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

基于牛顿迭代法的GNSS欺骗干扰参数估计

王佳奇，唐小妹，孙广富

GNSS spoofing signal parameters estimation based on Newton's method

WANG Jiaqi, TANG Xiaomei, and SUN Guangfu

引用本文:
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. DOI: 10.12265/j.gnss.2022171
WANG Jiaqi, TANG Xiaomei, SUN Guangfu. GNSS spoofing signal parameters estimation based on Newton's method[J]. Gnss World of China, 2022, 47(6): 86–90. DOI: 10.12265/j.gnss.2022171

在线阅读 View online: https://doi.org/10.12265/j.gnss.2022171

DOI: 10.12265/j.gnss.2022171

基于牛顿迭代法的 GNSS 欺骗干扰参数估计

王佳奇, 唐小妹, 孙广富
(国防科技大学 电子科学学院, 长沙 410073)

摘 要: 欺骗干扰是全球卫星导航系统 (GNSS) 发展面临的重要挑战, 针对小时延场景下欺骗干扰参数估计方法计算量大的问题, 提出了一种基于牛顿迭代法的参数估计方法. 该方法以码相位估计为核心, 通过构建欺骗场景下信号参数的非线性估计模型, 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. 实验结果表明: 该方法的平均迭代次数在 10 次左右, 相比于传统参数估计方法, 算法有效性大幅提升. 在准确性方面, 该方法能够有效提高小时延场景下的信号参数估计精度.

关键词: 全球卫星导航系统 (GNSS); 欺骗干扰; 参数估计; 牛顿迭代法; 最大似然估计 (MLE)

中图分类号: P228.4 **文献标志码:** A **文章编号:** 1008-9268(2022)06-0086-05

0 引 言

安全性是全球卫星导航系统 (GNSS) 发展的重要方向, 由于 GNSS 信号的落地电平微弱, 信号体制公开且向后兼容[1], GNSS 接收机很容易在捕获或跟踪阶段收敛至功率较高的欺骗信号[2-3]. 高级欺骗干扰通过在时延域、频率域和功率域的同步, 能够在不被预警的前提下拉偏目标接收机的定位授时结果, 是目前导航对抗技术研究的热点问题[4]. GNSS 作为时空信息的基准传感器, 若被敌方控制, 会在交通、电力以及通信等基础领域造成严重损失[5-6].

欺骗干扰参数估计是干扰监测系统的重要发展方向, 其可以为关键区域的接收机提供欺骗干扰的参数和攻击策略等先验信息, 为进一步的欺骗抑制提供信息支撑. 目前高级欺骗干扰的参数估计方法主要依据统计信号的估计理论, 对未知参数进行联合估计. 这类技术一般基于相关函数的观测曲线, 利用最大似然估计 (MLE) 法对信号参数进行估计[7]. 参数估计的 MLE 准则等价于在码相位监测空间中寻找子空间, 使接收信号到达子空间的距离最小. 传统 MLE 方法一般采用网格搜索的方式对信号码相位进行遍历, 信号幅度采用最小二乘法进行估计, 该方法估计精度较高, 但是估计过程需要遍历码相位子空间, 计算量较大[8-9]. 多径估计延迟锁定环路 (MEDLL) 技术基于 MLE 准则, 采用迭代方法对信号参数进行估计, 但是受噪声影响较为明显, 适用场景受限[10-11].

针对传统 MLE 参数估计技术需要的计算量较大这一问题, 本文根据信号参数的 MLE 准则和观测方程, 提出基于牛顿迭代法的 GNSS 欺骗干扰参数估计技术, 能够在小时延欺骗干扰场景下准确、有效估计出欺骗信号和真实信号的参数, 并通过仿真实验对算法的有效性进行了验证.

