全球定位系统
GNSS World of China
• 中国科学引文数据库（CSCD）
• 中文科技期刊数据库
• 中国核心期刊（遴选）数据库
• 日本科学技术振兴机构数据库（JST）
• 中国学术期刊（网络版）（CNKI）
• 中国学术期刊综合评价数据库（CAJCED）
• 中国超星期刊域出版平台

多相关器联合功率GNSS欺骗干扰检测方法研究

赵　慎，廖一霏，李世玲，周开军

Research on GNSS spoofing interference detection for multi-correlator combined power

ZHAO Shen, LIAO Yifei, LI Shiling, and ZHOU Kaijun

引用本文:
赵慎，廖一霏，李世玲，等．多相关器联合功率GNSS欺骗干扰检测方法研究[J]．全球定位系统，2024，49(4)：66-74．DOI: 10.12265/j.gnss.2023235
ZHAO Shen, LIAO Yifei, LI Shiling, et al. Research on GNSS spoofing interference detection for multi-correlator combined power[J]. Gnss World of China, 2024, 49(4): 66-74. DOI: 10.12265/j.gnss.2023235

在线阅读 View online: https://doi.org/10.12265/j.gnss.2023235

DOI: 10.12265/j.gnss.2023235

多相关器联合功率 GNSS 欺骗干扰检测方法研究

赵慎[1,2], 廖一霏[1], 李世玲[1,2], 周开军[1,2]

(1. 湖南工商大学智能工程与智能制造学院, 长沙 410205; 2. 湘江实验室, 长沙 410205)

摘　要: GNSS 民用信号因其公开性和脆弱性易受外界欺骗干扰. 作为欺骗干扰检测的有效方法, 信号质量监测 (signal quality monitoring, SQM) 技术通过检测接收机跟踪环路早码、即时码、晚码 (early late phase, ELP) 的相关结果, 与无欺骗时的相关特性对比, 判断是否存在欺骗干扰. 常规 SQM 算法仅利用 ELP 三个信息, 检测性能受限, 为此提出多相关器联合功率 (SQM detection of power combined Multi-correlator groups, SPCM) 算法. 以 ELP 之间多个等间隔相关器输出功率的加权为检测量, 且取相关时刻与即时码时间差的反比为加权系数; 进一步分析检测量的概率分布特性, 并基于 Neyman-Pearson 理论确定最佳检测阈值, 通过比较检测量与检测阈值的大小, 判断是否存在欺骗干扰. 基于美国德克萨斯大学奥斯汀分校公开的场景四数据集进行试验, 结果表明: 与 Ratio 和 ELP 等典型 SQM 算法相比, 在不同虚警率条件下, 所提出 SPCM 算法兼具高检测概率和快速预警响应时间性能.

关键词: 卫星导航; 欺骗干扰; 码跟踪环; 信号质量监测; 多相关器

中图分类号: P228; TN972　　**文献标志码:** A　　**文章编号:** 1008-9268(2024)04-0066-09

0　引　言

GNSS 因具备易用性、统一性和实时性的特性, 已成为信息化社会基础中时间和空间基准服务的重要支撑[1]. GNSS 民用信号的开放性和脆弱性凸显, 不法分子可对接收机实施干扰和欺骗. 常规欺骗分为压制式干扰和欺骗式干扰[2-3], 压制式干扰通过发射大功率干扰信号使接收机失锁, 易被检测出; 欺骗式干扰发射的欺骗信号功率小、结构与导航信号相似, 使得其隐蔽性好而检测难度大. 欺骗式干扰主要分为转发式欺骗和生成式欺骗两类: 转发式欺骗将接收到的导航信号经功率放大转发, 由于存在不可消除的时延, 接收机跟踪环路输出两个相关峰, 较易检测转发式欺骗; 生成式欺骗通过模拟生成虚假的导航信号, 以此对目标接收机的跟踪实施欺骗, 使其误锁在欺骗信号上得到错误的伪距信息, 达到隐蔽欺骗的目的. 因此, 生成式欺骗具有更强的隐蔽性和适用性, 对导航设备的时空信息安全具有较大危害. 如何高效检测出目标接收机是否收到欺骗干扰, 已成为 GNSS 中热点研究领域并引起广泛关注.

根据接收机结构和检测量的不同[4], 主要分为基于导航数据信息[5]、阵列天线[6-7]、射频前端[8]、基带信号处理[9]、定位结果后处理[10] 和机器学习融合等六类欺骗检测方法. 其中, 作为基带信号处理检测技术之一, 信号质量监测 (signal quality monitoring, SQM) 不改变接收机原有结构, 通过识别相关峰的异常程度判断导航信号中是否存在欺骗干扰, 具有简单、高效、低成本等优势. 在无欺骗时, 早码、即时码和晚码 (early late code, ELP) 相关器输出呈等腰三角形[11]; 当有欺骗时, 欺骗信号逐渐靠近对齐真实信号, 两者相互作用, 导致相关峰畸变.

针对以上特性, 文献 [12] 将用于多径检测的 Ratio 和 Delta 方法用于欺骗检测, Ratio 算法可检测相关峰尖锐异常, 而 Delta 算法旨在监测相关峰的不对称性. 文献 [13-14] 提出 ELP 算法, 当早码和晚码相关器输出的相位延迟存在大幅变化时, 判定为存在欺骗信号, 相比于 Ratio 算法和 Delta 算法, 其利用正交支路相关器的输出, 可有效改善检测性能. 综合以上算

收稿日期: 2023-12-25

资助项目: 国家自然科学基金项目 (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)

通信作者: 廖一霏 E-mail: liaoyifeifeifei@163.com

法的优点, 文献 [15] 提出复合 SQM 度量检测算法. 针对不同 SQM 指标的互补特性, 将其中两者加权组合进行检测, 并采取移动方差处理方法[16], 有效提升检测概率. 文献 [17] 提出了 S 曲线过零点偏差 (scurve bias, SCB) 检测算法, 基于 SCB 技术, 并结合 Sun 的移动方差技术, 判断 SCB 是否超出阈值, 改进 SCB 技术提高检测概率[18]. 文献 [19] 提出了功率监测与 SQM 融合 (power combined with SQM, PCS) 算法利用相关器输出的功率差值, 减小即时码的误差影响. 文献 [20] 计算早码、晚码之间的多相关器差值, 并对其加权二阶矩作为检测统计量, 以增加算法复杂度为代价提升检测性能.

