doi:10.11887/j.cn.202502020 http://journal.nudt.edu.cn

欠定场景下的GNSS欺骗干扰源稀疏测向

赵雨晴[1],沈 锋[1*],徐定杰[1],孟 振[2]
(1. 哈尔滨工业大学 仪器科学与工程学院,黑龙江 哈尔滨 150001;
2. 中国矿业大学 信息与控制工程学院,江苏 徐州 221116)

摘 要:针对传统的子空间类测向算法在欠定场景下失效,且需要信号源数量作为先验信息的问题,提出一种基于互质阵列的GNSS欺骗干扰源测向方法,以提升卫星导航接收机在欺骗环境下的应用安全。通过构建循环相关矩阵以降低噪声对互质阵列信号处理性能的影响,并通过矢量化循环相关矩阵获取虚拟域等效阵列信号。在此基础上,设计一个基于虚拟域信号稀疏重构的优化问题,通过最小化拟合误差,获得高精度、多自由度测向结果。仿真结果表明,所提算法相比于传统子空间类算法具有更高的测向精度,而且在欠定场景下,依旧可以提供可靠的欺骗源测向结果。

关键词:卫星导航;欺骗干扰;测向;稀疏重构
中图分类号:TN967.1 **文献标志码**:A **文章编号**:1001-2486(2025)02-212-07

论文拓展

Sparse direction finding for GNSS spoofing source in underdetermined scenarios

ZHAO Yuqing[1], *SHEN Feng*[1*], *XU Dingjie*[1], *MENG Zhen*[2]
(1. School of Instrument Science and Engineering, Harbin Institute of Technology, Harbin 150001, China;
2. School of Information and Control Engineering, China University of Mining and Technology, Xuzhou 221116, China)

Abstract: Aiming at the problem that the traditional subspace-like direction finding algorithm fails in underdetermined scenarios and requires the number of signal sources as a priori information, a GNSS spoofing source direction finding method based on coprime array was proposed to improve the application security of satellite navigation receivers in spoofing environment. The cyclic correlation matrix was constructed to reduce the impact of noise on the performance of the coprime array signal processing, and the virtual domain equivalent array signal was obtained by vectoring the cyclic correlation matrix. On this basis, an optimization problem based on sparse signal reconstruction in virtual domain was designed to achieve high-precision, multi-degree of freedom direction finding for sources by minimizing the fitting error. Simulation results show that compared with traditional subspace algorithm, the proposed algorithm has higher estimation accuracy, and the direction finding results are still reliable under the case of underdetermined.

Keywords: satellite navigation; spoofing; direction finding; sparse reconstruction

依赖于全球导航卫星系统(global navigation satellite system, GNSS)的定时和定位系统已经在诸多领域得到广泛应用。然而,GNSS信号到达地面时的功率水平极为微弱,使得卫星导航系统易受到各种干扰的影响,这对卫星导航安全应用提出了严峻的挑战[1-2]。从类别上区分,影响卫星导航安全应用的干扰主要分为压制干扰和欺骗干扰两类[3]。压制干扰机通过发射高功率信号降低目标接收机的载噪比,使其不能正常工作。利用阵列天线的空间处理,已经提出了许多相对成熟的压制干扰抑制技术[4]。与压制干扰相比,欺骗干扰则通过发射一组与真实卫星信号相同或相似的伪GNSS信号,使接收机跟踪到欺骗信号,从而获得错误的位置或时间信息,这无疑会带来更大的危险[5-6]。此外,通过软件定义无线电技术,设计便携式GNSS欺骗器变得更加可行,成本

收稿日期:2022-11-20
基金项目:国家自然科学基金资助项目(62203447, 61673128, 61573117)
第一作者:赵雨晴(1996—),女,黑龙江哈尔滨人,博士研究生,E-mail:zhaoyuqing@hit.edu.cn
*通信作者:沈锋(1981—),男,黑龙江哈尔滨人,教授,博士,博士生导师,E-mail:fshen@hit.edu.cn
引用格式:赵雨晴, 沈锋, 徐定杰, 等. 欠定场景下的GNSS欺骗干扰源稀疏测向[J]. 国防科技大学学报, 2025, 47(2): 212-218.
Citation: ZHAO Y Q, SHEN F, XU D J, et al. Sparse direction finding for GNSS spoofing source in underdetermined scenarios[J]. Journal of National University of Defense technology, 2025, 47(2): 212-218.