1 参数估计的 MLE 准则

1.1 信号模型

考虑单路伪码通道的基带信号参数估计情况, 忽略数据码的影响, GNSS 基带信号的表达式为

$$\begin{aligned} r(t) &= a_1 c(t-\tau_1)\mathrm{e}^{j\varphi_1} + a_2 c(t-\tau_2)\mathrm{e}^{j\varphi_2} + n(t) \\ &= \rho_1 c(t-\tau_1) + \rho_2 c(t-\tau_2) + n(t). \end{aligned} \tag{1}$$

式中: ρ 与信号的幅度和载波相位相关, 满足 $\rho_i = a_i\mathrm{e}^{j\varphi_i}$; a_i、τ_i 和 φ_i 分别表示第 i 路信号的幅度、码相位和载波相位, 其中 $i=1$ 表示真实信号, $i=2$ 表示欺骗信号; $n(t)$ 表示功率谱密度为 N_0 的高斯白噪声 (WGN); $c(t)$ 为 GNSS 信号的扩频码, 其理想自相关特性满足

$$R_0(\tau) = \frac{1}{T}\int_0^T c(t)c(t-\tau)\mathrm{d}t = \begin{cases} 1-\dfrac{|\tau|}{T_c}, & |\tau| \leqslant T_c \\ 0, & |\tau| > T_c \end{cases}. \tag{2}$$

式中, T_c 为扩频码码片的持续时间.

收稿日期: 2022-09-23
资助项目: 国家自然科学基金资助项目 (U20A0193)
通信作者: 唐小妹 E-mail: txm_nnc@126.com

1.2　MLE 估计值

在高斯噪声的情况下, 信号参数集$\theta=\{\tau_1,\tau_2,\rho_1,\rho_2\}$对应的似然函数为

$$P(r,\theta)=\exp\left\{-\frac{1}{2\sigma^2}\int_0^T|r(t)-r_1(t)-r_2(t)|^2\mathrm{d}t\right\}. \quad (3)$$

式中, $r_i(t)=\rho_i c(t-\tau_i)$, 即对真实信号和欺骗信号的估计. 式 (3) 取对数, 并经过复数模平方的运算转换, 可得对数似然函数的表达式为

$$\begin{aligned}L(r,\theta)=&-\int_0^T|r(t)|^2\mathrm{d}t+2\mathrm{Re}\left\{\rho_1^*\int_0^T r(t)c(t-\tau_1)\mathrm{d}t\right\}-\\&T|\rho_1|^2+2\mathrm{Re}\left\{\rho_2^*\int_0^T r(t)c(t-\tau_2)\mathrm{d}t\right\}-\\&T|\rho_2|^2-2\mathrm{Re}\{\rho_1\rho_2^*\}\int_0^T c(t-\tau_1)c(t-\tau_2)\mathrm{d}t. \quad (4)\end{aligned}$$

式中, 第二项和第四项为相关函数的观测值, 可在跟踪过程中采用多相关器架构得到. 考虑伪码的自相关特性, 代入式 (2), 式 (4) 可以简化为

$$\begin{aligned}L(r,\theta)=&-\int_0^T|r(t)|^2\mathrm{d}t-T|\rho_1|^2-T|\rho_2|^2+\\&2\mathrm{Re}\{\rho_1^*R(\tau_1)\}+2\mathrm{Re}\{\rho_2^*R(\tau_2)\}-\\&2T\mathrm{Re}\{\rho_1\rho_2^*\}R_0(\tau_1-\tau_2). \quad (5)\end{aligned}$$

对似然函数求偏导, 参数τ_1、ρ_1对应的偏导数为:

$$\begin{aligned}\frac{\partial L(r,\theta)}{\partial\tau_1}=&2\mathrm{Re}\left\{\rho_1^*\frac{\partial R(\tau_1)}{\partial\tau_1}\right\}-2T\mathrm{Re}\{\rho_1\rho_2^*\}\frac{\partial R_0(\tau_1-\tau_2)}{\partial\tau_1}\\=&2\mathrm{Re}\left\{\rho_1^*\frac{\partial}{\partial\tau_1}(R(\tau_1)-T\rho_2R_0(\tau_1-\tau_2))\right\}\\=&2\mathrm{Re}\left\{\rho_1^*\frac{\partial}{\partial\tau_1}\int_0^T[r(t)-\rho_2c(t-\tau_2)]c(t-\tau_1)\mathrm{d}t\right\},\end{aligned} \quad (6)$$

$$\frac{\partial L(r,\theta)}{\partial\rho_1}=2[R^*(\tau_1)-T\rho_1^*-T\rho_2^*R_0(\tau_1-\tau_2)]. \quad (7)$$