上述 SQM 算法大多仅利用三个相关器的信息, 通过监测 ELP 的同相相关或相关幅度变化, 实现导航欺骗检测. 随着诱导欺骗技术隐蔽性、控制精度的提高, 仅基于三个相关器检测欺骗的信息利用率低, 检测性能受限, 为此本文提出多相关器联合功率 (SQM detection of power combined Multi-correlator groups, SPCM) 算法. 通过细化相关间隔以增加相关器数量, 计算即时码左、右各 1 个码片内的多组相关器输出功率, 并根据与即时码时间间隔的反比关系设定权重, 取多相关器输出功率的线性加权为检测量, 进一步通过 N-P 理论确定最佳检测阈值, 实现多组检测信息下的导航欺骗检测.

1　信号模型

当存在欺骗时, 接收机的接收信号为真实信号、欺骗信号和高斯白噪声[21] 的加性组合, 在 t 时刻为

$$x(t) = x_{\rm r}(t) + x_{\rm s}(t) + n(t) \tag{1}$$

式中: $x_{\rm r}(t)$为真实信号; $x_{\rm s}(t)$为欺骗信号; $n(t)$表示均值为 0、方差为σ_n^2的高斯白噪声. 真实信号与欺骗信号的结构相同, 多普勒频移和码相位不同, 分别表示为:

$$\begin{aligned} x_{\rm r}(t) &= \sqrt{P_{\rm r}} D_{\rm r}(t-\tau_{\rm r}) C_{\rm r}(t-\tau_{\rm r}) e^{{\rm j}\phi_{\rm r}+{\rm j}2\pi(f_0+f_{\rm r})t} \\ x_{\rm s}(t) &= \sqrt{P_{\rm s}} D_{\rm s}(t-\tau_{\rm s}) C_{\rm s}(t-\tau_{\rm s}) e^{{\rm j}\phi_{\rm s}+{\rm j}2\pi(f_0+f_{\rm s})t} \end{aligned} \tag{2}$$

式中: $P_{\rm r}$和$P_{\rm s}$分别为真实信号和欺骗信号的功率; $D_{\rm r}$和$D_{\rm s}$分别为真实信号和欺骗信号的数据比特电平值; $C_{\rm r}$和$C_{\rm s}$分别是真实信号和欺骗信号的伪随机扩频码; $\tau_{\rm r}$和$\tau_{\rm s}$分别为真实信号和欺骗信号的码相位; $\phi_{\rm r}$和$\phi_{\rm s}$分别为真实信号和欺骗信号的载波相位; $f_{\rm r}$和$f_{\rm s}$分别为真实信号和欺骗信号的多普勒频移; f_0为导航信号的载波频率.

当不存在欺骗干扰时, 信号进入跟踪环路后经过混频器分为同相、正交支路, 与本地产生的即时 C/A 码进行相关运算. 当接收机锁定时, 接收信号与本地产生信号的频率完全相同, 假定相干积分累积时间内未发生数据位跳变, 且码相位和多普勒频移的影响相互独立, 相干积分输出为:

$$\begin{aligned} I_{\rm P}(n) &= \sqrt{P_{\rm r}} D(n) R(\hat{\tau}) \cos\phi_{\rm r} + \eta_{\rm I} \\ Q_{\rm P}(n) &= \sqrt{P_{\rm r}} D(n) R(\hat{\tau}) \sin\phi_{\rm r} + \eta_{\rm Q} \end{aligned} \tag{3}$$

式中: $I_{\rm P}$、$Q_{\rm P}$分别为同相、正交相关器的输出; $\eta_{\rm I}$、$\eta_{\rm Q}$分别为同相、正交支路的噪声; $\hat{\tau}$为真实信号与本地生成信号的码相位差; $R(\hat{\tau})$为真实信号与本地生成信号的相关函数. 以 GPS L1 频段为例, 表达式为

$$R(\hat{\tau}) = \begin{cases} 1-|\hat{\tau}|, & |\hat{\tau}| \leqslant 1 \\ 0, & |\hat{\tau}| > 1 \end{cases} \tag{4}$$

忽略多普勒频移误差影响, 理论上同相、正交支路输出服从高斯分布, 理论统计量为:

$$\begin{aligned} \mu_{\rm I} &= \sqrt{P_{\rm r}} R(\hat{\tau}) \cos\phi_{\rm r} \\ \mu_{\rm Q} &= \sqrt{P_{\rm r}} R(\hat{\tau}) \sin\phi_{\rm r} \\ \sigma_{\rm I}^2 = \sigma_{\rm Q}^2 = \sigma_0^2 &= \frac{1}{2T_{\rm s}({\rm C/N_0})} \\ \sigma_{\rm IQ} &= 0 \end{aligned} \tag{5}$$

式中, $\mu_{\rm I}$、$\mu_{\rm Q}$、$\sigma_{\rm I}^2$、$\sigma_{\rm Q}^2$分别为同相、正交支路相关器输出的均值和方差. 根据文献 [22] 中对正常功率下真实信号的仿真结果, 同相、正交支路之间互相关函数的方差$\sigma_{\rm IQ} = \sigma_{\rm QI} = 0.000\,33$, 由于量值较小可忽略不计. $\sigma_{\rm I}^2$、$\sigma_{\rm Q}^2$只取决于相关器的噪声, 与信号无关, σ_0^2为相关后噪声的方差. $T_{\rm s}$为相干积分时间, ${\rm C/N_0}$为接收信号的载噪比.

当存在欺骗信号时, 进入跟踪环路的混合信号如式 (1) 所示. 此时, 同相、正交支路相关器的输出:

$$\begin{aligned} I(n) &= \sqrt{P_{\rm r}} D(n) R(\hat{\tau}) \cos\phi_{\rm r} + \sqrt{P_{\rm s}} D(n) R(\tilde{\tau}) \cos\phi_{\rm s} + \eta_{\rm I} \\ Q(n) &= \sqrt{P_{\rm r}} D(n) R(\hat{\tau}) \sin\phi_{\rm r} + \sqrt{P_{\rm s}} D(n) R(\tilde{\tau}) \sin\phi_{\rm s} + \eta_{\rm Q} \end{aligned} \tag{6}$$

式中, $\tilde{\tau}$为欺骗信号与本地码的码相位差. 相关运算后的互相关函数表示为

$$R(\tau) = R(\hat{\tau}) + R(\tilde{\tau}) \tag{7}$$

式中: $R(\hat{\tau})$为真实信号与本地码的互相关函数; $R(\tilde{\tau})$为欺骗信号与本地码的互相关函数. 欺骗信号与真实信号的码相位差$\Delta\tau = |\hat{\tau} - \tilde{\tau}|$, 当$\Delta\tau$逐渐减小至 1 个码片内, 欺骗信号使$R(\tau)$的结果畸变.

