(2024)04-0056-10

0 引 言

GNSS 为电力系统、金融系统、通信系统及交通系统等领域提供了全天候、高精度、高效率的位置、速度和时间 (position, velocity and time, PVT) 信息服务, 满足了人们生产生活的需求^[1]。

卫星位于距地球表面约 20 000~36 000 km 的高空轨道上, 地球表面的接收机接收到的发射信号功率经空间传播和大气吸收后降低幅度明显, 典型功率值仅有 -160~-130 dBm, 这种微弱的信号容易受到欺骗干扰的影响。近年来国内外学者从不同方面对依据接收机的卫星欺骗干扰检测进行研究, 可大致分为三类: 基于导航数据信息的欺骗检测技术、基于信号特征的欺骗检测技术和机器学习检测技术, 其中基于信号特征的欺骗检测技术因其简单高效性得到普遍运用。

为欺骗目标接收机, 攻击者需要使用相应的通信设备和技术将发射的欺骗信号伪装成真实信号, 为目标接收机认为自己在另一个非实际的位置, 如图 1 所示, 欺骗信号与真实信号需相似但一定有差异之处, 这种差异与真实信号和欺骗信号之间的相互作用都可作为信号特征进行欺骗检测, 进而抑制或消除欺骗信号^[2]。一般的信号特征差异有信号功率、信号质量、多普勒一致性、空间处理等^[3-5]。

欺骗信号功率的大小需要在真实信号功率和无法解码信号功率之间找到一个平衡点, 以确保攻击的成功率。载噪比成为检测欺骗攻击的重要参数之一^[6], 接收机跟踪锁定到欺骗信号时会造成噪声基底的上升, 可涌现出一些进一步提高在功率匹配的欺骗干扰下的检测性能研究。文献^[7]针对利用导航接收机的输出信息, 提出了联合接收机输出的自动增益控制 (automatic gain control, AGC)、载噪比及位置信息,

收稿日期: 2024-01-30

资助项目: 湖南创新型省份建设专项经费资助 (2023GK1040); 湖南省教育厅项目 (22C0055); 国家自然科学基金青年项目 (62103348)

通信作者: 姚志强 E-mail: yaozhiqiang@xtu.edu.cn

实现了卫星导航弱压制干扰和欺骗干扰的检测与识别.然而,该类方法易受异常观测值或噪声波动影响.

信号质量检测技术是监测真实导航卫星信号与欺骗干扰信号之间的相互作用导致相关峰形变这一特征来检测欺骗攻击.欺骗干扰信号成功牵入跟踪环路的过程中,会造成相关峰的异常尖锐、平坦或不对称^[8].现有研究已根据不同时期相关器的输出值,设计了各种信号质量监测(signal quality monitoring, SQM)指标,常见的为 Delta 度量、Ratio 度量、早码、晚码和即时码(early late phase, ELP)度量^[9].SQM 使用的检测值只需知道早期相关器、即时相关器和晚期相关器的输出就可计算得到,不需要其他的外部依赖.通过设定适当的阈值来检测欺骗攻击是有效的.由于其简单性、高度适应性和鲁棒性, SQM 在多径检测和欺骗检测方面表现卓越.传统的 SQM 指标(如 Delta 指标、Ratio 指标)使用跟踪环路中单一同相支路相关器的输出来判定接收机是否受到了欺骗,但因真实信号和欺骗信号的相关作用造成载波相位波动,引起 SQM 检测量出现剧烈波动,整体欺骗干扰检测精度和鲁棒性下降,因此一些学者对传统的 SQM 指标提出了改进.

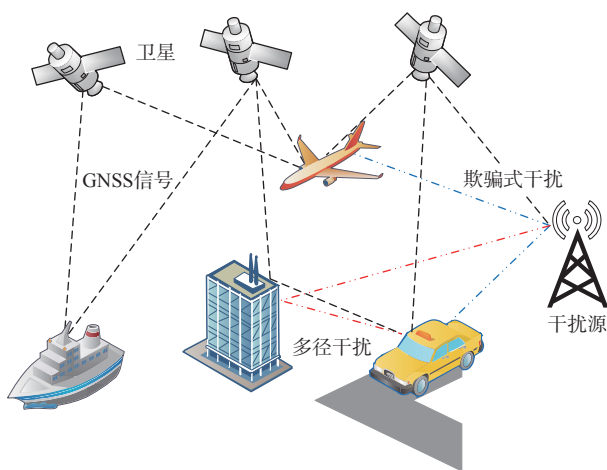


图1 导航欺骗干扰原理示意图

文献[10]提出了在伽利略接收机上使用多个不同基于码域的 SQM 指标进行检测失真的相关峰值并计算适当的检测阈值,但该阈值会随着检测环境的变化而改变造成检测鲁棒性低.文献[11]通过多个相关器采用标量跟踪结构来测量相关峰重叠时的自相关函数失真,但相关峰在无重叠情况下无法实现干扰检测.为解决这一问题,文献[12]提出了一种矢量跟踪结构对接收信号进行联合跟踪的方法.文献[13]提出信号检测器用于检测 GNSS 信号潜在的危险,提出两种新方法增强现有的 SQM 方法,即参考站投票

和度量差分过程.文献[14]提出一种基于支持向量机(support vector machine, SVM)的 GNSS 多参数联合检测方法,与仅选择 SQM 参数的方法相比,欺骗检测性能有显著提高.文献[15]提出引入一种新的自相关函数(auto-correlation function, ACF)相似度指标,用于表征基于图像特征提取技术的跟踪环路中的 ACF 失真和功率异常.所提检测器在 TEXBAT (texas spoofing test battery) 数据集中的检测概率为 87%,检测灵敏度优于传统的 SQM 指标.文献[16]将 SQM 技术与失真功率检测相结合,但功率检测模块增加了检测的复杂性.文献[17]利用正交信道能量建立新型检测指标,对欺骗和多径场景具有更高的检测灵敏度和鲁棒性.文献[18]提出了一种新型相关峰畸变检测方法,旨在通过测量提前、滞后和即时相关器之间的差异来实现检测.文献[19]从多径对矢量接收机的影响机理出发,提出一种联合多通道 SQM 指标的矢量接收机多径检测方法.所提方法能够有效地检测与直达信号幅度比小于 0.5、相对码延时在 0.3~0.6 码片的多径干扰.文献[20]提出了一种基于牛顿迭代法的参数估计方法.该方法采用牛顿迭代法对信号码相位进行估计,在此基础上采用最小二乘法对信号幅度和载波相位进行估计.

