利用信号重构的全球导航卫星系统欺骗干扰抑制方法

卢 丹* 白天霖

(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：欺骗式干扰通过发射与真实卫星信号相似的信号误导接收机产生错误的定位结果，具有极大的危害。该文针对转发式欺骗干扰，提出一种基于信号重构的单天线欺骗干扰抑制方法。该方法首先通过参数估计方法估计出欺骗信号载波频率和码相位，然后构建欺骗信号子空间正交投影矩阵以抑制干扰。仿真实验结果表明该方法对欺骗干扰具有良好的抑制效果，能够保障接收机在干扰环境中实现有效定位，并具有较低的运算复杂度。

关键词：卫星导航；欺骗式干扰；信号重构；干扰抑制

中图分类号：TN967.1 **文献标识码**：A **文章编号**：1009-5896(2020)05-1268-06

DOI: 10.11999/JEIT190321

Global Navigation Satellite System Spoofing Mitigation Method by Utilizing Signal Reconstruction

LU Dan BAI Tianlin

(*Tianjin Key Laboratory for Advanced Signal Processing*, *Civil Aviation University of China*, *Tianjin* 300300, *China*)

Abstract: Spoofing misleads the receiver to generate the wrong position information by trans-mitting signals similar to authentic satellite signals, which has great harm. In this paper, a single-antenna spoofing mitigation algorithm based on signal reconstruction is proposed for meaconing. Firstly, the carrier frequency and code phase of spoofing signal are obtained by parameter estimation method, and then the orthogonal projection matrix of spoofing signal subspace is constructed to suppress spoofing. The simulation results show that the algorithm has a good suppression effect on spoofing and ensure the receiver can locate effectively in the interference environment, and the algorithm also has lower computational complexity.

Key words: Satellite navigation; Spoofing; Signal reconstruction; Interference suppression

1 引言

全球导航卫星系统(Global Navigation Satellite System, GNSS)在日常生活和军事领域的应用广泛，在物联网，智慧城市建设等关键任务中担当着重要角色。但GNSS信号发射功率只有几十瓦，到达地面接收机时非常微弱，极易受到外界各类干扰的影响[1]。其中欺骗式干扰与真实卫星信号相似，能使接收机在毫无意识的情况下产生错误的定位结果，干扰隐蔽性强，危害极大。因此，需要针对欺骗式干扰的特点研究有效的抗干扰方法。

欺骗式干扰可以分为两大类：转发式和生成式。其中生成式欺骗干扰是由欺骗设备产生与真实GNSS信号格式一致的欺骗信号，再由发射设备发射出去。这种方式技术相对复杂，实现难度较大。而转发式干扰是干扰机先接收真实GNSS信号，经过延时、放大后再发射出去，以此来欺骗目标接收机，这种技术复杂度低，容易实现，本文主要讨论转发式干扰。

现有的抗欺骗干扰技术分为欺骗式干扰检测和欺骗式干扰抑制[2]。其中，欺骗检测技术是目前抗欺骗干扰的主要手段，主要包括信号功率检测[3]，信号空间特性检测[4,5]和基于信号质量监视的检测技术[6,7]等。欺骗信号在攻击接收机时，可以在接收机天线处产生零陷信号从而抑制真实信号，但这是极其困难的[8,9]，因此欺骗信号和真实信号会同时存在，欺骗干扰检测技术通过监测信号特征的异常变化识别出欺骗信号[10]，但不对欺骗信号做进一步处理，如果重新捕获卫星信号仍会受到欺骗，不能完成正确的定位解算。而欺骗式干扰抑制技术旨在消除欺骗干扰，它可以与欺骗检测技术相结合，使接收机能够在干扰环境下捕获跟踪真实卫星信号以得到正确的定位结果。目前研究较多的欺骗抑制技术是基于多天线的，利用波束控制和零陷控制抑

收稿日期：2019-05-06；改回日期：2019-11-30；网络出版：2019-12-17
*通信作者： 卢丹 dlu@cauc.edu.cn

制欺骗干扰[11,12]，但阵列天线技术成本和复杂度较高，适用场景有限。可见这些抗欺骗技术都不是全能的，每种方法都有其局限性，因此将多种方法结合能应对多样欺骗，但这势必增加抗欺骗的计算量，一次成功的欺骗检测可能花费数小时的离线计算[13]，这在实际应用中是不合理的，因此需要研究快速有效的抗欺骗手段。文献[14]提出了一种独立于天线个数的欺骗干扰抑制算法，可以应用在单天线接收机中，其通过捕获跟踪得到欺骗信号的载频和时延后，通过子空间投影抑制干扰后再次捕获跟踪用以定位解算，由于需要两次捕获，该算法计算量较大。本文利用一种参数估计方法替代捕获跟踪，用以估计欺骗信号载频和时延，降低了算法的复杂度和运算量，然后构建欺骗信号子空间正交投影矩阵以消除欺骗信号，进而使接收机捕获跟踪真实卫星信号并产生正确的定位结果。