基于以上信号模型, 接收机从锁定真实信号逐渐被牵引至锁定欺骗信号过程中, 结果如图 1 所示.

图 1(a) 中, 欺骗信号与真实信号间隔远大于 1 个码片宽度, 仅能观察到真实信号的相关峰; 随着欺骗信号与真实信号的间隔减小, 直至两信号完全重叠, 相关图形如图 1(b) 所示, 此时相关峰峰值达到最大; 之后接收机逐渐被欺骗信号牵引锁定, 如图 1(c) 所示; 最后两信号完全分离, 出现两个相关峰, 如图 1(d) 所示.

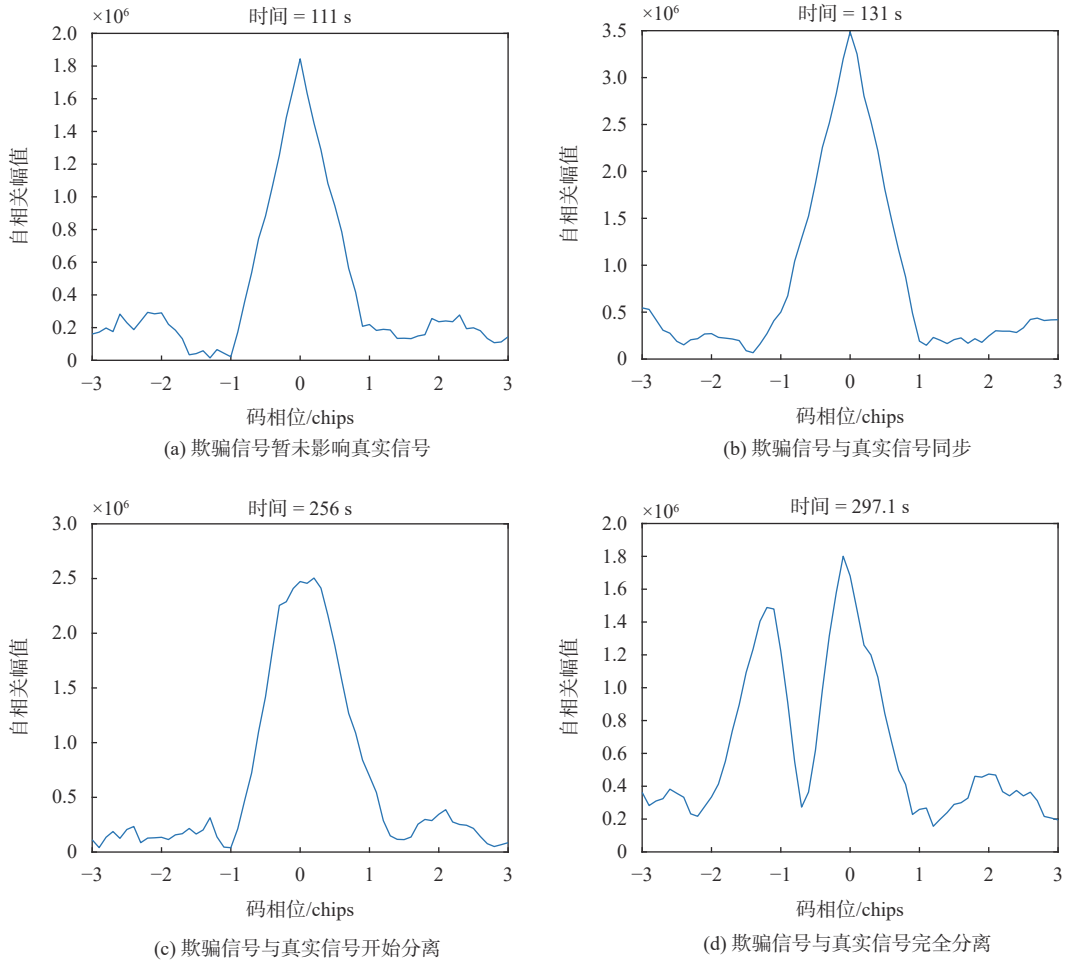


图 1 欺骗攻击示意图

2 检测算法

2.1 传统 SQM 算法

SQM 利用 EPL 的输出构建检测量, 通过统计检测量得到检验门限, 将检测量与门限对比, 判断是否存在欺骗. 作为 SQM 的经典算法, 传统 Ratio 和 ELP 的检测量以 0.5 码片为间隔, 分别为:

$$\text{Ratio} = \frac{E_{\text{I}} + L_{\text{I}}}{2P_{\text{I}}} \tag{8}$$

$$\text{ELP} = \arctan\left(\frac{Q_E}{I_E}\right) - \arctan\left(\frac{Q_L}{I_L}\right) \tag{9}$$

式中: E_{I}、L_{I}、P_{I}为同相相关器 EPL 的输出, Q_E、Q_L为正交相关器早码、晚码的输出. Ratio 旨在利用E_{I}、L_{I}、P_{I}三者间比值关系, 判断相关峰的异常程度; ELP 则通过早码与晚码相位差的量值大小, 检测相位变化. 二者缺点在于, Ratio 算法仅利用了同相支路信息, 无法消除载波相位误差的影响; 当欺骗信号与真实信号的相位差为 π 的整数倍时, ELP 算法失效[19]. 综合分析可知, 两种算法均存在一定的局限性, 导致 SQM 方法的检验性能不佳.

2.2 SPCM 检测算法

针对传统 SQM 方式的不足, 本文提出对多组相关器输出的线性加权方法, 改善相关函数对称性的检测精度, 以提升检测性能. 图 2 为基于多相关器输出的检测原理框图.