不管是传统的相关峰对称性检测方法、Ratio 方法或者相关峰斜率方法,新型相关峰畸变检测方法与之相比都具有优良性,无先验信息条件具有更大的检测范围,并且不需要引入除法,不会因小的噪声抖动产生误差,同时也不需要加入额外的相关器.对于信号特征的欺骗检测研究较多,Phelt 提出 Delta 检测量和 Ratio 检测量,Delta 检测量是一种对称度量,基于提前同相支路减去滞后同相支路的幅值或者绝对值之差来检测非对称相关峰;Ratio 则是基于提前同相支路和滞后同相支路相对于即时同相支路的输出比值是否超出只存在真实信号情况下的阈值来检测形状畸变.ELP 检测量则是利用 Delta 检测量和 Ratio 检测量未使用到的相位信息进行检测,根据只存在真实信号情况下提前支路载波相位和滞后支路载波相位相等这一特点来检测欺骗攻击,但当一些欺骗信号与真实导航卫星信号的相对载波相位为 π 的整数倍时,此方法不再具有有效性.传统算法并没有实现低复杂度、高检测率的特性,且缺乏复杂环境适应性.为此,本文提出一种新型 SQM 检测量,将检测数据值进行滑动平均处理,减少异常波动值对检测虚警率的影响,并推导了检测量的统计分布特性,设置在无先验信息下的计算门限与测量门限,实现低成本、高

准确度的欺骗检测. 本文所提算法主要针对接收机码相位和载波相位估计准确的场景, 适用于频率锁定或解锁的场景, 不受欺骗信号与真实导航信号相对载波相位差不能为 π 的整数倍的限制.

1 GNSS 欺骗检测模型

天线接收到的中频信号经 I/Q 解调后, 再与本地复制的 C/A 码进行相关运算, 得到跟踪通道同相 I 和正交 Q 支路相关器的输出值. 接收的 GNSS 中频信号可表示为:

$$r(nT_s) = \sum_{l=1}^M (S_l^A(nT_s) + S_l^S(nT_s)) + \eta(nT_s) \quad (1)$$

式中: n 为采样序列号; T_s 为中频信号采样周期; 下标 l 为卫星的伪随机码编号; M 为收到的真实导航卫星信号数量; $S_l^A(\cdot)$ 为真实导航卫星信号; $S_l^S(\cdot)$ 为欺骗干扰装置发射的欺骗信号; 上标 A 和 S 分别为真实导航卫星信号和欺骗信号; $\eta(nT_s)$ 为带限加性高斯白噪声.

欺骗信号与真实导航卫星信号的数量相等, 伪随机噪声码一一对应, 具有相同的信号结构, 第 l 个信道信号模型可以表示为:

$$S_l^{A/S}(nT_s) = \alpha^{A/S} P_l C_l^{A/S}(nT_s - \tau_l^{A/S}) D_l^{A/S}(nT_s - \tau_l^{A/S}) \sin(2\pi(f_{IF} + f_l^{A/S})nT_s + \phi_l^{A/S}) \quad (2)$$

式中: 真实信号的相对振幅为 $\alpha^A = 1$, 欺骗信号的相对振幅 $\alpha^S > 1$; P_l 为天线接收到的信道 l 的接收功率; $C_l(\cdot)$ 、 $D_l(\cdot)$ 分别为伪随机扩频码和导航数据比特; f_{IF} 为中心频率; f_l 为多普勒频率; τ_l 为码传播时延 (码相位); ϕ_l 为初始载波相位.

天线接收到的中频信号经 I/Q 解调后, I、Q 支路分别与本地复制的 C/A 码进行数字相关得到相关结果, 相关结果经过一定时间的相干积分处理后, I、Q 支路的相干积分值 $I(n)$ 和 $Q(n)$ 可以表示为:

$$\begin{aligned} I(n) &= PD^A(n)R(\tau^A) \sin c(f_e^A T_{\text{coh}}) \cos \phi_e^A \\ &\quad + \alpha^S PD^S(n)R(\tau^S) \sin c(f_e^S T_{\text{coh}}) \cos \phi_e^S + \eta_I \\ Q(n) &= PD^A(n)R(\tau^A) \sin c(f_e^A T_{\text{coh}}) \sin \phi_e^A \\ &\quad + \alpha^S PD^S(n)R(\tau^S) \sin c(f_e^S T_{\text{coh}}) \sin \phi_e^S + \eta_Q \end{aligned} \quad (3)$$

式中: P 代表真实信号的幅值; τ^A 、 τ^S 为即时复制 C/A 码与真实信号和欺骗信号码相位之间的相位差异, $\tau^{A/S} = dT_s$, 其中 d 为早期或者晚期相关器与即时相关器的间隔, 对于一般接收机来说, 相关器间距 d 的范围在 0.1~0.5 码片, 所有实验的相关器间隔统一定义为 0.5 码片; f_e^A 与 f_e^S 分别表示本地接收 C/A 码和真实导航卫星信号及本地接收 C/A 码和欺骗信号

的多普勒差; ϕ_e^A 与 ϕ_e^S 分别表示本地接收 C/A 码和真实导航卫星信号及本地接收 C/A 码和欺骗信号的载波相位差; T_{coh} 为相干积分时间; η_I 和 η_Q 为 I 支路和 Q 支路的高斯噪声; $\sin c(x) = [\sin(\pi x)]/\pi x$; $R(\cdot)$ 为 C/A 码自相关函数, 其最大值为 1. 以 GPS L1 信号的 C/A 码为例, 可表示为:

$$R(\tau^{A/S}) = \begin{cases} 1 - |\tau^{A/S}|, & |\tau^{A/S}| \leq 1 \\ 0, & |\tau^{A/S}| > 1 \end{cases} \quad (4)$$

2 提出的欺骗检测算法

SQM 是不同跟踪相关器和监控相关器的组合, 根据信号相关函数输出是否发生畸变来判定接收机是否受到欺骗干扰. 而当一些欺骗信号与真实导航卫星信号的相对载波相位为 π 的整数倍时, ELP 检测方法不再具有检测有效性, 因此为了提高检测准确性和鲁棒性, 本节设计一种新的检测指标.

只存在真实信号时, 同相 I 支路包含能量和一些噪声, 而正交 Q 支路基本上仅是噪声而已; 当欺骗信号存在时, 真实信号与欺骗信号之间的载波相位差导致正交 Q 支路出现一点能量变化. 欺骗信号功率大于真实信号时, 会让目标接收机优先捕获跟踪到, 同时欺骗装置发射天线相对于接收机的运动也会造成接收信号噪声基底上升, 因此我们可以根据欺骗前后 I、Q 支路能量变化建立一个新型 SQM 检测量 M_{value} , 表达式为:

$$M_{\text{value}}(n) = \left| \frac{I_{Ed}(n) \times Q_{Ed}(n) + I_{Ld}(n) \times Q_{Ld}(n)}{I_p(n)} \right| \quad (5)$$

式中: $I_{Ed}(n)$ 、 $I_p(n)$ 和 $I_{Ld}(n)$ 分别为第 n 个相干积分内同相通道的早期、即时和晚期相关器输出; $Q_{Ed}(n)$ 和 $Q_{Ld}(n)$ 分别为第 n 个相干积分内正交通道的早期和晚期相关器输出.