令$\frac{\partial L(r,\theta)}{\partial\tau_1}=0$、$\frac{\partial L(r,\theta)}{\partial\rho_1}=0$, 且相关域观测值关于 T 归一化, 可得信号$r_1(t)$参数的 MLE 值为

$$\begin{cases}\hat\tau_1=\max\limits_{\hat\tau_1}\left(\mathrm{Re}\left\{[R(\hat\tau_1)-\hat\rho_2R_0(\hat\tau_1-\hat\tau_2)]\mathrm{e}^{-j\hat\varphi_1}\right\}\right)\\\hat\rho_1=R(\hat\tau_1)-\hat\rho_2R_0(\hat\tau_1-\hat\tau_2)\end{cases}. \quad (8)$$

同理, 可得信号$r_2(t)$参数的 MLE 值为

$$\begin{cases}\hat\tau_2=\max\limits_{\hat\tau_2}\left(\mathrm{Re}\left\{[R(\hat\tau_2)-\hat\rho_1R_0(\hat\tau_2-\hat\tau_1)]\mathrm{e}^{-j\hat\varphi_2}\right\}\right)\\\hat\rho_2=R(\hat\tau_2)-\hat\rho_1R_0(\hat\tau_2-\hat\tau_1)\end{cases}. \quad (9)$$

2　基于牛顿迭代的参数估计方法

2.1　观测模型

对于 GNSS 信号而言, 噪声水平远高于信号功率, 需要通过相关运算提取信号的相关函数观测值来进行参数估计. 以跟踪环路的本地码相位为中心, 采用多相关器架构, 监测左右 M 码片, 则相关器输出可表示为

$$R(\boldsymbol{\delta})=\boldsymbol{H}(\boldsymbol{\tau})\boldsymbol{\rho}(\boldsymbol{a},\boldsymbol{\varphi})+\boldsymbol{\eta}. \quad (10)$$

式中: $\boldsymbol{\delta}=[-M,-M+\Delta\delta,\cdots,M-\Delta\delta,M]^{\mathrm{T}}\cdot T_c$, $\Delta\delta$为相邻相关器间隔; $R(\boldsymbol{\delta})$为实际观测得到的相关函数; $\boldsymbol{\tau}$为信号分量与本地信号的码相位差, 简称为码相位; $\boldsymbol{H}(\boldsymbol{\tau})$为观测矩阵, 在高级欺骗干扰场景下, 单路通道内一般只有一路欺骗信号, 因而其表达式为

$$\boldsymbol{H}(\boldsymbol{\tau})=\begin{bmatrix}R_0(\delta_1-\tau_1),\cdots,R_0(\delta_n-\tau_1)\\R_0(\delta_1-\tau_2),\cdots,R_0(\delta_n-\tau_2)\end{bmatrix}^{\mathrm{T}}. \quad (11)$$

$\boldsymbol{\rho}(\boldsymbol{a},\boldsymbol{\varphi})$取决于信号分量的幅度和载波相位, 其中$\boldsymbol{a}=[a_1,a_2]$, $\boldsymbol{\varphi}=[\varphi_1,\varphi_2]$, 则有

$$\boldsymbol{\rho}(\boldsymbol{a},\boldsymbol{\varphi})=\left[a_1\mathrm{e}^{j\varphi_1},a_2\mathrm{e}^{j\varphi_2}\right]^{\mathrm{T}}. \quad (12)$$

为方便说明, 本节将$\rho_i=a_i\mathrm{e}^{j\varphi_i}$称为幅度.