2　数据模型

针对转发式欺骗干扰，假设接收机天线接收到M个真实卫星信号和M个欺骗信号，则下变频后的中频信号可以表示为

$$x_{\mathrm{IF}}(t)=x_{\mathrm{a}}(t)+x_{\mathrm{s}}(t)+e(t) \tag{1}$$

其中，$e(t)$表示高斯白噪声，$x_{\mathrm{a}}(t)$和$x_{\mathrm{s}}(t)$分别表示真实信号和欺骗信号，表达式为

$$x_{\mathrm{a}}(t)=\sum_{m=1}^{M}\alpha_{\mathrm{a}}^{m}d^{m}(t-\tau_{\mathrm{a}}^{m})c^{m}(t-\tau_{\mathrm{a}}^{m})\mathrm{e}^{\mathrm{j}(\omega_{\mathrm{a}}^{m}t+\theta_{\mathrm{a}}^{m})} \tag{2}$$

$$x_{\mathrm{s}}(t)=\sum_{m=1}^{M}\alpha_{\mathrm{s}}^{m}d^{m}(t-\tau_{\mathrm{s}}^{m})c^{m}(t-\tau_{\mathrm{s}}^{m})\mathrm{e}^{\mathrm{j}(\omega_{\mathrm{s}}^{m}t+\theta_{\mathrm{s}}^{m})} \tag{3}$$

其中，下标a和s分别代表真实信号和欺骗信号，$d(t)$表示导航电文，$c(t)$表示卫星信号的C/A码，α,τ,ω和θ分别表示信号的幅度、时延、载波频率(中频)和载波相位。

式(1)中信号经过A/D采样后得到数字中频信号，可用矩阵形式表示为

$$\boldsymbol{X}_{\mathrm{IF}}=\boldsymbol{X}_{\mathrm{A}}+\boldsymbol{X}_{\mathrm{S}}+\boldsymbol{e} \tag{4}$$

其中，$\boldsymbol{X}_{\mathrm{IF}}=[x_{\mathrm{IF}}(t_1),x_{\mathrm{IF}}(t_2),\cdots,x_{\mathrm{IF}}(t_N)]^{\mathrm{T}}$，$\boldsymbol{e}=[e(t_1),e(t_2),\cdots,e(t_N)]^{\mathrm{T}}$表示高斯白噪声，$t_n$是第$n$次采样的时间，$N$是总样本点数。$\boldsymbol{X}_{\mathrm{S}}$是由$M$个欺骗信号组成，具体形式为

$$\boldsymbol{X}_{\mathrm{S}}=\boldsymbol{Q}_{\mathrm{S}}\boldsymbol{\alpha}_{\mathrm{S}}=\left[\boldsymbol{q}_{\mathrm{S}}^{1},\boldsymbol{q}_{\mathrm{S}}^{2},\cdots,\boldsymbol{q}_{\mathrm{S}}^{M}\right]\begin{bmatrix}\alpha_{\mathrm{s}}^{1}\\ \alpha_{\mathrm{s}}^{2}\\ \vdots\\ \alpha_{\mathrm{s}}^{M}\end{bmatrix} \tag{5}$$

定义$\boldsymbol{Q}_{\mathrm{S}}$为欺骗信号的基本数据矩阵，这里$\alpha_{\mathrm{s}}^{m}$是第$m$个欺骗信号的振幅，$\boldsymbol{q}_{\mathrm{S}}^{m}$是由第$m$个欺骗信号的导航电文，C/A码和载波3部分组成，定义为

$$\boldsymbol{q}_{\mathrm{S}}^{m}=\begin{bmatrix}d^{m}(t_1-\tau_{\mathrm{s}}^{m})c^{m}(t_1-\tau_{\mathrm{s}}^{m})\mathrm{e}^{\mathrm{j}(\omega_{\mathrm{s}}^{m}t_1+\theta_{\mathrm{s}}^{m})}\\ d^{m}(t_2-\tau_{\mathrm{s}}^{m})c^{m}(t_2-\tau_{\mathrm{s}}^{m})\mathrm{e}^{\mathrm{j}(\omega_{\mathrm{s}}^{m}t_2+\theta_{\mathrm{s}}^{m})}\\ \vdots\\ d^{m}(t_N-\tau_{\mathrm{s}}^{m})c^{m}(t_N-\tau_{\mathrm{s}}^{m})\mathrm{e}^{\mathrm{j}(\omega_{\mathrm{s}}^{m}t_N+\theta_{\mathrm{s}}^{m})}\end{bmatrix} \tag{6}$$