接收机捕获跟踪到欺骗信号后, 跟踪环路输出相关峰的幅度变化和形变都会影响检测的灵敏度, 且幅度变化越大、畸变越明显, 越易检测到欺骗干扰. 新型 SQM 检测量 M_{value} 没有使用跟踪支路载波相位信息, 可以避免出现 ELP 检测量在相对载波相位为 π 的整数倍时检测失效的情况.

接下来, 对 M_{value} 数据值进行滑动平均处理, 减少异常波动值出现造成检测虚警率增高的情况, 有助于提高所提新型 SQM 检测量 M_{value} 的性能. 首先在所有的 M_{value} 数据值选取一段窗口长度为 L 的子集并计算均值, 然后以固定的滑动间隔 L 前移选取新的子集并计算均值, 重复进行直至滑动窗口到达数据集末

端. 总滑动次数为数据集总长度与窗口长度的比值, 其中第 k 个滑动窗口的新型 SQM 检测量均值可以表示为:

$$M_{\text{value-avg}}(k) = \frac{1}{L} \sum_{i=(k-1)*L+1}^{i=(k-1)*L+L} M_{\text{value}}(i) \quad (6)$$

式中, $M_{\text{value}}(i)$ 为 M_{value} 数据集中第 i 个样本的值.

跟踪通道不同时延的相关器输出均服从高斯分布, 其均值不同但方差相同. 只存在真实信号的情况下, 根据信号检测与估计的相关理论对新型 SQM 检测量 M_{value} 进行推导, 确立其概率分布.

不失一般性, 只存在真实卫星信号时, I、Q 支路的相干积分结果可表示为:

$$\begin{aligned} I(n) &= PR(dT_s) \sin c(f_e^A T_{\text{coh}}) \cos \phi_e^A + \eta_I \\ Q(n) &= PR(dT_s) \sin c(f_e^A T_{\text{coh}}) \sin \phi_e^A + \eta_Q \end{aligned} \quad (7)$$

假设残余多普勒频移误差可以忽略不计, η_I 和 η_Q 不相关, 此时 $I(n)$ 和 $Q(n)$ 服从正态分布. 在没有欺骗的情况 $I(n)$ 和 $Q(n)$ 的理论统计如下:

$$\begin{cases} \mu_{I(n)} = PR(dT_s) \sin c(f_e^A T_{\text{coh}}) \cos \phi_e^A \\ \mu_{Q(n)} = PR(dT_s) \sin c(f_e^A T_{\text{coh}}) \sin \phi_e^A \\ \sigma_{I(n)}^2 = \sigma_{Q(n)}^2 = \sigma_0^2 \\ \sigma_{I(n)Q(n)}^2 = 0 \end{cases} \quad (8)$$

式中: $\mu_{I(n)}$ 和 $\mu_{Q(n)}$ 分别为跟踪通道 I、Q 支路相关器输出均值; $\sigma_{I(n)}^2$ 和 $\sigma_{Q(n)}^2$ 分别为跟踪通道 I、Q 支路相关器输出方差, 假设 $\sigma_{I(n)Q(n)}^2 = 0$.

将 M_{value} 看作不同 x/y 之间乘积的绝对值, 表示为:

$$\begin{aligned} M_{\text{value}} &= \left| \frac{I_{Ed} \times Q_{Ed} + I_{Ld} \times Q_{Ld}}{I_P} \right| = \left| \frac{I_{Ed}}{I_P} \times \frac{Q_{Ed}}{I_P} + \frac{I_{Ld}}{I_P} \times \frac{Q_{Ld}}{I_P} \right| \\ &= \left| \frac{x_1}{y} \times \frac{x_2}{y} + \frac{x_3}{y} \times \frac{x_4}{y} \right| = |z_1 \times z_2 + z_3 \times z_4| \end{aligned} \quad (9)$$

经式 (9) 得知早期、即时、晚期的同相正交相关器输出值的理论分布, 上式展开可得:

$$\begin{cases} x_1 = I_{Ed}, x_2 = Q_{Ed}, x_3 = I_{Ld}, x_4 = Q_{Ld}, y = I_P \\ \mu_{x_1} = \mu_{x_3} = PR(dT_s) \sin c(f_e^A T_{\text{coh}}) \cos \phi_e^A = PR(dT_s) \\ \mu_{x_2} = \mu_{x_4} = PR(dT_s) \sin c(f_e^A T_{\text{coh}}) \sin \phi_e^A = 0 \\ \mu_y = R(0) \\ \sigma_{x_1}^2 = \sigma_{x_2}^2 = \sigma_{x_3}^2 = \sigma_{x_4}^2 = \sigma_y^2 = \sigma_0^2 \\ \sigma_{x_1 y} = \sigma_{x_3 y} = \text{Cov}[I_{Ed}, I_P] = \text{Cov}[I_{Ld}, I_P] \\ \quad = E\{(I_{Ed} - E(I_{Ed})) \cdot I_P\} = \sigma_0^2 R(dT_s) \\ \sigma_{x_2 y} = \sigma_{x_4 y} = \text{Cov}[Q_{Ed}, I_P] = \text{Cov}[Q_{Ld}, I_P] \\ \quad = E\{(Q_{Ed} - E(Q_{Ed})) \cdot I_P\} = 0 \end{cases} \quad (10)$$

已知 $f(x, y) = x/y$ 泰勒展开后的方差为 $\sigma_{f(x, y)}^2 = \frac{1}{\mu_y^2} \sigma_x^2 + \frac{\mu_x^2}{\mu_y^4} \sigma_y^2 - 2 \frac{\mu_x}{\mu_y^3} \sigma_{x, y}$, 将 $z_1 = \frac{x_1}{y}$ 、 $z_2 = \frac{x_2}{y}$ 、 $z_3 = \frac{x_3}{y}$ 和

$z_4 = \frac{x_4}{y}$ 代入后可得到对应的均值和方差, 可表示为:

$$\begin{cases} E[z_1] = E[z_3] = \frac{\mu_{x_1}}{\mu_y} = \frac{\mu_{x_3}}{\mu_y} \approx \frac{1}{2} \\ \text{Var}[z_1] = \text{Var}[z_3] = \frac{\sigma_{x_1}^2}{R^2(0)} + \frac{\mu_{x_1}^2}{R^4(0)} \sigma_y^2 \\ \quad - 2 \frac{\mu_{x_1}}{R^3(0)} \sigma_{x_1 y} = \frac{3}{4} \sigma_0^2 \\ E[z_2] = E[z_4] = \frac{\mu_{x_2}}{\mu_y} = \frac{\mu_{x_4}}{\mu_y} = 0 \\ \text{Var}[z_2] = \text{Var}[z_4] = \frac{\sigma_{x_2}^2}{R^2(0)} + \\ \quad \frac{\mu_{x_2}^2}{R^4(0)} \sigma_y^2 - 2 \frac{\mu_{x_2}}{R^3(0)} \sigma_{x_2 y} = \sigma_0^2 \end{cases} \quad (11)$$