信号参数的 MLE 准则等价于在$\boldsymbol{H}(\boldsymbol{\tau})$的列向量中寻找二维子空间, 使观测向量$R(\boldsymbol{\delta})$向子空间投影的残差最小. 相应地可采用网格搜索的方式对信号码相位进行估计, 搜索方式如图 1 所示[8].

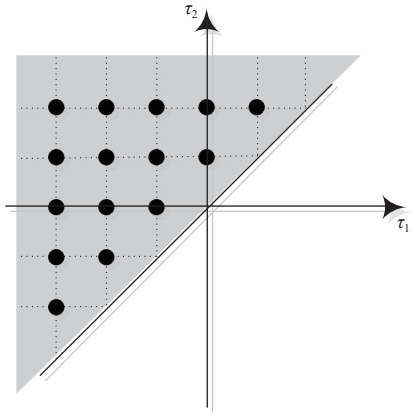

图 1　信号码相位的网格搜索

MEDLL 技术主要以迭代运算的形式来实现对信号功率、码相位和载波相位的估计. 两种方法的具体实施过程分别参考文献 [7, 12].

2.2　算法模型

式 (10) 所示的观测模型, 可以用以下一个非线性函数来描述

$$R(\boldsymbol{\delta})=f(\tau_1,\tau_2,\rho_1,\rho_2,\boldsymbol{\delta}). \quad (13)$$

为减小噪声对信号参数估计的影响, 信号幅度采用最小二乘法进行估计, 估计过程为

$$\hat{\boldsymbol{\rho}}=\left[\boldsymbol{H}^{\mathrm{T}}(\hat{\boldsymbol{\tau}})\boldsymbol{Q}^{-1}\boldsymbol{H}(\hat{\boldsymbol{\tau}})\right]^{-1}\boldsymbol{H}^{\mathrm{T}}(\hat{\boldsymbol{\tau}})\boldsymbol{Q}^{-1}R(\boldsymbol{\delta}). \quad (14)$$

式中，$\boldsymbol{Q}$为 Toeplitz 矩阵，窄距相关器输出的噪声具有相关性，矩阵元素为$Q_{a,b}=R(|a-b|\Delta\delta)$[13].

进而式 (13) 可以简化为

$$R(\boldsymbol{\delta})=f(\tau_1,\tau_2,\boldsymbol{\delta}). \tag{15}$$

假设解的初始值为$(\tau_1^{k-1},\tau_2^{k-1})$，信号幅度$(\rho_1^{k-1},\rho_2^{k-1})$通过式 (14) 进行计算. 以式 (15) 的第 n 个方程为例，该方程在该点处线性化的泰勒展开式为

$$\begin{aligned}R(\delta_n)=&f\left(\tau_1^{k-1},\tau_2^{k-1},\delta_n\right)+\\&\frac{\partial f(\tau_1^{k-1},\tau_2^{k-1},\delta_n)}{\partial\tau_1}\left(\tau_1-\tau_1^{k-1}\right)+\\&\frac{\partial f(\tau_1^{k-1},\tau_2^{k-1},\delta_n)}{\partial\tau_2}\left(\tau_2-\tau_2^{k-1}\right).\end{aligned} \tag{16}$$

式中，$\dfrac{\partial f(\tau_1^{k-1},\tau_2^{k-1},\delta_n)}{\partial\tau_1}$表示非线性函数$f(\tau_1,\tau_2,\delta_n)$在点$(\tau_1^{k-1},\tau_2^{k-1})$对$\tau_1$的偏导，可以表示为

$$\frac{\partial f(\tau_1^{k-1},\tau_2^{k-1},\delta_n)}{\partial\tau_1}=\rho_1^{k-1}\left.\frac{\partial R_0(\tau_1-\tau_1^{k-1})}{\partial\tau_1}\right|_{\tau_1=\delta_n}. \tag{17}$$