3　欺骗干扰抑制算法

接收机接收到卫星信号后，首先由欺骗检测模块检测当前信号是否受到欺骗干扰，若不存在欺骗干扰，则继续完成定位；若检测到欺骗干扰，则通过本文方法进行干扰抑制，消除干扰后接收机即可完成正确的导航定位。本文的干扰抑制方法主要分为两步，第1步是估计欺骗信号的关键参数(载频和时延)，重构欺骗信号，第2步通过子空间投影抑制干扰。算法流程如图1所示。本小节将首先介绍子空间投影的原理，然后引入欺骗信号的参数估计。

3.1　欺骗信号子空间投影

子空间投影是一种经典的信号处理方法[15]。在基于多天线的欺骗抑制方法中，利用信号的空间特征构建欺骗信号子空间[16]。为了摆脱天线个数的限制，考虑到GNSS信号是扩频信号，近似正交的扩频码也是构造子空间的理想元素，并且这种构建子

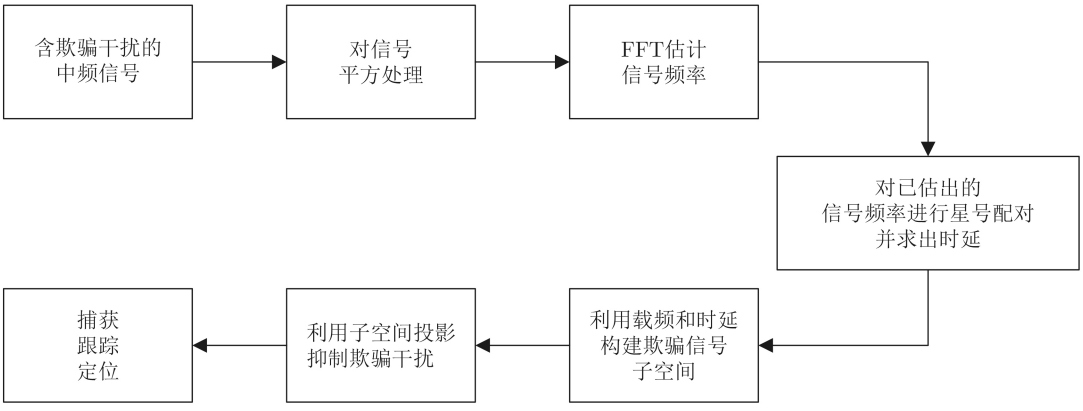


图 1 欺骗干扰抑制算法流程图

空间的方式是独立于接收天线个数的，因此可以用于单天线接收机中。

接收机利用欺骗信号的导航电文，载频和时延等参数，就可以根据式(6)构建欺骗信号的基本数据矩阵$\boldsymbol{Q}_{\mathrm{S}}$，进一步可以得到欺骗信号子空间正交投影矩阵

$$\boldsymbol{P}_{\perp}=\boldsymbol{Q}_{\mathrm{S}}\left(\boldsymbol{Q}_{\mathrm{S}}^{\mathrm{H}}\boldsymbol{Q}_{\mathrm{S}}\right)^{-1}\boldsymbol{Q}_{\mathrm{S}}^{\mathrm{H}} \tag{7}$$

则欺骗信号的零空间为

$$\boldsymbol{P}_{N}=\boldsymbol{I}-\boldsymbol{P}_{\perp} \tag{8}$$

将中频信号$\boldsymbol{X}_{\mathrm{IF}}$在欺骗信号零空间$\boldsymbol{P}_{N}$上投影，理论上可以将中频信号中的欺骗信号消除，达到欺骗抑制的效果

$$\begin{aligned}\boldsymbol{X}&=\boldsymbol{P}_{N}\boldsymbol{X}_{\mathrm{IF}}=(\boldsymbol{I}-\boldsymbol{P}_{\perp})\boldsymbol{X}_{\mathrm{IF}}\\&=\underbrace{(\boldsymbol{I}-\boldsymbol{P}_{\perp})\boldsymbol{X}_{\mathrm{A}}}_{\text{真实信号}}+\underbrace{(\boldsymbol{I}-\boldsymbol{P}_{\perp})\boldsymbol{X}_{\mathrm{S}}}_{\text{欺骗信号}}+\underbrace{(\boldsymbol{I}-\boldsymbol{P}_{\perp})\boldsymbol{n}}_{\text{噪声}}\\&=\underbrace{(\boldsymbol{I}-\boldsymbol{P}_{\perp})\boldsymbol{X}_{\mathrm{A}}}_{\text{真实信号}}+\underbrace{(\boldsymbol{I}-\boldsymbol{P}_{\perp})\boldsymbol{n}}_{\text{噪声}}\end{aligned} \tag{9}$$