经推导 z_1 和 z_3 服从同均值方差的高斯分布, z_2 和 z_4 服从同均值方差的高斯分布, 当两个独立的高斯分布相乘时依旧为一个高斯分布, 即 $z_1 \times z_2$ 和 $z_3 \times z_4$ 各自服从相同均值相同方差的高斯分布, 两个独立的高斯分布相加时仍为一个高斯分布, 即 $z_1 \times z_2 + z_3 \times z_4$ 为正态分布, 可表示为:

$$\begin{cases} E[z_1 \times z_2 + z_3 \times z_4] = \frac{4}{7} \\ \text{Var}[z_1 \times z_2 + z_3 \times z_4] = \frac{6}{7} \sigma_0^2 \end{cases} \quad (12)$$

综上所述, $r_1 \times r_2 + r_3 \times r_4 \sim N(\mu_m, \sigma_m^2)$, 其中 $\mu_m = 4/7$ $\sigma_m^2 = 6\sigma_0^2/7$, 已知 $z_1 \times z_2 + z_3 \times z_4$ 的均值和方差可利用概率密度函数推导得出 $|z_1 \times z_2 + z_3 \times z_4|$ 的均值和方差, 得知 M_{value} 为一个高斯分布变量, 可表示为:

$$\begin{aligned} E[|z_1 \times z_2 + z_3 \times z_4|] &= E[|t|] \\ &= \int_{-\infty}^{+\infty} |t| f(t) dt = M_{\text{value-mean}} \\ D[|z_1 \times z_2 + z_3 \times z_4|] &= D[|t|] \\ &= \int_{-\infty}^{+\infty} (|t| - \mu_m)^2 f(t) dt = M_{\text{value-var}} \end{aligned} \quad (13)$$

此时 $M_{\text{value}} \sim N(M_{\text{value-mean}}, M_{\text{value-var}})$, 为高斯分布.

为了验证上述推导的新型 SQM 检测量 M_{value} 统计特性的正确性, 我们进一步运行了模拟试验, 并在没有欺骗的情况下绘制了新型 SQM 检测量 M_{value} 的直方图. 图 2 显示了在没有欺骗的情况下, 推导出的理论概率密度函数 (probability density function, PDF) 曲线与直方图之间的比较. 我们可以看到, 新型 SQM 检测量 M_{value} 的理论 PDF 曲线与仿真结果吻合较好,

这表明上述推导的统计特性是可靠的。

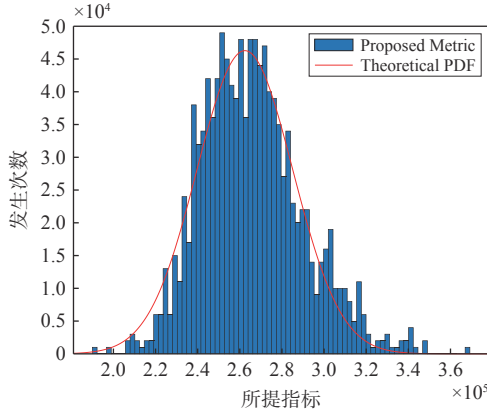


图 2 新型 SQM 检测量 M_{value} 的直方图与理论 PDF 曲线

3 检测门限及概率分析

欺骗信号的检测性能是衡量检测算法有效性的关键因素之一。为了解决欺骗信号检测问题,采用二元信号检测方法可以将欺骗攻击真实性分析验证问题转化为统计学中的假设检验问题,此时欺骗攻击的分析验证可以转化为有欺骗干扰和无欺骗干扰这两种情况,分别用 H_0 和 H_1 表示。此外,二元信号检测方法还可采用最大后验概率估计和贝叶斯决策理论等方法对欺骗信号进行检测。该二元信号检测函数可表示为:

$$\phi = \begin{cases} 0 \sim H_0, & \text{无欺骗干扰} \\ 1 \sim H_1, & \text{有欺骗干扰} \end{cases} \quad (14)$$

在评估欺骗干扰检测效果时,虚警概率 P_f 和检测概率 P_d 是两个重要的检测指标。虚警概率 P_f 反映了检测算法的可靠性和实用性,即在真实情况下错误地判断存在欺骗干扰的概率。检测概率 P_d 则反映了检测算法的灵敏度,也称为检测率,是指在存在欺骗干扰的情况下正确地判断干扰存在的概率。对于欺骗干扰检测算法来说,一个较低的虚警概率 P_f 和一个较高的检测概率 P_d 是理想的检测效果。因此,这两个指标的调整和平衡是关键,可以通过优化算法和选择合适的阈值来实现。上文中我们已经分析了新型 SQM 检测量 M_{value} 的统计特征,假设虚警概率为 $P_{\text{fa-cal}}$,是新型 SQM 检测量 M_{value} 大于检测门限的概率,可由以下公式得到:

$$P_{\text{fa-cal}} = \int_0^{\text{Threshold}_{\text{cal}}} f_M(x) dx = \text{erfc} \left(\frac{M_{\text{value-mean}} - \text{Threshold}_{\text{cal}}}{\sqrt{2M_{\text{value-var}}}} \right) \quad (15)$$

式中: $f_M(x)$ 为不存在欺骗攻击时新型 SQM 检测量 M_{value} 的概率密度函数; $\text{erfc}(\cdot)$ 为互补误差函数。根据上式可以得到计算阈值 $\text{Threshold}_{\text{cal}}$ 的表达式为:

$$\text{Threshold}_{\text{cal}} = M_{\text{value-mean}} + \sqrt{2M_{\text{value-var}}} \text{erfc}^{-1}(2P_{\text{fa-cal}}) \quad (16)$$

上述计算门限 $\text{Threshold}_{\text{cal}}$ 是根据新型 SQM 检测量 M_{value} 的统计分布特征值得到的,为理论门限。在实际应用中可根据当前真实 GNSS 数据得到其真实门限值,也为测量门限值 $\text{Threshold}_{\text{mea}}$ 。