相应地，式 (13) 可以近似转换为线性方程组

$$\boldsymbol{G}\cdot\Delta\boldsymbol{x}=\boldsymbol{b}. \tag{18}$$

其中：

$$\boldsymbol{G}=\begin{bmatrix}\rho_1^{k-1}\left.\dfrac{\partial R_0(\tau_1-\tau_1^{k-1})}{\partial\tau_1}\right|_{\tau_1=\delta_1} & \rho_2^{k-1}\left.\dfrac{\partial R_0(\tau_2-\tau_2^{k-1})}{\partial\tau_2}\right|_{\tau_2=\delta_1}\\ \rho_1^{k-1}\left.\dfrac{\partial R_0(\tau_1-\tau_1^{k-1})}{\partial\tau_1}\right|_{\tau_1=\delta_2} & \rho_2^{k-1}\left.\dfrac{\partial R_0(\tau_2-\tau_2^{k-1})}{\partial\tau_2}\right|_{\tau_2=\delta_2}\\ \vdots & \vdots\\ \rho_1^{k-1}\left.\dfrac{\partial R_0(\tau_1-\tau_1^{k-1})}{\partial\tau_1}\right|_{\tau_1=\delta_n} & \rho_2^{k-1}\left.\dfrac{\partial R_0(\tau_2-\tau_2^{k-1})}{\partial\tau_2}\right|_{\tau_2=\delta_n}\end{bmatrix}, \tag{19}$$

$$\Delta\boldsymbol{x}=[\tau_1,\tau_2]^{\mathrm{T}}-\left[\tau_1^{k-1},\tau_2^{k-1}\right]^{\mathrm{T}}, \tag{20}$$

$$\boldsymbol{b}=R(\boldsymbol{\delta})-f(\tau_1,\tau_2,\boldsymbol{\delta}). \tag{21}$$

相应地，$\Delta\boldsymbol{x}$可用最小二乘法进行计算，其计算式为

$$\Delta\boldsymbol{x}=\mathrm{Re}\left\{\left(\boldsymbol{G}^{\mathrm{T}}\boldsymbol{G}\right)^{-1}\boldsymbol{G}^{\mathrm{T}}\boldsymbol{b}\right\}. \tag{22}$$

进而非线性方程组的解可以表示为

$$\boldsymbol{x}_k=\boldsymbol{x}_{k-1}+\Delta\boldsymbol{x}. \tag{23}$$

基于牛顿迭代的 MLE 参数估计算法流程如下：

1) 状态参量初始化，给出解的初始值(τ_1^0,τ_2^0)，并根据式 (14) 计算(ρ_1^0,ρ_2^0)，迭代次数 k 初始值设置为 1；

2) 计算雅可比矩阵$\boldsymbol{G}$和估计误差向量$\boldsymbol{b}$；

3) 根据式 (22)~(23) 得到解的更新值(τ_1^k,τ_2^k)，并计算(ρ_1^k,ρ_2^k)；

4) 迭代次数 $k=k+1$，重复进行步骤 2)~3)，直至满足预设条件

$$\left|\hat{\tau}_1^k-\hat{\tau}_1^{k-1}\right|\leqslant 5\times10^{-3},\left|\hat{\tau}_2^k-\hat{\tau}_2^{k-1}\right|\leqslant 5\times10^{-3}. \tag{24}$$

为方便比较，实验过程设置码相位分辨率$\Delta\delta=0.05$，码相位监测区间为±3 个码片，即 $M=3$；码相位估计的初始值设置为$(\tau_1^0,\tau_2^0)=(-0.5,0.5)$.

3 仿真性能分析

为了评估本节算法的有效性，采用蒙特卡洛仿真方法，分析欺骗信号与真实信号不同码相位偏差$\Delta\tau$下的参数估计性能. 蒙特卡洛仿真次数设置为 1 000，假设欺骗信号与真实信号的载波相位在区间$[-\pi,\pi]$均匀分布，真实信号的码相位在区间$[-\Delta\delta/2,\Delta\delta/2]$均匀分布，设置欺骗信号的功率高于真实信号 3 dB，即相对幅度为 1.41，相干积分之后的信噪比 (SNR) 为 20 dB. 由算法模型可知，码相位估计是信号参数估计过程中的核心，故以码相位估计结果为例，对应的参数估计均方根误差 (RMSE) 和偏差如图 2~3 所示.