由于PRN码的良好特性，不同PRN码所构成的空间近似正交，因此式(9)可以近似为

$$\begin{aligned}\boldsymbol{X}&=(\boldsymbol{I}-\boldsymbol{P}_{\perp})\boldsymbol{X}_{\mathrm{A}}+(\boldsymbol{I}-\boldsymbol{P}_{\perp})\boldsymbol{n}\\&\approx\boldsymbol{X}_{\mathrm{A}}+(\boldsymbol{I}-\boldsymbol{P}_{\perp})\boldsymbol{n}\end{aligned} \tag{10}$$

以上，通过子空间投影，欺骗信号被抑制，真实信号得到保留。子空间投影法的关键在于准确地重构欺骗信号，而这需要欺骗信号的导航电文、时延、载波频率和载波相位4个参数。然而，在一定条件下，可以证明导航电文和载波相位这两个参数不影响欺骗信号子空间正交投影矩阵的构建[14]，因此只需要估计欺骗信号的载频和时延用于构建投影矩阵。本文利用参数估计方法，得到欺骗信号的载频和时延的估计值。

3.2 欺骗信号载率和时延估计

由于卫星信号中导航电文和C/A码的存在，式(1)中每颗卫星的信号的频谱含有多个频率成分，不能直接通过傅里叶变换估计出信号含多普勒的载频，对式(1)的信号A/D转换后进行平方处理，把所有含噪声项合并为$e_1(n)$，可以得到

$$x_{\mathrm{IF}}^2(n)=x_{\mathrm{a}}^2(n)+x_{\mathrm{s}}^2(n)+2x_{\mathrm{a}}(n)x_{\mathrm{s}}(n)+e_1(n) \tag{11}$$

由于不同卫星信号的C/A码相关系数很小，相同卫星信号时延不同时，C/A码互相关系数也很小，并且信号和噪声是不相关的，所以这些乘积项的傅里叶分析结果接近0，将它们也并进噪声项$e_2(n)$。导航电文和C/A码取值为±1，因而式(11)可以简化为

$$\begin{aligned}x_{\mathrm{IF}}^2(n)=&\sum_{m=1}^{M}(\alpha_{\mathrm{a}}^{m})^2\mathrm{e}^{2\mathrm{j}(\omega_{\mathrm{a}}^{m}n+\theta_{\mathrm{a}}^{m})}\\&+\sum_{m=1}^{M}(\alpha_{\mathrm{s}}^{m})^2\mathrm{e}^{2\mathrm{j}(\omega_{\mathrm{s}}^{m}n+\theta_{\mathrm{s}}^{m})}+e_2(n)\end{aligned} \tag{12}$$

转发式欺骗干扰信号的信噪比一般比真实信号高3 dB以上，功率可能仍低于噪声，平方会让噪声更高，但是平方能够去除导航电文和C/A码对载波频率的影响，使信号只含有单一的频率分量，而且一方面欺骗源可能是多个，多个信号累加后干信比会增加，另一方面增加时域积累时间(FFT点数)，如采用20 ms或更长的信号，也能让信号频域峰值更高，得到明显高于噪声的峰值，这是以计算量的增加为代价的。另外每颗卫星信号的多普勒频移不同，因此可以在频谱上加以区分。式(12)中的信号傅里叶变换可以表示为

$$F(\omega)=\left|\sum_{n=-N/2}^{N/2-1}x_{\mathrm{IF}}^2(n)\mathrm{e}^{-\mathrm{j}\omega n}\right| \tag{13}$$

$F(\omega)$中前M个最大值所对应的ω，即为欺骗信号2倍载频所对应的频率估计值。通过FFT得到的$\hat{\omega}$的范围在$[-\pi,\pi]$之间，则信号载频估计值的范围在$[-\pi/2,\pi/2]$之间，然而信号载频ω真实值在$[-\pi,\pi]$之间，所以信号载频的真实估计值可能是$\hat{\omega}/2$或$\hat{\omega}/2+\pi$。因此在得到估计值$\hat{\omega}$后，需要进一步判断此频率是否正确。由于接收机的中频已知，卫星信号多普勒频移的范围一般在±10 kHz，可以借此确定真实的载频估计值。