测量门限 $\text{Threshold}_{\text{mea}}$ 可以根据非欺骗干扰情况下的可用数据集数据来确定,对真实 GNSS 数据计算得出的新型检测度量值 M_{value} 进行升序排列为:

$$M_{\text{value}}(1) \leq M_{\text{value}}(2) \leq \dots M_{\text{value}}(n) \leq \dots M_{\text{value}}(N_m - 1) \leq M_{\text{value}}(N_m) \quad (17)$$

式中, N_m 为真实信号数据集长度。

$P_{\text{fa-meas}}$ 通常用于评估系统在无信号干扰的情况下的错误率。在设定检测需满足的最高虚警概率 $P_{\text{fa-meas}}$ 下, $P_{\text{fa-meas}}$ 满足:

$$P_{\text{fa-meas}} = \frac{\text{count}(M_{\text{value}}(n) > \text{Threshold}_{\text{mea}})}{N_m} \times 100\% \quad (18)$$

式中: $M_{\text{value}}(n)$ 为真实信号 M_{value} 数据集第 n 个样本值; $\text{count}(M_{\text{value}}(n) > \text{Threshold}_{\text{mea}})$ 为检测量 M_{value} 大于测量门限值 $\text{Threshold}_{\text{mea}}$ 的计数总值。根据上式可以得到测量阈值 $\text{Threshold}_{\text{mea}}$ 的表达式为:

$$\text{Threshold}_{\text{mea}} = M_{\text{value}}([N_m \times (1 - P_{\text{fa-meas}})]) \quad (19)$$

其中, $[\cdot]$ 为取整函数。

相较于用单一理论门限进行欺骗检测,本文基于 I、Q 支路能量变化的双重门限 SQM 检测算法,取实际测量阈值和理论计算阈值的最大值,使用理论门限和实际测量门限更具实用性和鲁棒性。

欺骗干扰的时变特性使得我们无法具体得知新型 SQM 检测量 M_{value} 的分布特征,意味着无法通过解析表达式概率密度函数的方法计算检测概率 P_d 。可以根据统计论中的检测概率 $\hat{P}_d$ 来代替检测概率 P_d 的方法, $\hat{P}_d$ 的表达式为:

$$\hat{P}_d = \frac{\text{num}(M_{\text{value-avg}}(k) > (\text{Threshold}_{\text{cal}} \parallel \text{Threshold}_{\text{mea}}))}{N} \quad (20)$$

式中: $M_{\text{value-avg}}(k)$ 为移动平滑处理后的新型 SQM 检测量 M_{value} 输出值; $\text{num}(\cdot)$ 为满足条件的数目; N 为干扰样本总量。

4 实验结果及分析

本节在美国德克萨斯大学奥斯汀分校无线电导航实验室的 GPS 信号数据库 TEXBAT^[21] 上开展欺骗检测实验. 对比的检测方法是检测混合异常信号和卫星信号所导致的 C/A 码互相关函数的失真. 由于 DS1 场景属于特定条件下的“静态开关”攻击, 不会产生明显的波形畸变, 不易检测到, 在此不进行讨论. DS7 和 DS8 数据集属于渐进式导航欺骗干扰, 该类数据集采用功率匹配和载波对齐的方法高度隐蔽地将欺骗信号成功牵入接收机跟踪环路. DS8 数据集采用零延迟安全伪码的估计和重放方法, 可以非常准确地估计接收机数据位. 我们将分析重点放在 DS2~DS6 数据集上, 其说明如表 1 所示.

表 1 数据集场景说明

场景	功率优势/dB	频率锁定	起飞时间/s
静态开关	-	不锁定	-
静态超负荷时间推移	10.0	不锁定	133
静态匹配功率时间推移	1.3	锁定	195
静态匹配动力推移	0.4	锁定	225
动态超负荷时间推移	9.9	不锁定	199
动态匹配动力推移	0.8	锁定	199

本组实验使用 DS2~DS6 数据集进行分析, 即对接收机码相位和载波相位估计精确的场景. 欺骗攻击从 110 s 开始, 并始终保持和真实信号的导航数据位的同步, 随着不断的改变载波相位和信号的幅度, 将接收机跟踪环路牵引至欺骗信号.

表 1 可以看出场景 2 和场景 5 都用于频率解锁模式, 场景 3 和场景 6 都用于频率锁定模式. 场景 2 和场景 5 之间或场景 3 和场景 6 之间的主要区别在于平台的可移动性. 原则上, 平台移动性只是最小限度地改变欺骗信号和真实信号之间的相对相位和频率关系, 因此所提出的方法在场景 5 和场景 6 上的性能分别接近于场景 2 和场景 3. 为了简洁起见, 我们使用场景 2 和场景 3 集中进行性能评估.

在场景 2 中, 一个频率解锁的欺骗攻击从 110~250 s 被启动. 欺骗信号和真实信号之间的载波相位偏移总是随时间而变化. 在交互阶段之后, 目标 GNSS 接收机的跟踪环路最终锁定了欺骗信号. 新型 SQM 检测量 M_{value} 对频率解锁的欺骗攻击的时域瞬态响应如图 3 所示. 真实信号和欺骗信号之间的相互作用导致 M_{value} 振幅的增加, 反映出异常信号在 110~250 s 波动. 对于 110 s 之前和 250 s 之后的时间段,

最终的检测量 M_{value} 保持稳定, 这是因为真实信号或欺骗信号都被跟踪环路锁定. 此外, 我们还可以看到, 当新型 SQM 检测量 M_{value} 值滑动间隔平均为 4 s 时, 瞬态响应变得更平滑, 这代表了更稳定和更突出的欺骗检测.

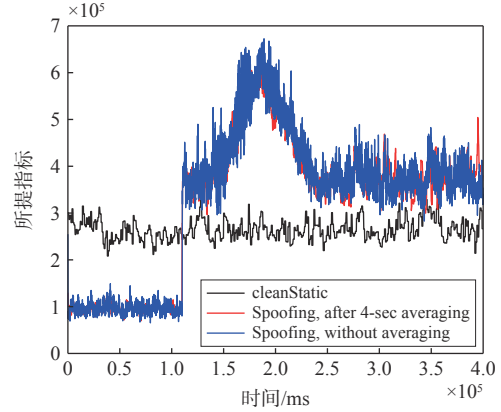


图 3 场景 2 中所提 SQM 检测量 M_{value} 时域瞬态响应

以跟踪的 23 号卫星为例, 检测窗口长度为 400 ms, 测试时间为前 400 s. 图 4 为在场景 2 中传统 SQM 检测量 Ratio、ELP 和 MSQM 检测量^[17] 以及本文所提检测指标随时间的变化关系和检测门限值, 本文检测门限值为虚警概率为 0.1% 时对应的实际测量阈值和理论计算阈值的最大值. 根据二元检测, 可将大于门限的时刻认定为该时刻检测到了欺骗信号. 由图可知, Ratio 在 140 s 之后才检测到了欺骗, 但实际上场景 2 中约 110 s 就已经开始注入欺骗, 欺骗信号改变码相位并不断靠近, 导致接收机的检测输出值出现跳变, 可见 Ratio 检测量检测性能低且检测漏警率高. ELP 检测量在欺骗未注入时就已检测到了欺骗, 虚警率高, 检测鲁棒性低, 而 MSQM 在 250 s 之后欺骗信号与真实信号完全分离, 并未检测到欺骗, 不具有稳