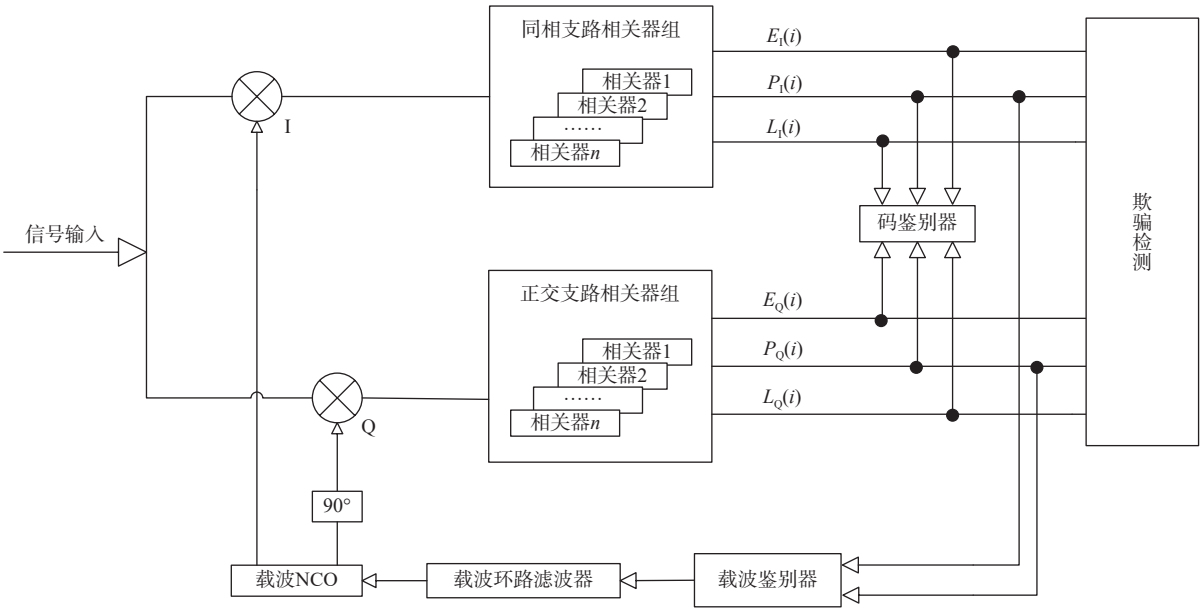


图 2　多相关器实现框图

取不同间隔相关器输出的相关功率, 利用相关峰对称性和 ELP 的比例关系, 将早码、晚码按照与即时码的相关时间间隔设置权重系数, 通过多组功率线性加权, 形成 SPCM 检测量

$$\mathrm{SPCM}=\sum_{i=1}^{n}(1-l_i)*(y_E(i)+y_L(i))-2*\sum_{i=1}^{n}(1-l_i)^2*y_P(i) \tag{10}$$

式中: 相关器组输出功率$y_\alpha(i)=I_\alpha^2(i)+Q_\alpha^2(i)$; l_i为相关器和相关时刻与即时码的码片间距; n 为相关器对数, 文中取 n=9, 在即时码两侧、相距间隔各为 0.1 码片的九个相关器; 不存在干扰时, $y_E(i)$、$y_L(i)$以$y_P(i)$为中心呈对称特性, 并且满足$y_E(i)/y_P(i)=(1-l_i)$. 设置早、晚码的输出权重为$1-l_i$, 并调整$y_P(i)$的系数为$(1-l_i)^2$. 由于远离即时码的输出功率受噪声影响较大, 按反比关系设定早、晚码权重, 目的是通过减小宽带相关器的权重、提高窄带相关器的权重, 减小误差影响.

将式 (10) 进一步表示为

$$\mathrm{SPCM}=\sum_{i=1}^{n}\left((1-l_i)*y_E(i)-(1-l_i)^2*y_P(i)\right)+\sum_{i=1}^{n}\left((1-l_i)*y_L(i)-(1-l_i)^2*y_P(i)\right) \tag{11}$$

式中, 左项与右项的概率分布特性相同, 不失一般性, 以左项为例进行分析. 由式 (5) 可知, 无欺骗时, I_{l_i}、Q_{l_i}均服从高斯分布, 即$I_{l_i}\sim \mathrm{N}(\mu_{I_{l_i}},\sigma_0^2)$, $Q_{l_i}\sim \mathrm{N}(\mu_{Q_{l_i}},\sigma_0^2)$; 根据非中心 χ^2分布定义, $\sum_{i=1}^{n}(1-l_i)*y_E(i)$、$\sum_{i=1}^{n}(1-l_i)^2*y_P(i)$为自由度 V=2n 的非中心 χ^2分布. $y_E(i)/y_P(i)=(1-l_i)$, 故$\sum_{i=1}^{n}(1-l_i)*y_E(i)$与$\sum_{i=1}^{n}(1-l_i)^2*y_P(i)$均值相等. 取$\delta=\sum_{i=1}^{V}\mu_i^2$, 则二者的非中心参数相同且服从 $\chi^2(2n,\delta)$, 其特征函数为

$$\varphi=(1-2\mathrm{j}t)^{-n}\mathrm{e}^{\frac{\mathrm{j}t\delta}{1-2\mathrm{j}t}} \tag{12}$$

式中: j 为虚数; $\sum_{i=1}^{n}y_E$与$\sum_{i=1}^{n}(1-l_i)*y_P(i)$相互独立, $\sum_{i=1}^{n}\left((1-l_i)*y_E(i)-(1-l_i)^2*y_P(i)\right)$特征函数为

$$\begin{aligned}\phi&=\phi_{y_E}(t)\cdot\phi_{(1-l_i)*y_P}(-t)\\&=[(1\text{-}2\mathrm{j}t)^{-n}\mathrm{e}^{\frac{\mathrm{j}t\delta}{1-2\mathrm{j}t}}][(1+2\mathrm{j}t)^{-n}\mathrm{e}^{\frac{-\mathrm{j}t\delta}{1+2\mathrm{j}t}}]\\&=(1+4t^2)^{-n}\mathrm{e}^{\frac{-4t^2\delta}{1+4t^2}}\end{aligned} \tag{13}$$

根据中心极限定理, 随着自由度 V 增大, 非中心 χ^2分布趋近于高斯分布. 在不同自由度下, 非中心 χ^2分布的概率密度函数如图 3 所示.

根据上述分析, 式 (11) 中左项可近似看作高斯分布, 右项亦如此. 结合高斯分布的性质, SPCM 检测量近似服从高斯分布. 图 4 中的蓝色统计结果为无欺骗条件下实际数据分布直方图, 红色为理论分布的概率密度曲线, 二者表现出很好的一致性, 由此验证了上述分析的合理性.