然而，利用FFT求解频率的精度不高，不一定能满足子空间投影的需要。文献[14]中定义$\mu=\mathrm{SIR}_{\mathrm{out}}(\mathrm{dB})-\mathrm{SIR}_{\mathrm{in}}(\mathrm{dB})$为抗干扰增益，用来定量分析干扰抑制的效果，并且理论推导证明了其可表示为式(14)，μ越大，干扰抑制效果越好。

$$\mu=-10\lg\left[1-\mathrm{sinc}^2\left(\frac{\Delta fL}{f_{\mathrm{s}}}\right)\right] \tag{14}$$

式中，Δf为载频估计的误差，L为投影长度，即每L个采样点投影1次，f_{s}为采样频率，当采样频率为5.714 MHz时，可得图2。可以看到，当投影长度确定时，抗干扰增益和频率估计误差成反比。以投影长度L为100为例，若要求抗干扰增益大于20，频率估计误差应小于3000 Hz，此时FFT的精度能够满足。但如果欺骗干扰功率太大，需要较大的抗干扰增益，如40或60 dB，此时需要较高的频率估计精度要求，FFT不能满足，本文方法不再适用。但是，大功率欺骗很容易被检测出来，因此大多数转发式欺骗的功率只是略高于真实信号，本文方法

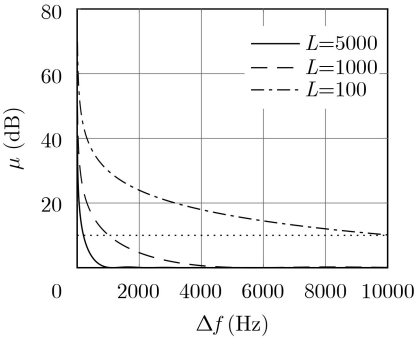


图 2 $\mu,\Delta f$以及度L的关系曲线图

仅针对这类小功率欺骗干扰，采用适当的投影长度(如L=100)，就能够利用FFT得到满足子空间投影精度要求的载频估计值。

在得到含多普勒的M个信号频率之后，还需要搜索31个卫星星号进行配对并估计时延。对于星号$q(q\in[1,31])$，利用第m个频率估计值$\hat{\omega}_m$得到该信号的估计值$\hat{s}_q(n)$，这里假设导航电文不发生反转且其值为1，则

$$\hat{s}_q(n)=d(n)c_q(n)\mathrm{e}^{\mathrm{j}\hat{\omega}_m n}=c_q(n)\mathrm{e}^{\mathrm{j}\hat{\omega}_m n} \tag{15}$$

则数字中频信号可以改写成

$$x_{\mathrm{IF}}(n)=\alpha_q\hat{s}_q(n-\tau_q)+e_3(n) \tag{16}$$

其中，$e_3(n)=x_{\mathrm{a}}(n)+x_{\mathrm{s}}(n)-\alpha_q\hat{s}_q(n-\tau_q)+e(n)$。

对式(16)进行离散傅里叶变换得到

$$X(k)=\alpha_q\hat{S}_q(k)\mathrm{e}^{\mathrm{j}\omega_q k}+E_3(k) \tag{17}$$

其中，$X(k),\hat{S}_q(k)$和$E_3(k)$分别是$x_{\mathrm{IF}}(n),\hat{s}_q(n)$和$e_3(n)$的离散傅里叶变换。用$f_{\mathrm{s}}$表示采样率，则$\omega_q=-2\pi\tau_q f_{\mathrm{s}}/N$。

估计出式(17)中的ω_q就可以得到信号时延的估计值$\hat{\tau}_q$，因此最小化以下非线性最小二乘代价函数[17]

$$Z(\hat{\omega}_q)=\sum_{k=-N/2}^{N/2-1}\left|X(k)-\hat{S}_q(k)\alpha_q\mathrm{e}^{\mathrm{j}\omega_q k}\right|^2 \tag{18}$$

令

$$\hat{\boldsymbol{S}}_q=\mathrm{diag}\left\{\hat{S}_q(-N/2),\hat{S}_q(-N/2+1),\cdots,\hat{S}_q(N/2-1)\right\}$$

$$\boldsymbol{a}(\omega_q)=\left[\mathrm{e}^{\mathrm{j}\omega_q(-N/2)},\mathrm{e}^{\mathrm{j}\omega_q(-N/2+1)},\cdots,\mathrm{e}^{\mathrm{j}\omega_q(N/2-1)}\right]^{\mathrm{T}},$$

$$\boldsymbol{X}=[X(-N/2),X(-N/2+1),\cdots,X(N/2-1)]^{\mathrm{T}},$$

则式(18)的矩阵表示为

$$Z(\hat{\omega}_q)=\left\|\boldsymbol{X}-\alpha_q\hat{\boldsymbol{S}}_q\boldsymbol{a}(\omega_q)\right\|^2 \tag{19}$$