更低[7]。因此,需要一种可靠的抗欺骗技术来提高 GNSS 应用的安全性。

面对日益严重的欺骗干扰威胁,一些抗欺骗方法应运而生。从技术上来看,GNSS 抗欺骗主要包括欺骗干扰检测、欺骗干扰抑制以及欺骗源定位三个方面[8]。其中,欺骗干扰检测技术主要通过密码防御、辅助设备验证以及信号特征辨识等方式,检测当前接收信号中是否存在欺骗信号[9-10]。欺骗抑制技术是指在欺骗检测的基础之上,通过天线阵调零或子空间投影等方式消除欺骗,使接收信号中只存在真实信号从而为用户恢复正常的定位、测速和授时服务[11]。最好的防御方式是进攻,欺骗源定位技术可通过无源定位方法,反向测量欺骗干扰的方位或位置,为从源头上消除欺骗提供了可能[12]。高精度的欺骗干扰源测向结果不仅为 GNSS 抗欺骗方法提供先验信息和技术支撑[13-15],对于提升欺骗干扰检测、抑制以及反向定位的性能也具有重要意义。

目前的 GNSS 信号源测向技术主要包括单天线法[16]和阵列天线法[17]。其中,单天线法硬件复杂度低,实现方法简单,但在复杂电子对抗情况下的效果受限[18]。基于阵列信号处理的方法对硬件复杂度的要求较高,但是当以抗干扰稳健性为前提时,这是可以接受的。然而,目前的阵列天线测向算法大都采用均匀阵列结构,其估计精度和自由度的提升都要靠增加阵元数量来实现,这意味着更高的成本和体积,而且在欠定场景下,即信号数(干扰和真实信号)多于物理传感器数量时,基于均匀阵列的测向方法无法对信号源的来向进行估计[19]。除此之外,当前基于阵列处理的欺骗干扰源测向方法都属于子空间类方法,其要求信源数已知,且在小样本采样快拍数时估计精度较差。

作为一种新型阵列,稀疏布置的互质阵列在雷达、声呐、无线通信等领域已经有了广泛的应用[20]。与传统阵列抗干扰方法普遍采用的均匀阵列相比,稀疏排布的天线阵列及其虚拟域信号处理的应用使抗干扰的自由度不再受限于物理阵元的个数,而且在相同个数物理阵元的情况下可以获得更高的空间分辨率。文献[21]详细分析了基于稀疏配置的最小冗余阵列在 GNSS 压制干扰抑制中的作用,为在卫星导航中利用稀疏阵列进行干扰抑制指明了方向。但值得注意的是,该处理框架是针对压制干扰而言的,无法缓解危害性更高的欺骗攻击。通常,压制干扰相对于真实卫星信号具有明显的功率优势,而欺骗信号为了成功接管目标接收机而不被检测到,其功率与真实卫星信号保持相当,都淹没于噪声之下,这为在接收机解扩前进行欺骗检测与抑制带来了困难。除此之外,传统的最小冗余阵列不具有系统化的阵列结构,需要通过查表或者设计优化问题才能确定物理阵列的结构,而且在部分情况下最优阵列结构设计是不存在的,这严重限制了其应用范围。

针对上述挑战,本文设计了一种基于互质阵列信号稀疏重构的欺骗源测向方法,它无须信号源数量作为先验信息,还可以满足高精度、多自由度、复杂场景下的欺骗干扰防御需求。与最小冗余阵列相比,具有系统化稀疏阵列结构的互质阵列的阵元布设方案较为简单直观且易操作,通过获取其虚拟差分阵列结构同样可以获得比均匀阵列更高的分辨率和更大的自由度。

1　互质阵列接收信号模型

首先根据空间域的互质阵列结构,构建其在卫星导航欺骗背景下的接收信号模型。本文采用了一种广义互质阵列结构——扩展互质阵列[20],其结构如图 1 所示,由一对分别具有 $2M$ 和 N 个传感器阵元的均匀线性阵列组成,其中 M 和 N 是互质整数。

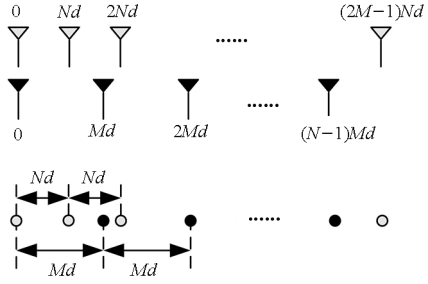

图 1　扩展互质阵列结构

Fig. 1　Extended coprime array geometry

如图 1 所示,第一个均匀线性阵列由间距为 Nd 的 $2M$ 个天线阵元组成,而另一个均匀线性阵列由间距为 Md 的 N 个传感器阵元组成。通常参数 $d=\lambda/2$,其中 λ 表示信号波长。由于质数的特质,除第一个作为参考的传感器阵元之外,当两个子阵对齐时,其他阵元不会相互重叠。因此,扩展互质阵列共包含 $2M+N-1$ 个物理传感器用于 GNSS 信号接收。

由于技术上的限制,目前的欺骗干扰机大部分都是利用单天线发射欺骗信号,即多个虚假的伪随机噪声(pseudo random noise, PRN)码信号都具有相同的入射方向。在不失一般性的情况