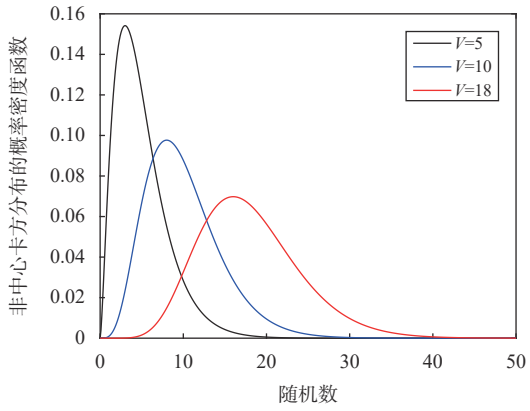


图 3 不同自由度下的卡方分布

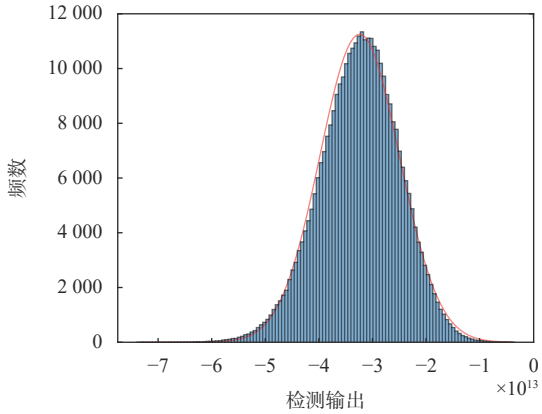


图 4 SPCM 检测量输出分布

理论上, 无欺骗时, SPCM 算法检测量的均值为 0; 欺骗信号进入环路, 相关峰随之畸变引起检测量输出异常. 通过结合窄带、宽带相关器, 并利用多个环路输出信息, SPCM 算法可更准确地拟合相关峰曲线, 实现更精准、快速的欺骗判断. 实际场景中, 由于多径和噪声的影响, 实际相关的比例系数与理论存在偏差, 使得在无欺骗环境下 SPCM 检测量的均值存在一定零偏.

2.3 检测门限及概率分析

欺骗检测可以视为二元假设检验问题[23], 将检验结果分为两个判决假设情况: 无欺骗干扰 H_0 和有欺骗干扰 H_1. 欺骗检测通常将检测量与判决门限比较, 当检测量超过判决门限设置的范围, 判定欺骗存在. 为分析虚警率 P_{fa} 和检测概率 P_d, 定义检测量 $S=\mathrm{SPCM}$, 由 2.2 节分析, 其近似服从高斯分布 $S\sim \mathrm{N}(\mu,\sigma^2)$.

若已知存在欺骗干扰时 SPCM 的概率密度函数, 则检测概率

$$P_d=\int_{-\infty}^{\mathrm{Th_l}}P(S/H_1)\,\mathrm{d}S+\int_{\mathrm{Th_u}}^{+\infty}P(S/H_1)\,\mathrm{d}S \tag{14}$$

为设置合适的判决门限, 基于奈曼-皮尔逊 (Neyman-Pearson, NP) 检测器[24] 判断上、下门限 $\mathrm{Th_u}$ 和 $\mathrm{Th_l}$

$$\begin{aligned}\mathrm{Th_u}&=\mu+\sqrt{2}\sigma\mathrm{erfc}^{-1}(P_{fa})\\ \mathrm{Th_l}&=\mu-\sqrt{2}\sigma\mathrm{erfc}^{-1}(P_{fa})\end{aligned} \tag{15}$$

由于欺骗信号的多样性和时变性, 无法理论计算 SPCM 的概率密度函数. 实际中一般采用统计方式得到检测概率 P'_d, 以超过判决门限样本数 Num 与样本总数 N 的比值 P'_d 代替 P_d, 且

$$P'_d=\frac{\mathrm{Num}(\mathrm{SPCM}(t)<\mathrm{Th_l})+\mathrm{Num}(\mathrm{SPCM}(t)>\mathrm{Th_u})}{N} \tag{16}$$

综上所述, SPCM 算法检验流程图如图 5 所示.

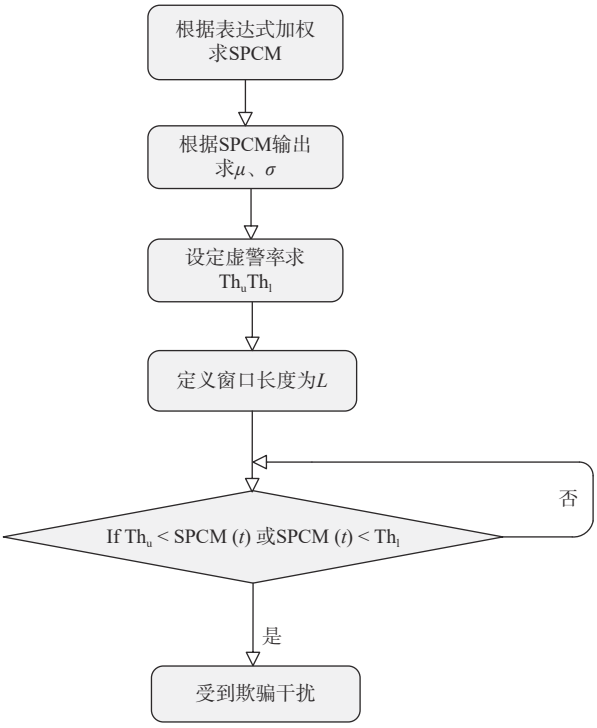


图 5 SPCM 算法检验流程图

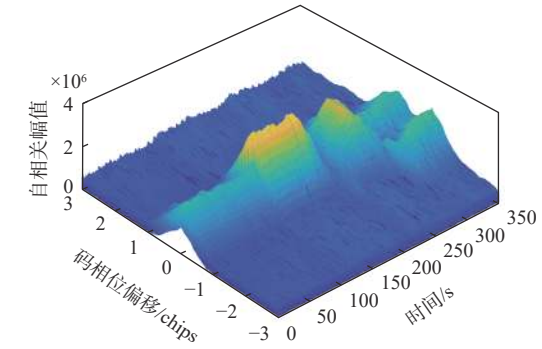
3 试验分析

3.1 试验仿真结果

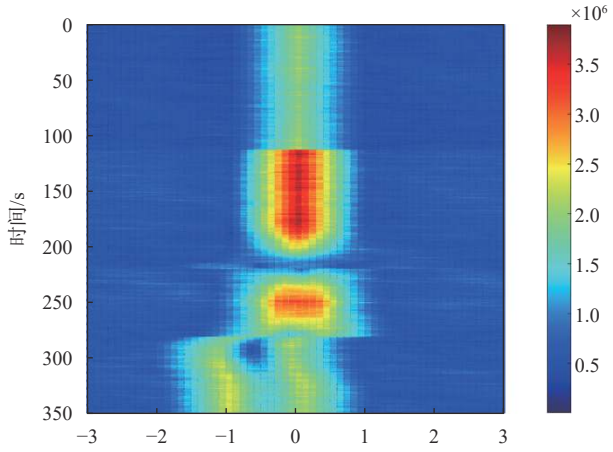
基于美国德克萨斯大学奥斯汀分校无线电导航实验室提供的 TEXBAT 数据集[25], 对比 Ratio、ELP 与 SPCM 算法进行算法验证和性能评估. TEXBAT 作为公开欺骗测试数据集, 采用 25 MHz 采样率, 采集 L1 附近 20 MHz 带宽导航信号, 包含 8 个欺骗干扰场景 (DS1-DS8), 其中 DS1-DS6 从 100 s 注入欺骗.