根据式(19)可以得到ω_q的估计值为

$$\hat{\omega}_q=\arg\max_{\omega_q}\left|\boldsymbol{a}^{\mathrm{H}}(\omega_q)\hat{\boldsymbol{S}}_q^{\mathrm{H}}\boldsymbol{X}\right|^2 \tag{20}$$

进一步可以求得卫星q在一个C/A码周期内的时延估计值为

$$\hat{\tau}_q=-\hat{\omega}_q N/(2\pi f_{\mathrm{s}}) \tag{21}$$

可以利用FFT求解式(20)，不仅能够得到时延估计值，还可以得到本地重构信号$\hat{s}_q(n)$和接收信号$x_{\mathrm{IF}}(n)$相关值。由于C/A码的特性，只有本地重构信号和接收信号的PRN号相同时，相关值达到最大，从而完成PRN号匹配并能求得对应的时延估计值。在得到欺骗信号载频和时延后，即可构建欺骗信号子空间，进而抑制干扰。

4　仿真实验

本小节首先通过仿真实验分别从干扰抑制前后捕获相关峰变化和定位结果变化对本文所提方法的有效性进行验证。仿真参数见表1。

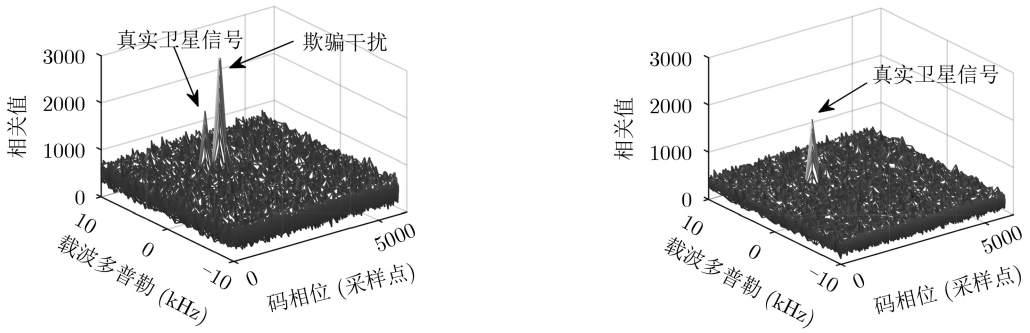
表 1　仿真参数

星号	中频(MHz)	采样率(MHz)	信噪比(dB)	干噪比
1 2 3 6 14 20 22 25	1.405	5.714	–20	–15

图3(a)和图3(b)分别表示欺骗干扰抑制前后星号为PRN1的卫星信号捕获结果。在仿真中，转发式欺骗干扰比真实信号延时500个样本点，因此在干扰抑制前的捕获结果中，有两个相关峰。由于欺骗信号比真实信号功率大，两个相关峰中的更高的一个是欺骗信号相关峰，因此接收机将会捕获欺骗信号。然而在干扰抑制后，图3(b)中只有一个真实信号的相关峰存在，由此可以证明算法抑制了欺骗信号。

在干扰抑制前后定位结果变化的实验中，假设接收机以40 m/s的速度做匀速圆周运动，圆周半径500 m。将真实信号延时后再放大作为欺骗信号。仿真产生36 s的数据进行处理，图4表示干净的真实信号的定位结果，接收机从A点圆周运动到B点。图5(a)表示加入干扰后的定位结果，由于接收机被欺骗，接收机的定位结果显示其从As点圆周运动到Bs点，与真实运动轨迹不同。图5(b)表示采取干扰抑制后的定位结果，可以看出抑制后的轨迹和真实信号一致，证明了本文算法能够消除干扰，帮助接收机产生正确的定位结果。

本文算法通过参数估计得到欺骗信号的载频和时延，而文献[14]中采用常规的捕获跟踪功能也能实现这一目标，然而捕获是一个2维搜索的过程，而且需要精细频率估计，运算复杂度比本文方法高，因此运算速度相对较慢。表2给出了文献算法和本文算法计算量的比较[18]，其中Q是卫星总数，M是欺骗信号个数，一般为4～12，P常规捕获算法的频点搜索次数，一般为21。两种算法投影过程的计算量相同，因此不计入表中。可以看到本文算法计算量明显降低，下面通过仿真实验对此进行验证。