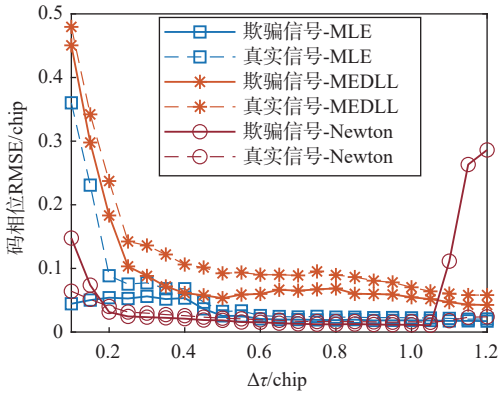

图 2 信号码相位的估计精度 (SNR=20 dB)

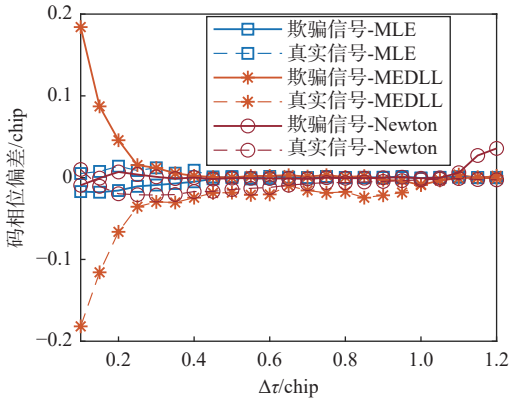

图 3 信号码相位估计的偏差 (SNR=20 dB)

从图中可以看到，欺骗信号的码相位偏差$\Delta\tau$越小，参数估计的难度越大. MEDLL 技术在码相位偏

差$\Delta\tau<0.3$码片的情况下，估计结果有偏，而传统 MLE 估计方法和本文提出的基于牛顿迭代的 MLE 改进方法的估计结果基本无偏. 在估计精度方面，由于牛顿迭代过程并不局限于码相位监测点的位置，即算法分辨率受相关器间隔的影响较小，本文算法在$\Delta\tau<1$码片时的参数估计精度要高于基于网格搜索的传统 MLE 参数估计法. 需要注意的是，在$\Delta\tau>1$码片的情况下，本文算法对欺骗信号码相位的估计结果开始出现偏差，这与初始值的选取有关，此时牛顿迭代法容易收敛至局部最优解.

进一步对算法计算量进行分析，保持仿真参数不变，不同码相位偏差$\Delta\tau$下本文算法的迭代次数如图 4 所示. 从整体上而言，在 SNR 为 20 dB 的条件下，不同码相位偏差下的迭代次数，即信号码相位的搜索次数小于 10. 传统 MLE 参数估计方法基于网格搜索对信号码相位进行估计，其搜索次数为$(2M/\Delta\delta)(2M/\Delta\delta-1)/2$，与其相比，本文算法的计算量大大减小.

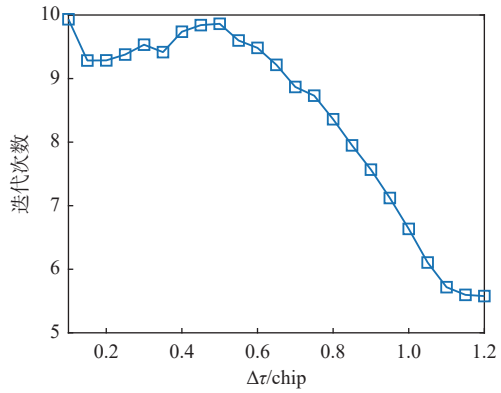

图 4　迭代次数

进一步评估 SNR 对算法估计性能的影响，设置相关后的 SNR 分别为 15 dB、20 dB、30 dB，其他仿真参数不变，欺骗信号码相位的估计结果和算法迭代次数如图 5~7 所示.