为验证算法有效性, 选用欺骗信号与真实信号功率相近, 且频率锁定的 DS4 数据集, 欺骗过程中相关函数输出随时间变化情况如图 6 所示. 由图 6(a) 可观

察出无欺骗干扰、欺骗信号注入、跟踪环路锁定于欺骗信号的全过程. 图 6(b) 为相关器输出功率结果, 由于欺骗信号对真实信号频率锁定不稳定, 导致功率泄露, 表现为图中功率跳变.



(a) 相关幅度输出的三维图



(b) 相关幅度输出的俯视图

图 6　61 个相关器随时间变化的相关幅度输出图

在导航信号质量评价中, 载噪比作为关键性能评价指标, 对于高动态导航接收机具有重要意义. 为进一步体现欺骗信号加入对真实信号的影响, 将两种场景下的载噪比进行对比分析, 如图 7 所示. 红色曲线为 DS4 欺骗场景, 蓝色为未欺骗场景. 当欺骗信号加入后, 在功率匹配的优势下, 欺骗信号与真实信号相互作用, 载噪比产生明显波动. 当接收机完全跟踪至欺骗信号后, 载噪比开始趋于稳定.

以 PRN6 为例, 图 8 为传统 SQM 检测量变化曲线. 由图 8 可见, Ratio 与 ELP 方法的检测量均在 113 s 时存在微小跳变, 同时在 113~180 s 波动较小. 该时间段内, 欺骗信号处于与真实信号对齐阶段, 传统 SQM 的两种算法均未能检测出欺骗干扰.

图 9 为所提出的 SPCM 检测量变化曲线, 并将其分成四个阶段, 对应欺骗信号牵引接收机的四种状态. 第一阶段 (100~113 s), 欺骗信号注入并逐渐靠近真实信号, 此时 SPCM 检测量未表现出明显变化; 第二阶段 (113~180 s), 欺骗信号与真实信号的码相位逐渐靠拢, 以高于真实信号 0.4 dB 的功率优势对接收机实施欺骗, SPCM 检测量急剧跳变; 第三阶段 (180~282 s), 欺骗信号实现与真实信号的码相位对齐, 接收机被牵引直至完全锁定于欺骗信号; 第四阶段 (282~350 s), 接收机完全锁定于欺骗信号, 此时真实信号与欺骗信号彻底分离.

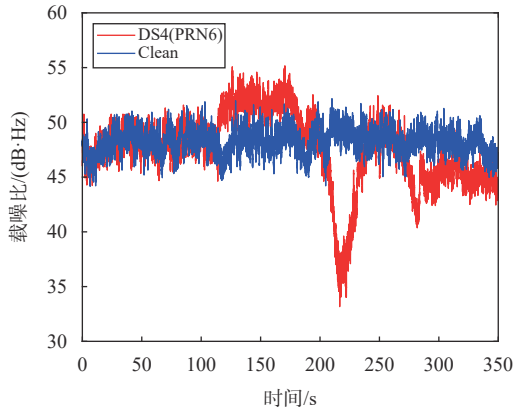
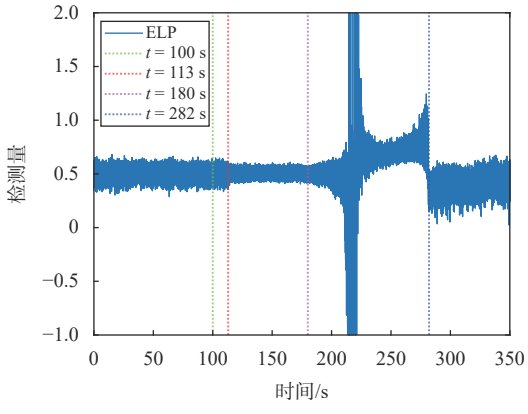
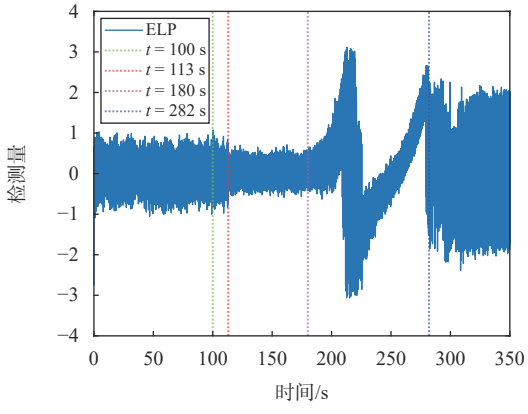


图 7　PRN6 载噪比变化曲线



(a) Ratio检测量



(b) ELP检测量

图 8　传统 SQM 检测量示意图

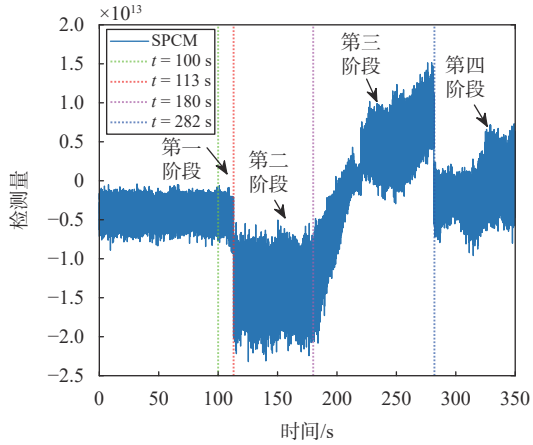


图 9 SPCM 检测量随时间变化图

3.2 检测性能评估

设置虚警率 $P_{fa}=10\%$，由式 (15) 计算 SPCM 的检测上限 $\mathrm{Th_u}=-2.295\,5\times10^{12}$、检测下限 $\mathrm{Th_l}=-5.462\,5\times10^{12}$. 采用长为 1 s 的移动窗口，通过式 (16) 计算每个移动窗口内 SPCM、Ratio、ELP 的检测概率，如图 10所示.