(a) 干扰抑制前 (b) 干扰抑制后

图 3 PRN1的捕获结果

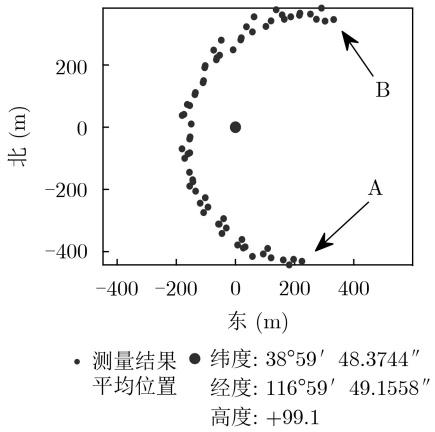
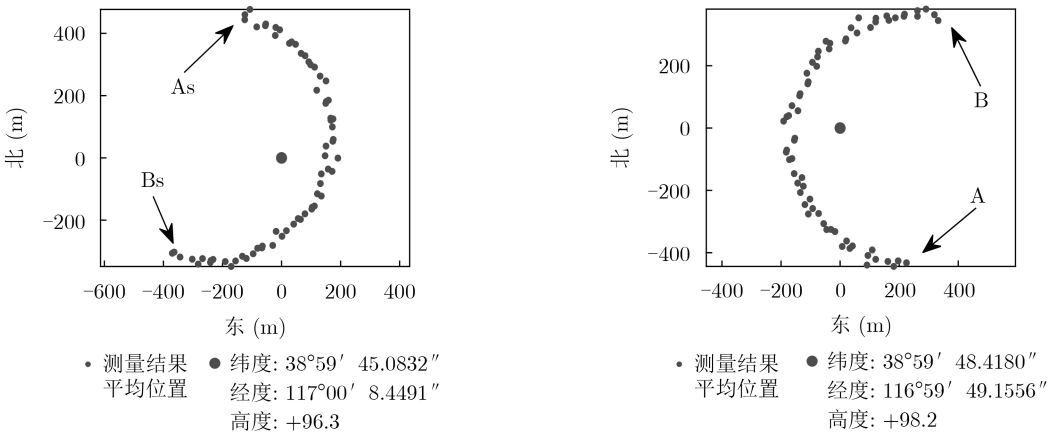


图 4 真实卫星信号定位结果

仿真中分别模拟4～12颗卫星被欺骗的场景，进行了100组实验，然后统计两种方法在卫星数目不同时的平均处理时间。实验平台的处理器为Intel i5-7500，主频3.4 GHz，内存为8 GB，仿真生成10 ms的GPS信号数据。如表3所示，随着被欺骗的卫星数量增加，两种方法的运行时间随之增加，但本文算法运行时间较文献算法大幅缩短，证明了本文算法通过参数估计减小了计算量，提高了算法的运算速度。

5 结束语

本文针对GNSS转发式欺骗干扰，提出了一种



(a) 干扰抑制前 (b) 干扰抑制后

图 5 欺骗干扰抑制前后定位结果

表 2 两种算法计算量比较

	乘法次数	加法次数	FFT计算次数	时间复杂度
文献算法	$7QP+4Q$	$2QP+3Q$	$2QP$	$O(QP)$
本文算法	$6QM+4M$	$3QM+7M$	$Q(M+1)+1$	$O(QM)$

表 3 算法计算时间随卫星个数变化表(s)

卫星数量	4	5	6	7	8	9	10	11	12
文献算法	2.507	2.544	2.567	2.597	2.641	2.642	2.689	2.698	2.733
本文算法	0.235	0.268	0.293	0.313	0.336	0.355	0.380	0.402	0.421

可用于单天线接收机的欺骗干扰抑制方法。本文方法首先利用FFT估计欺骗信号含多普勒频移的载频，其次利用得到的载频，根据非线性最小二乘准则估计出一个伪码周期内的时延，然后利用载频和时延，构建欺骗信号子空间正交投影矩阵以抑制欺骗干扰。本文方法可以和欺骗检测技术相结合，提高接收机的抗欺骗干扰能力。但是由于FFT精度的限制，本文方法仅适用于对抗功率略高于真实信号的欺骗干扰。仿真实验验证了本文方法对转发式欺骗干扰具有较好的抑制效果，能够帮助接收机在欺骗环境下得到正确的导航定位结果，并且拥有较低的计算复杂度。

参 考 文 献

[1] 吴仁彪, 王文益, 卢丹, 等. 卫星导航自适应抗干扰技术[M]. 北京: 科学出版社, 2015: 1–22.
WU Renbiao, WANG Wenyi, LU Dan, *et al*. Adaptive Interference Mitigation in GNSS[M]. Beijing: Science Press, 2015: 1–22.