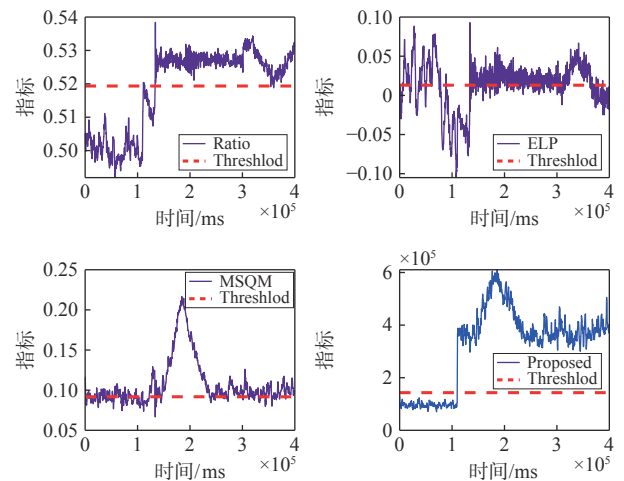


图 4 场景 2 中的各检测量时域瞬态响应

定的检测性能。

此外本文评估了所提出的方法在锁频场景下的性能,即 TEXBAT 场景 3, 场景 2 和场景 3 之间的比较有助于我们分析相对载波相位对检测性能的影响。图 5 为在场景 3 中相同设置下传统 SQM 检测量 Ratio、ELP 和对比文献检测量 MSQM 以及本文所提出的检测指标随时间的变化关系和检测门限值,可见存在载波相位漂移时,Ratio 检测量和 ELP 检测量只能检测到一部分的欺骗干扰,MSQM 检测量虽能检测到大部分的欺骗干扰,但同样在 140 s 左右才检测到了欺骗注入,检测漏警率高。

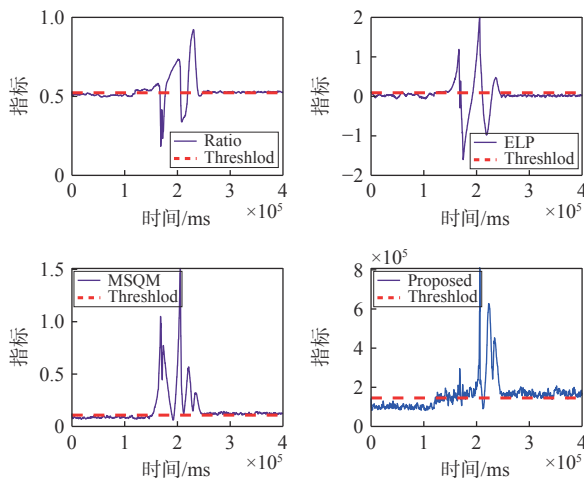
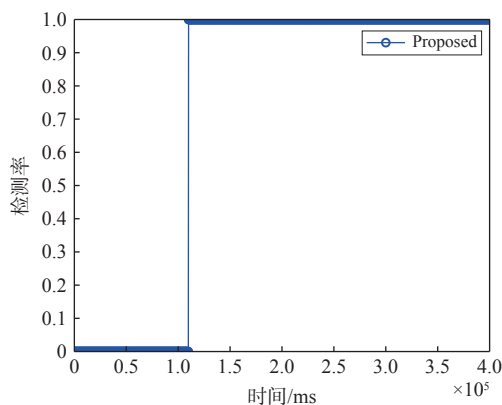
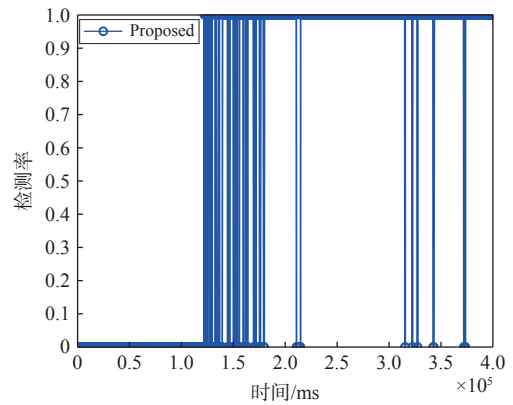


图 5 场景 3 中的新型 SQM 检测量 M_{value} 时域瞬态响应

图 6 为欺骗检测结果判决图,如图 6(a) 所示,在场景 2 下,本文所提出的检测指标在欺骗信号注入到跟踪环路锁定欺骗信号的阶段皆可检测到欺骗;在场景 3 下,本文所提出的检测指标输出值会受到载波相位漂移的干扰造成波动,在欺骗信号逐步靠近真实信号阶段,波动会造成检测概率降低,如图 6(b) 所示,但整体来看,检测性能依旧是最优。相较于传统检测门限,本文使用实际理论门限和理论计算门限双重阈值,具有实用性、更高的鲁棒性和良好的检测性能。



(a) 场景 2 下的欺骗检测判决结果图



(b) 场景 3 下的欺骗检测判决结果图

图 6 不同场景下的新型 SQM 检测量 M_{value} 欺骗判决结果图

结合图 4、图 5 和图 6, 欺骗信号引入到接收机环路后, 新型 SQM 检测量 M_{value} 能够在更短的时间内判定存在欺骗干扰, 这意味着新型 SQM 检测量 M_{value} 比其他检测量更为敏感和准确。这是由于新型 SQM 检测量 M_{value} 能够更早地捕捉到目标接收机码跟踪环路输出异常的情况, 减少漏警率。这些优势使得新型 SQM 检测量 M_{value} 成为一种有潜力的工具, 用于对抗欺骗干扰并提高系统的安全性。在场景 2 和场景 3 中新型 SQM 检测量 M_{value} 都能高效检测到欺骗干扰, 故在频率是否锁定的场景下都是检测欺骗的最佳度量。

上述分析在某个场景下单个卫星的检测判决过程, 不具有普遍性。图 7 是对比不同算法在 DS2~DS6 场景下 8 个通道的平均检测概率图。对比算法与所提算法均只使用欺骗前后跟踪环路 I/Q 支路相关器输出, 其他干扰信号对跟踪环路的影响, 如环路失锁, 不在适用范围内。可以看出无论是在不同功率优势下的欺骗场景还是频率是否锁定以及动静态场景下新型 SQM 检测量 M_{value} 都能够保持良好的检测性能。这进一步突显了新型 SQM 检测量 M_{value} 的可靠性。