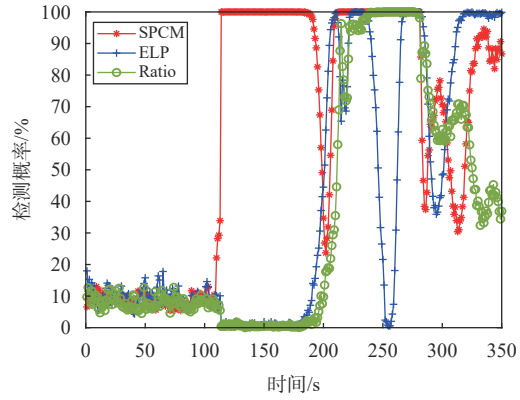


图 10 检测概率对比

分析图 10 中检测概率结果可知，在无欺骗时段 (0~100 s)，三种算法的检测概率均约为 10%，与预设的虚警概率一致；在 110~180 s 时段，SPCM 的检测概率高于 90% 且接近 100%，而 Ratio 和 ELP 的检测概率近似为 0；在 205~280 s 的第三阶段内，Ratio 和 SPCM 的检测概率基本高于 90%，ELP 略逊一筹. 由此可见，Ratio 与 ELP 算法对欺骗干扰的有效检测时刻远滞后于欺骗注入时刻，此时欺骗信号对接收机的跟踪环路已造成不可逆的影响，无法满足实际应用中欺骗预检的需要. 综上所述，相比于传统 SQM 算法，SPCM 算法可提升欺骗干扰的检测概率，且可实现更快的欺骗预警响应.

进一步计算三种算法的接收机工作特性 (receiver operating characteristic, ROC) 曲线，如图 11 所示. ROC 曲线离左上角越近，检测越准确. 在相同虚警率下，SPCM 的检测概率远高于 Ratio 和 ELP，并在全区间内都高于 90%. 当虚警率为 0.1% 时，检测概率也达到 90.57%，确保在小虚警率下检测的准确性，扩展了算法应用范围.

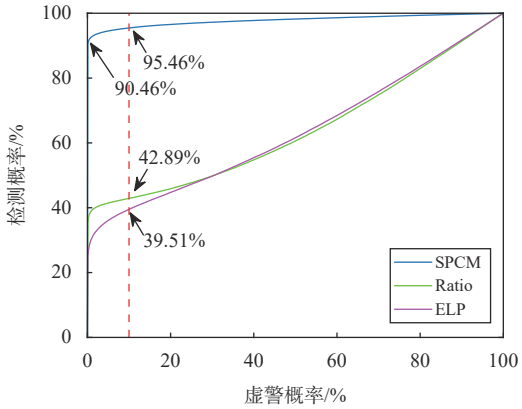
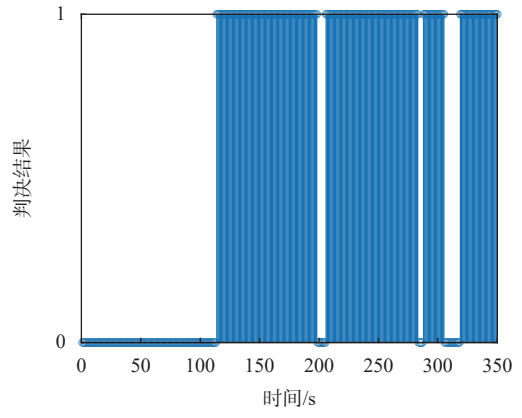
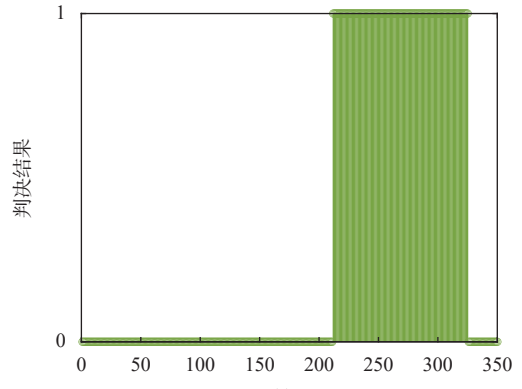


图 11 ROC 曲线对比

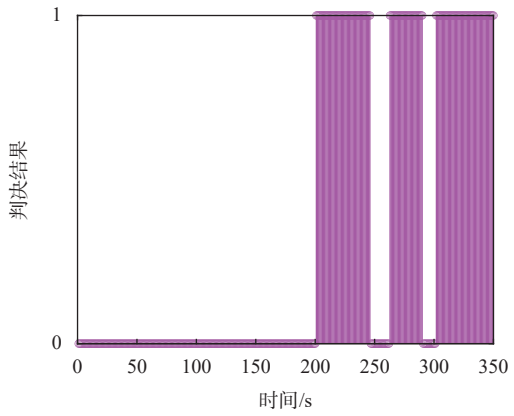
结合 ROC 曲线结果，为进一步评估算法的检测精度，设置虚警率 $P_{fa}=0.1\%$，对 SPCM 的检测概率进行二元判决. 设定判决检测阈值为 50%，大于 50% 输出为 1，则判断为有欺骗；小于 50% 输出为 0，则判断为无欺骗，结果如图 12 所示. 由图可见，SPCM 在



(a) SPCM检测量



(b) Ratio检测量



(c) ELP检测量

图 12　不同检测量的二元判决结果

第二、第三阶段判决为 1 的次数远超 Ratio、ELP 算法, 且判定欺骗开始时间远早于二者. 故在小虚警率下, SPCM 算法仍保证高灵敏度与检测率.

4　结　论

针对传统 SQM 欺骗检测预警响应慢、检测概率低的问题, 本文提出了 SPCM 算法. 从提高信息利用率出发, 算法以即时码两侧多组相关器输出功率的线性加权作为检测量; 为减小误差影响, 取相关时刻与即时码时间差的反比为加权系数. 基于 TEXBAT 的 DS4 数据集的试验表明, 与 Ratio、ELP 算法相比, SPCM 算法可将欺骗预警响应提前至欺骗对齐时刻, 且具有较高的检测概率性能. 同时, SPCM 需计算多组相关器, 以牺牲运算量实现高检验性能, 对处理生成式欺骗干扰有一定的借鉴价值.