[2] JAFARNIA JAHROMI A. GNSS signal authenticity verification in the presence of structural interference[D]. [Ph.D. dissertation], University of Calgary, 2013: 18-51.

[3] 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*, 2018, 54(2): 739–754. doi: 10.1109/TAES.2017.2765258.

[4] PSIAKI M L, O'HANLON B W, POWELL S P, *et al*. GNSS spoofing detection using two-antenna differential carrier phase[C]. The 27th International Technical Meeting of the Satellite Division of the Institute of Navigation, Tampa, USA, 2014: 2776–2800.

[5] BROUMANDAN A, JAFARNIA-JAHROMI A, DANESHMAND S, *et al*. Overview of spatial processing approaches for GNSS structural interference detection and mitigation[J]. *Proceedings of the IEEE*, 2016, 104(6): 1246–1257. doi: 10.1109/JPROC.2016.2529600.

[6] HU Yanfeng, BIAN Shaofeng, CAO Kejin, *et al*. GNSS spoofing detection based on new signal quality assessment model[J]. *GPS Solutions*, 2018, 22(1): No. 28. doi: 10.1007/s10291-017-0693-7.

[7] SUN Chao, CHEONG J W, DEMPSTER A G, *et al*. Moving variance-based signal quality monitoring method for spoofing detection[J]. *GPS Solutions*, 2018, 22(3): No. 83. doi: 10.1007/s10291-018-0745-7.

[8] WESSON K D, SHEPARD D P, BHATTI J A, *et al*. An evaluation of the vestigial signal defense for civil GPS anti-spoofing[C]. The 24th International Technical Meeting of the Satellite Division of The Institute of Navigation, Portland, USA, 2011: 2646–2656.

[9] HUMPHREYS T E, LEDVINA B M, PSIAKI M L, *et al*. Assessing the spoofing threat: Development of a portable GPS civilian spoofer[C]. The 21st International Technical Meeting of the Satellite Division of The Institute of Navigation, Savanna, Georgia, 2008: 2314-2325.

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

[11] MAGIERA J and KATULSKI R. Applicability of null-steering for spoofing mitigation in civilian GPS[C]. 2014 The 79th IEEE Vehicular Technology Conference, Seoul, South Korea, 2014: 1-5. doi: 10.1109/VTCSpring.2014.7022835.

[12] DANESHMAND S, JAFARNIA-JAHROMI A, BROUMANDAN A, *et al*. A low-complexity GPS anti-spoofing method using a multi-antenna array[C]. The 25th International Technical Meeting of the Satellite Division of the Institute of Navigation, Nashville, USA, 2012: 1233–1243.

[13] PSIAKI M L, HUMPHREYS T E, and STAUFFER B. Attackers can spoof navigation signals without our knowledge. Here's how to fight back GPS lies[J]. *IEEE Spectrum*, 2016, 53(8): 26–53. doi: 10.1109/MSPEC.2016.7524168.

[14] HAN Shuai, CHEN Lei, MENG Weixiao, *et al*. Improve the security of GNSS receivers through spoofing mitigation[J]. *IEEE Access*, 2017, 5: 21057–21069. doi: 10.1109/access.2017.2754414.

[15] SCHARF L L and FRIEDLANDER B. Matched subspace detectors[J]. *IEEE Transactions on Signal Processing*, 1994, 42(8): 2146–2157. doi: 10.1109/78.301849.

[16] 崔建华, 程乃平, 倪淑燕. 阵列天线抑制欺骗式导航干扰信号方法研究[J]. 电子学报, 2018, 46(2): 365–371. doi: 10.3969/j.issn.0372-2112.2018.02.015.
CUI Jianhua, CHENG Naiping, and NI Shuyan. Research on spoofing suppressing method using antenna array for navigation signal[J]. *Acta Electronica Sinica*, 2018, 46(2): 365–371. doi: 10.3969/j.issn.0372-2112.2018.02.015.

[17] LI Jian and WU Renbiao. An efficient algorithm for time delay estimation[J]. *IEEE Transactions on Signal Processing*, 1998, 46(8): 2231–2235. doi: 10.1109/78.705444.

[18] LI Jie, WU Renbiao, WANG Wenyi, *et al*. A novel GPS signal acquisition algorithm[J]. *Advances in Information Sciences & Service Sciences*, 2012, 4(17): 597–604.

卢　丹：女，1978年生，副教授，主要研究方向为卫星导航抗干扰、阵列信号处理.

白天霖：男，1993年生，硕士生，研究方向为卫星导航抗干扰.