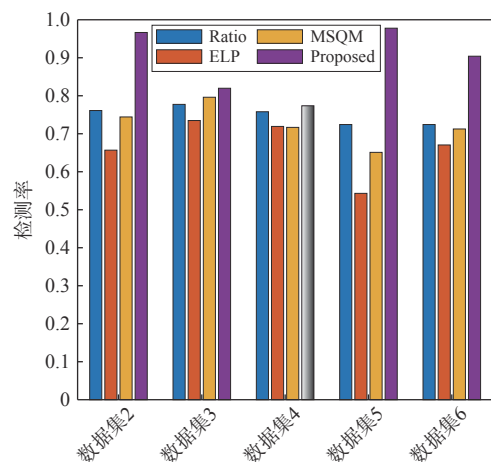


图 7 不同场景下的欺骗检测概率图

和适用性. 它的性能不仅限于特定的干扰场景, 而且在不同场景和信号类型下, 都能够展现出稳定和出色的表现. 综上所述, 新型 SQM 检测量 M_{value} 较传统检测量 Ratio、ELP 以及 MSQM 检测量具有更高的灵敏度、检测率和稳健性, 检测性能更优.

为了验证所提算法在欺骗信号与真实信号载波相位差为 π 的整数倍时, 对欺骗信号的检测有效, 接下来进一步开展出现这种特定条件时的欺骗检测实验. 因本文算法所适用的公开数据集场景 DS2~DS6 并未出现载波相位差为 π 的整数倍的情况, 本文生成了存在欺骗信号与真实信号的载波相位差为 π 的整数倍时的数据, 并与前文提到的 ELP 算法进行检测实验对比.

如图 8 所示, 图 (a) 和图 (b) 分别为 ELP 和所提新型 SQM 检测量及门限的对应关系. 从图中可以看出, 在出现相对载波相位差为 π 的整数倍的两处, ELP 检测方法的检测量均落在双门限内, 表现出检测失效现象. 相反, 本文提出的新型 SQM 检测方法仍保持有效. 本文提出的新型 SQM 算法不受欺骗信号与真实信号载波相位差不能为 π 的整数倍条件的限制.

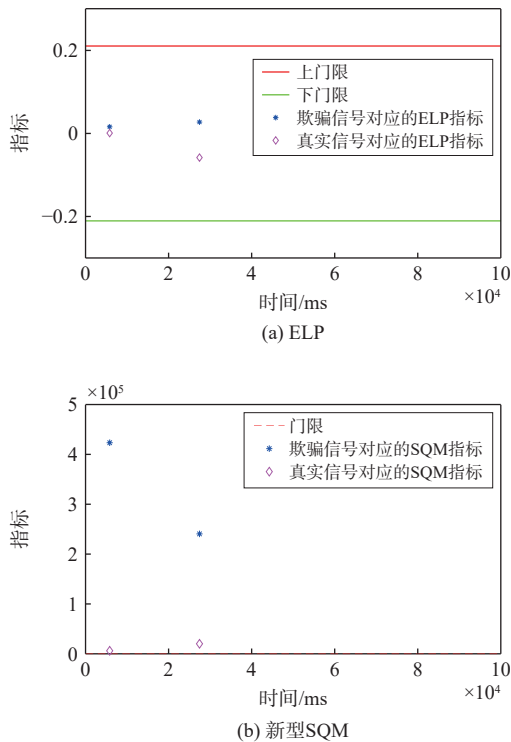


图 8 ELP 与新型 SQM 在相位差为 π 的整数倍时的检测效果对比图

5 结论

本文针对现有 SQM 检测方法适用场景有限的

问题, 提出了一种无需使用跟踪支路载波相位信息的新型 SQM 方法进行导航欺骗干扰检测, 引入同相 I 支路和正交 Q 支路相关器输出值建立新型 SQM 作为欺骗检测量. 给出了在无先验信息下确定检测门限的具体过程, 利用美国德州大学的公共数据库 TEXBAT 的实采信号进行实验分析, 对比了所提 SQM 指标与传统检测量以及 MSQM 算法的检测性能. 实验结果表明, 对于不同卫星的信号和不同场景下, 所提算法能够在较短的时间内检测到欺骗攻击, 并且检测性能优于对比文献算法, 具有更高的灵敏度、检测率和稳健性. 研究成果对未来开发具有中、高级欺骗防御能力的新一代 GNSS 接收机具有参考价值.

随着欺骗攻击方式的多样化和隐蔽性不断增高, 组合式干扰和渐进式干扰等已成为常见攻击方式, 国外研究学者或组织已经开始探索针对此类信号的联合检测方法, 而国内仍处于初级起步阶段, 尚缺乏深入探索以及实际应用的研究. 在后续研究中, 可以考虑组合式干扰的建模与识别, 涉及到对不同干扰信号源的特征提取和组合干扰信号的融合识别, 将各个干扰信号源的特征进行组合并考虑它们之间的相互影响, 利用机器学习和信号处理等技术进行分解和识别.

参考文献

- [1] MORALES-FERRE R, RICHTER P, FALLETTI E, et al. A survey on coping with intentional interference in satellite navigation for manned and unmanned aircraft[J]. *IEEE communications surveys and tutorials*, 2019, 22(1): 249-291. DOI: 10.1109/COMST.2019.2949178
- [2] 潘海涛, 蔡成林. 基于 BP 神经网络的导航信号欺骗干扰检测[J]. *现代电子技术*, 2022, 45(1): 7-10.
- [3] HU Y F, BIAN S F, CAO K J, et al. GNSS spoofing detection based on new signal quality assessment model[J]. *GPS solutions*, 2018, 22(1): 1-13. DOI: 10.1007/s10291-017-0693-7
- [4] 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
- [5] PIRSIYAVASH A, BROUMANDAN A, LACHAPPELLE G, et al. Detection and classification of GNSS structural interference based on monitoring the quality of signals at the tracking level[C]//The 6th ESA international colloquium of scientific and fundamental aspects of Galileo, 2017: 1-10.
- [6] 邓旭, 吕志伟, 周玫龙, 等. 采用载噪比的卫星导航欺骗检测算法设计[J]. *导航定位学报*, 2022, 10(2): 109-118.