参考文献

[1] ISLAM S, BHUIYAN M Z H, PAAKKONEN I, et al. Impact analysis of spoofing on different-grade GNSS receivers[C]// IEEE/ION Position, Location and Navigation Symposium, 2023: 492-499. DOI:10.1109/PLANS53410.2023.10139934

[2] TURNER M, WIMBUSH S, ENNEKING C, et al. Spoofing detection by distortion of the correlation function[C]// IEEE/ION Position, Location and Navigation Symposium, 2020: 566-574. DOI:10.1109/PLANS46316.2020.9110173

[3] 耿正霖, 聂俊伟, 王飞雪. GNSS 抗欺骗干扰技术研究 [J]. 全球定位系统, 2013, 38(4): 65-70.

[4] 谢钢. GPS 原理与接收机设计 [M]. 北京: 电子工业出版社, 2009: 1-13.

[5] WU Z J, LIANG C, ZHANG Y. Blockchain-based authentication of GNSS civil navigation message[J]. IEEE transactions on aerospace and electronic systems, 2023, 59(4): 4380-4392. DOI: 10.1109/TAES.2023.3241041

[6] 任彬彬, 倪少杰, 陈飞强, 等. GNSS 调零抗干扰天线的反欺骗性能分析 [J]. 全球定位系统, 2021, 46(6): 30-36.

[7] LEE Y S, YEOM J S, JUNG B C. A novel array antenna-based gnss spoofing detection and mitigation technique[C]// IEEE 20th Consumer Communications & Networking Conference (CCNC), 2023: 489-492. DOI:10.1109/CCNC51644.2023.10060423

[8] SAKORN C, SUPNITHI P. Calculating AGC and C/N0 thresholds of mobile for jamming detection[C]//The 18th International Conference on Electrical Engineering/ Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), 2021. DOI:10.1109/ECTI-CON51831.2021.9454850

[9] YANG B, TIAN M, JI Y W, et al. Research on GNSS spoofing mitigation technology based on spoofing correlation peak cancellation[J]. IEEE communications letters, 2022, 26(12): 3024-3028. DOI: 10.1109/LCOMM.2022.3204944

[10] ZHANG X, DING C C, XIA H, et al. INS-Aided multi-antenna GNSS carrier phase double difference spoofing detection[J]. IEEE access, 2023(11): 19523-19533. DOI: 10.1109/ACCESS.2023.3247968

[11] JAFARNIA-JAHROMI A, BROUMANDAN A, NIELSEN J, et al. GPS vulnerability to spoofing threats and a review of antispoofing techniques[J]. International journal of navigation and observation, 2012: 1-16. DOI: 10.1155/2012/127072

[12] PHELTS R E. Multicorrelator techniques for robust mitigation of threats to GPS signal quality[D]. Palo Alto, Calif, USA: Stanford University, 2001.

[13] MUBARAK O M, DEMPSTER A G. Performance comparison of ELP and DELP for multipath detection[C]// International Technical Meeting of the Satellite Division of the Institute of Navigation, 2009.

[14] 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

[15] 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

[16] SUN C, CHEONG J W, DEMPSTER A G, et al. Moving variance-based signal quality monitoring method for spoofing detection[J]. GPS solutions, 2018, 22(3): 83. DOI: 10.1007/s10291-018-0745-7

[17] WANG W Y, LI N, WU R B, et al. Detection of induced GNSS spoofing using S-Curve-Bias[J]. Sensors, 2019, 19(4): 922. DOI:10.3390/s19040922

[18] 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.

[19] 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.

[20] ZHOU W L, LV Z W, DENG X, 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

[21] JAHROMI A J. GNSS signal authenticity verification in the presence of structural interference[D].Department of Geomatics Engineering, University of Calgary, 2013. DOI:10.11575/PRISM/26310

[22] JAHROMI A J, BROUMANDAN A, NIELSEN J, et al. GPS spoofer countermeasure effectiveness based on signal strength, noise power, and C/N_0 measurements[J]. International journal of satellite communications and networks, 2012, 30(4): 181-191. DOI: 10.1002/sat.1012

[23] 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

[24] SENGIJPTA S K. Fundamentals of statistical signal processing: estimation theory[J]. Technometrics, 1995, 37(4): 465-466. DOI: 10.1080/00401706.1995.10484391

[25] HUMPHREYS T E, BHATTI J A, SHEPARD D P, et al. The texas spoofing test battery: toward a standard for evaluating gps signal authentication techniques[C]//International Technical Meeting of the Satellite Division of the Institute of Navigation, 2012. DOI:10.15781/T26D5PT4X

作者简介

赵慎 (1983—), 男, 博士, 研究方向为阵列信号处理、导航时空信息安全. E-mail: zhaoshen_nudt@163.com

廖一霏 (2000—), 女, 研究生, 研究方向为导航时空信息安全. E-mail: liaoyifeifeifei@163.com

李世玲 (1991—), 女, 博士, 研究方向为多智能体系统非合作博弈. E-mail: lishilingjjwai@163.com

周开军 (1979—), 男, 教授, 研究方向为仿生视觉信息处理、生物特征识别. E-mail: zkj@hutb.edu.cn

Research on GNSS spoofing interference detection for multi-correlator combined power

ZHAO Shen[1,2], LIAO Yifei[1], LI Shiling[1,2], ZHOU Kaijun[1,2]

(1. *College of Intelligent Engineering and Intelligent Manufacturing*, *Hunan University of Technology and Business*, *Changsha* 410205, *China*; 2. *Xiangjiang Laboratory*, *Changsha* 410205, *China*)

Abstract: Global Navigation Satellite System (GNSS) civil signals are vulnerable to external spoofing because of their openness and vulnerability. As an effective method for spoofing detection, Signal Quality Monitoring (SQM) monitors the correlation results of early code, late code and phase code (ELP) after the receiver's tracking loop, and compares them with the correlation characteristics without spoofing to determine whether spoofing interference exists. The conventional SQM algorithm uses only three ELP information and the detection performance is limited. Therefore, a multi-correlator combined power algorithm is proposed. The weight of the output power of multiple equally spaced correlators between ELP is taken as the detection quantity, and the inverse ratio of the correlation time and the real-time code time difference is taken as the weighting coefficient. The probability distribution characteristics of the detected quantity were further analyzed, and the optimal detection threshold was determined based on the Neyman-Pearson theory. By comparing the detected quantity and the detection threshold, the existence of deception interference was determined. Based on the Scenario 4 set published by the University of Texas, the test results show that compared with typical SQM algorithms such as Ratio and ELP, the proposed algorithm has both high detection probability and fast early warning response time under different false alarm rates.

Keywords: satellite navigation; deceptive interference; code tracking loop; signal quality monitoring; Multi-correlator