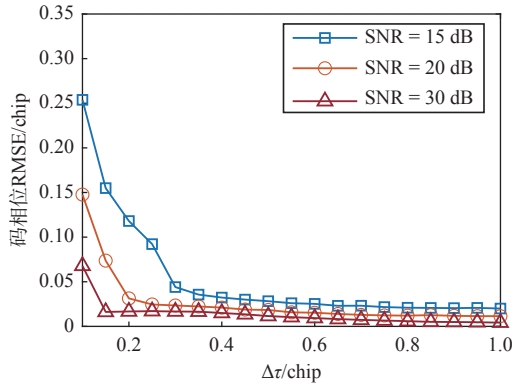

图 5　不同 SNR 条件下的欺骗码相位参数估计精度

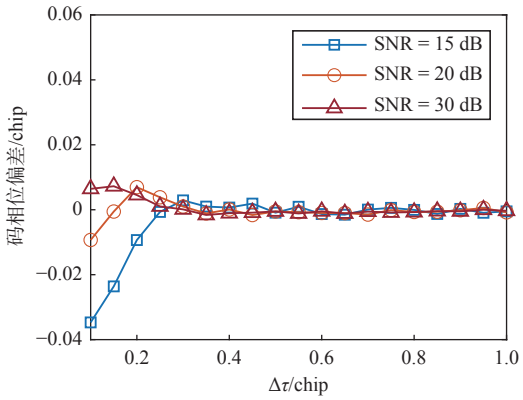

图 6　不同 SNR 条件下的欺骗码相位参数估计偏差

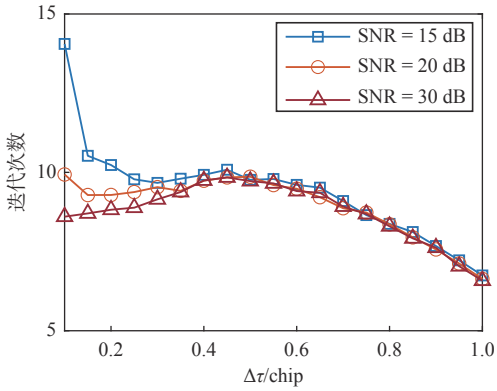

图 7　不同 SNR 条件下的迭代次数

从图中可以看到，噪声对码相位偏差$\Delta\tau<0.3$码片情况下的参数估计影响较大，随着 SNR 下降，欺骗信号的码相位估计值出现微小的偏差，参数估计精度也随之下降，同时算法的迭代次数上升. 由式 (14) 和式 (21) 可知，噪声直接影响信号幅度估计值和参量的更新过程，进而导致迭代次数增加以及信号码相位估计的准确度下降. 值得注意的是，噪声对$\Delta\tau>0.3$码片情况下的参数估计过程影响较小.

4　结　论

本文在参数估计的 MLE 准则下，提出了一种基于牛顿迭代的码相位快速搜索方法，能够有效地应用于码相位偏差$\Delta\tau$小于 1 码片的小时延欺骗干扰场景. 实验结果表明，该方法不局限于相关函数观测点的位置，能够有效提高信号参数的估计精度，参数估计精度要优于传统 MLE 方法和 MEDLL 技术. 在计算量方面，在 SNR 为 20 dB 的情况下，算法的平均迭代次数基本在 10 次以内，相比于传统 MLE 方法基于网格搜索遍历参数空间，本文算法在参数域的搜索次数明显下降，提高了参数估计算法在实际应用中的有效性.

参考文献

[1] JAFARNIA-JAHROMI A, BROUMANDAN A, NIELSEN J, et al. GPS vulnerability to spoofing threats and a review of anti-spoofing techniques[J]. International journal of navigation and observation, 2012(9): 1-16. DOI: 10.1155/2012/127072

[2] JAHROMI J. A GNSS signal authenticity verification in the presence of structural interference [D]. Calgary: University of Calgary, 2013.