- [7] 靳睿敏, 郭艺, 杨会赞, 等. 基于导航接收机的 GNSS 弱干扰检测识别技术 [J]. 全球定位系统, 2022, 47(6): 91-95.
- [8] PIRSIAVASH A, BROUMANDAN A, LACHAPPELLE G. Two-dimensional signal quality monitoring for spoofing detection[C]//The ESA/ESTEC NAVITEC 2016 Conference, Noordwijk, The Netherlands, 2016: 14-16.
- [9] MIRALLES D, BORNOT A, ROUQUETTE P, et al. An 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. DOI: [10.1109/MITS.2020.2994117](https://doi.org/10.1109/MITS.2020.2994117)
- [10] JAHROMI A J, BROUMANDAN A, DANESHMAND S, et al. Galileo signal authenticity verification using signal quality monitoring methods[C]//2016 International Conference on Localization and GNSS (ICL-GNSS). IEEE, 2016: 1-8.
- [11] KHAN A M, AHMAD A. Global Navigation Satellite Systems spoofing detection through measured autocorrelation function shape distortion[J]. *International journal of satellite communications and networking*, 2022, 40(2): 148-156. DOI: [10.1002/sat.1425](https://doi.org/10.1002/sat.1425)
- [12] ZHANG X R, 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. DOI:[10.1049/iet-rsn.2020.0021](https://doi.org/10.1049/iet-rsn.2020.0021)
- [13] WANG X, CUI X, WANG C, et al. Signal quality monitoring of SBAS for satellite-induced elevation-dependent anomaly[J]. *GPS solutions*, 2023, 27(3): 1-18. DOI: [10.1007/s10291-023-01437-1](https://doi.org/10.1007/s10291-023-01437-1)
- [14] CHEN Z K, LI J Z, LI J, et al. GNSS multiparameter spoofing detection method based on support vector machine[J]. *IEEE sensors journal*, 2022, 22(18): 17864-17874. DOI: [10.1109/JSEN.2022.3193388](https://doi.org/10.1109/JSEN.2022.3193388)
- [15] FANG J X T, YUE J, XU B, et al. A post-correlation graphical way for continuous GNSS spoofing detection[J]. *Measurement*, 2023(216): 112974. DOI: [10.1016/j.measurement.2023.112974](https://doi.org/10.1016/j.measurement.2023.112974)
- [16] WESSON K D, GROSS J N, HUMPHREYS T E, et al. GNSS signal authentication via power and distortion monitoring[J]. *IEEE transactions on aerospace and electronic systems*, 2017, 54(2): 739-754. DOI: [10.1109/TAES.2017.2765258](https://doi.org/10.1109/TAES.2017.2765258)
- [17] 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](https://doi.org/10.1109/TIM.2021.3102753)
- [18] 高威雨, 李洪, 陆明泉. 一种新型相关峰畸变检测方法及其在欺骗检测中的应用 [C]//第十一届中国卫星导航年会论文集——S11 抗干扰与反欺骗技术, 2020(7): 83-89.
- [19] 贾琼琼, 朱传胜. 基于多通道 SQM 指标联合的矢量接收机多径干扰检测方法 [J]. 全球定位系统, 2023, 48(3): 110-119.
- [20] 王佳奇, 唐小妹, 孙广富. 基于牛顿迭代法的 GNSS 欺骗干扰参数估计 [J]. 全球定位系统, 2022, 47(6): 86-90.
- [21] 高扬骏, 吕志伟. TEXBAT 场景的 GPS 接收机授时欺骗影响分析 [J]. 测绘科学技术学报, 2019, 36(2): 127-132, 138.

作者简介

邓敏 (1987—), 女, 副教授, 研究方向为导航干扰与抗干扰技术、资源调度、认知无线电. E-mail: iem-deng@xtu.edu.cn

廖欣璐 (2000—), 女, 硕士研究生, 研究方向为导航干扰与抗干扰技术. E-mail: 202221623157@smail.xtu.edu.cn

郭莹莹 (1997—), 女, 硕士研究生, 研究方向为导航干扰检测技术. E-mail: 2221027024@qq.com

姚志强 (1975—), 男, 教授, 研究方向为研究方向为导航定位、下一代宽带无线通信. E-mail: yaozhiqiang@xtu.edu.cn

A novel GNSS spoofing interference detection technology based on SQM

DENG Min^{1,2}, LIAO Xinlu¹, GUO Yingying¹, YAO Zhiqiang¹

(1. School of Automation and Electronic Information, Xiangtan University, Hunan Province Key Laboratory of Credible Intelligent Navigation and Positioning, Xiangtan 411105, China; 2. Hunan National Center for Applied Mathematics in Hunan, Xiangtan 411105, China)

Abstract: The Global Navigation Satellite System (GNSS) plays a strategic role in positioning, navigation, and timing in infrastructure application. Given the characteristics of GNSS signals such as extremely low landing power and transparent civil code structure, civil satellite signals are extremely

vulnerable to interference and spoofing attacks, which makes GNSS suffer from serious interference problems. In this paper, to address the problems of low detection probability and poor reliability of traditional SQM (signal quality monitoring) detection quantities, we propose a new type of SQM detection quantities without the carrier phase information of tracking loop. Then, the metric values are moving averaged to reduce the effect of abnormal fluctuation value on the false alarm probability. Besides, the statistical distribution characteristic of the proposed metric is derived. The computation threshold and measurement threshold without a priori information are set up. The proposed method can avoid the failure detection when the relative carrier phases of spoofing and authorized satellite navigation signal are integer multiples of π . The comparison experimental results based on the public database with real measured signals of TEXBAT (texas spoofing test battery) show that the proposed algorithm is able to detect spoofing attacks with better accuracy in a shorter time under different real signal scenarios. The research results are valuable for the development of anti-spoofing communication devices in the future to improve the detection performance effectively without making large-scale changes to the hardware structure of the receiver.

Keywords: GNSS; spoofing detection; spoofing attack; SQM detection metric; measurement threshold

(上接第 55 页)

Consistency deception detection technique for GNSS/INS based on open-closed-loop alternation

CHENG Yuyang, PENG Xinzhi, FENG Fan, XU Yiyu, YUAN Xuelin, ZHU Xiangwei

(School of Electronics and Information Technology, Sun Yat-Sen University,
Shenzhen 518107, China)

Abstract: The Global Navigation Satellite System (GNSS) and inertial navigation system (INS) are widely used in fields such as vehicles and drones. However, GNSS receivers are susceptible to deceptive signals. Therefore, this paper proposes a consistency deception detection technique using INS observations. Inertial devices have the characteristics of being less susceptible to deceptive signal interference and prone to cumulative errors. By alternately feeding back estimated errors in an open-closed loop manner, a GNSS/INS integrated navigation system is constructed. During the open-loop period, a deception detection window is established, and the consistency between the statistical detection measurements of the inertial device, acceleration, and angular velocity obtained from GNSS is evaluated to determine the presence of deception. Experimental results demonstrate that with a window time of 70 s, the detection probability reaches 99.2% while the false alarm probability is 5.2%.

Keywords: INS; GNSS; deception detection; consistency detection; open-closed-loop