[3] MA C, YANG J, CHEN J Y, et al. Effects of a navigation spoofing signal on a receiver loop and a UAV spoofing approach[J]. GPS solutions, 2020, 24(3): 1-13. DOI: 10.1007/s10291-020-00986-z

[4] PSIAKI M L, HUMPHREYS T E. GNSS spoofing and detection[J]. Proceedings of the IEEE, 2016, 104(6): 1258-1270. DOI: 10.1109/JPROC.2016.2526658

[5] SHEPARD D P, HUMPHREYS T E. Characterization of receiver response to a spoofing attacks[C]//The 24th International Technical Meeting of the Satellite Division of the Institute of Navigation, 2011: 2608-2618.

[6] BHATTI J, HUMPHREYS T E. Hostile control of ships via false GPS signals: demonstration and detection[J]. NAVIGATION: Journal of the institute of navigation, 2017, 64(1): 51-66. DOI: 10.1002/navi.183

[7] 徐成涛. 基于统计模型的多径误差评估和现代导航信号多径抑制技术研究[D]. 长沙: 国防科学技术大学, 2016.

[8] BLANCO-DELGADO N, NUNES F D. Multipath estimation in multicorrelator GNSS receivers using the maximum likelihood principle[J]. IEEE transactions on aerospace and electronic systems, 2012, 48(4): 3222-3233. DOI: 10.1109/TAES.2012.6324696

[9] SHANG X Y, SUN F P, ZHANG L D, et al. Detection and mitigation of GNSS spoofing via the pseudorange difference between epochs in a multicorrelator receiver[J]. GPS solutions, 2022, 26(2): 1-14. DOI: 10.1007/s10291-022-01224-4

[10] VAN NEE R D J. The multipath estimating delay lock loop[C]// IEEE Second Symposium on Spread Spectrum Techniques and Applications, 1992: 39-42. DOI: 10.1109/ISSSTA.1992.665623

[11] 叶锦宇, 寇艳红. 基于MEDLL的分级搜索抗多径算法[J]. 北京航空航天大学学报, 2016, 42(6): 1228-1235.

[12] 王佳奇, 孙广富, 唐小妹, 等. 基于NELDER-MEAD的GNSS欺骗干扰参数估计方法[J/OL]. (2022-08-04) [2022-09-22]. http://kns.cnki.net/kcms/detail/11.2406.TN.20220803.1653.010.html

[13] GROSS J N, KILIC C, HUMPHREYS T E. Maximum-likelihood power-distortion monitoring for GNSS-signal authentication[J]. IEEE transactions on aerospace and electronic systems, 2019, 55(1): 469-475. DOI: 10.1109/TAES.2018.2848318

作者简介

王佳奇 (1997—), 男, 硕士, 研究方向为卫星导航对抗技术.

唐小妹 (1982—), 女, 博士, 研究员, 研究方向为卫星导航信号处理技术和接收机设计.

孙广富 (1970—), 男, 博士, 研究员, 研究方向为卫星导航信号接收技术.

GNSS spoofing signal parameters estimation based on Newton's method

WANG Jiaqi, TANG Xiaomei, SUN Guangfu

(*College of Electronic Science and Technology*, *National University of Defense Technology*, *Changsha* 410073, *China*)

Abstract: Spoofing interference is a major threat to the development of Global Navigation Satellite System (GNSS) applications. In order to solve the large computation resource consumption problem of estimation methods, this paper proposed a spoofing signal parameters estimation method based on Newton's method. This method constructed a nonlinear estimation model of signal parameters in the spoofing scenario, taking the estimation of code phases as the core. The code phases were iterated by Newton's method, and the signal amplitudes and carrier phases were estimated by the least square method. The simulation results showed that the average number of iterations was about 10, greatly improving the effectiveness of signal parameters estimation compared with the traditional estimation method. Moreover, this method could also improve the estimation accuracy in the small delay scenarios.

Keywords: Global Navigation Satellite System (GNSS); spoofing interference; parameter estimation; Newton's method; maximum likelihood estimation (MLE)