下,存在 L 个真实信号、Q 个欺骗信号从方向 $\boldsymbol{\theta}=[\theta_1,\theta_2,\cdots,\theta_K]$ 入射到互质阵列。由于所有欺骗信号都来自同一方向,即 $K=L+1$,互质阵列接收到的中频信号可表示为:

$$\boldsymbol{x}(t)=\sum_{l=1}^{L}\boldsymbol{a}_l^{\mathrm{A}}s_l^{\mathrm{A}}(t)+\boldsymbol{a}^{\mathrm{S}}\sum_{q=1}^{Q}s_q^{\mathrm{S}}(t)+\boldsymbol{n}(t) \tag{1}$$

式中,$\boldsymbol{a}_l^{\mathrm{A}}$ 和 $\boldsymbol{a}^{\mathrm{S}}$ 分别表示第 l 个真实信号和欺骗信号的导向矢量,$\boldsymbol{n}(t)$ 表示复高斯噪声矢量,$s_l^{\mathrm{A}}(t)$ 表示第 l 个真实信号,$s_q^{\mathrm{S}}(t)$ 表示第 q 个欺骗信号,上标 A 和 S 分别表示真实信号和欺骗信号。以 GPS L_1 的 C/A 码为例,$s_l^{\mathrm{A}}(t)$ 和 $s_q^{\mathrm{S}}(t)$ 可以分别表示为:

$$\begin{cases}s_l^{\mathrm{A}}(t)=\sqrt{P_l^{\mathrm{A}}}D_l^{\mathrm{A}}(t-\tau_l^{\mathrm{A}})C_l^{\mathrm{A}}(t-\tau_l^{\mathrm{A}})\mathrm{e}^{\mathrm{j}2\pi(f_{\mathrm{IF}}+f_l^{\mathrm{A}})t+\mathrm{j}\varphi_l^{\mathrm{A}}}\\ s_q^{\mathrm{S}}(t)=\sqrt{P_q^{\mathrm{S}}}D_q^{\mathrm{S}}(t-\tau_q^{\mathrm{S}})C_q^{\mathrm{S}}(t-\tau_q^{\mathrm{S}})\mathrm{e}^{\mathrm{j}2\pi(f_{\mathrm{IF}}+f_q^{\mathrm{S}})t+\mathrm{j}\varphi_q^{\mathrm{S}}}\end{cases} \tag{2}$$

其中,f_{IF} 表示中频频率,参数 φ、P、f 和 τ 分别表示每个信号的相位、功率、多普勒频率和码延迟,$C(t)$ 是 C/A 码,$D(t)$ 是导航数据码。

在式(1)中,$\boldsymbol{a}_l^{\mathrm{A}}$ 和 $\boldsymbol{a}^{\mathrm{S}}$ 描述了从不同天线单元接收到的信号在某一方向上的载波相位差。由于 Q 个欺骗信号的入射方向相同,所以欺骗信号都具有相同的导向矢量。对于入射方向为 θ_k 的信号,其对应的导向矢量可以表示为:

$$\boldsymbol{a}=[1,\cdots,\mathrm{e}^{-\mathrm{j}\frac{2\pi}{\lambda}d_i\sin\theta_k},\cdots,\mathrm{e}^{-\mathrm{j}\frac{2\pi}{\lambda}d_{2M+N-1}\sin\theta_k}]^{\mathrm{T}} \tag{3}$$

其中,$d_i(i=1,2,\cdots,2M+N-1)$ 表示实际物理阵元的位置。

值得注意的是,上述模型基于广泛使用的 GPS L_1 C/A 信号。然而,由于不同 GNSS 信号的相似性,本文提出的方法可以很容易地推广到其他卫星定位系统。

2 所提欺骗干扰源测向算法

2.1 循环相关协方差矩阵构建

在 GNSS 接收机解扩之前,欺骗信号和真实信号都被掩埋在噪声层之下。通常情况下真实信号的信噪比(signal-to-noise ratio, SNR)为 −20 dB 左右,而欺骗信号仅比真实信号高 1.1 dB 就可以成功诱导目标接收机产生错误的导航和定位结果,这为欺骗信号的测向带来挑战。为了解决这个问题,充分利用了 GNSS 信号的自相干特性来估计协方差矩阵,从而消除或者显著降低协方差矩阵中的噪声分量。具体而言,式(2)中的 C/A 码是周期重复的,因此每个真实信号和欺骗信号在码周期 $T_{\mathrm{C/A}}$ 处具有循环平稳性,定义接收信号 $\boldsymbol{x}(t)$ 与其对应的参考信号 $\boldsymbol{x}(t-T_{\mathrm{C/A}})$ 之间的循环相关协方差矩阵为:

$$\begin{aligned}\boldsymbol{R}_{xx}^{(G)}&=E[\boldsymbol{x}(t)\boldsymbol{x}^{\mathrm{H}}(t-T_{\mathrm{C/A}})]\\&=\sum_{l=1}^{L}\boldsymbol{a}_l^{\mathrm{A}}(\boldsymbol{a}_l^{\mathrm{A}})^{\mathrm{H}}\boldsymbol{R}_{s_l^{\mathrm{A}}s_l^{\mathrm{A}}}+\boldsymbol{a}^{\mathrm{S}}(\boldsymbol{a}^{\mathrm{S}})^{\mathrm{H}}\sum_{q=1}^{Q}\boldsymbol{R}_{s_q^{\mathrm{S}}s_q^{\mathrm{S}}}+\\&\quad\sum_{m=1}^{L}\boldsymbol{a}_m^{\mathrm{A}}(\boldsymbol{a}^{\mathrm{S}})^{\mathrm{H}}\boldsymbol{R}_{s_m^{\mathrm{S}}s_m^{\mathrm{A}}}\end{aligned} \tag{4}$$

其中,$\boldsymbol{R}_{s_l^{\mathrm{A}}s_l^{\mathrm{A}}}$ 和 $\boldsymbol{R}_{s_q^{\mathrm{S}}s_q^{\mathrm{S}}}$ 分别表示 $T_{\mathrm{C/A}}$ 处第 l 个真实信号和第 q 个欺骗信号的循环自相关函数。根据文献[14],则

$$\begin{cases}\boldsymbol{R}_{s_l^{\mathrm{A}}s_l^{\mathrm{A}}}\approx C_{\mathrm{IF}}P_l^{\mathrm{A}}\\ \boldsymbol{R}_{s_q^{\mathrm{A}}s_q^{\mathrm{A}}}\approx C_{\mathrm{IF}}P_q^{\mathrm{S}}\end{cases} \tag{5}$$

其中,C_{IF} 是一个范数为 1 的复常数,$\boldsymbol{R}_{s_m^{\mathrm{S}}s_m^{\mathrm{A}}}$ 是具有相同 PRN 码的真实信号和欺骗信号之间的互相关结果,可以表示为

$$\boldsymbol{R}_{s_m^{\mathrm{S}}s_m^{\mathrm{A}}}=\rho_{s_m^{\mathrm{S}}s_m^{\mathrm{A}}}\sqrt{P_m^{\mathrm{A}}}\sqrt{P_m^{\mathrm{S}}} \tag{6}$$

其中,$\rho_{s_m^{\mathrm{S}}s_m^{\mathrm{A}}}(0\leqslant\rho_{s_m^{\mathrm{S}}s_m^{\mathrm{A}}}\leqslant1)$ 表示二者间的相关系数。一般情况下,欺骗信号与真实信号的码相位差大于一个码片,即 $\rho_{s_m^{\mathrm{S}}s_m^{\mathrm{A}}}$ 认为是 0。因此,式(4)可以重写为:

$$\begin{aligned}\boldsymbol{R}_{xx}^{(G)}&=E[\boldsymbol{x}(t)\boldsymbol{x}^{\mathrm{H}}(t-T_{\mathrm{C/A}})]\\&=\sum_{l=1}^{L}\boldsymbol{a}_l^{\mathrm{A}}(\boldsymbol{a}_l^{\mathrm{A}})^{\mathrm{H}}\boldsymbol{R}_{s_l^{\mathrm{A}}s_l^{\mathrm{A}}}+\boldsymbol{a}^{\mathrm{S}}(\boldsymbol{a}^{\mathrm{S}})^{\mathrm{H}}\sum_{q=1}^{Q}\boldsymbol{R}_{s_q^{\mathrm{S}}s_q^{\mathrm{S}}}\end{aligned} \tag{7}$$

从式(7)中可以看出,由于假设 $\boldsymbol{n}(t)$ 为高斯噪声,所以 $\boldsymbol{R}_{xx}^{(G)}$ 中的噪声得到有效抑制。在实际中 $\boldsymbol{R}_{xx}^{(G)}$ 无法精确地得到,通常用采样协方差矩阵 $\hat{\boldsymbol{R}}_{xx}^{(G)}$ 代替:

$$\hat{\boldsymbol{R}}_{xx}^{(G)}\approx\frac{1}{N}\boldsymbol{X}_N\boldsymbol{X}_{N\mathrm{ref}}^{\mathrm{H}} \tag{8}$$

其中,$\boldsymbol{X}_N$ 代表采样数据块,$\boldsymbol{X}_{N\mathrm{ref}}$ 是对应的参考数据块:

$$\begin{cases}\boldsymbol{X}_N=[x(k),x(k-1),\cdots,x(k-N+1)]\\ \boldsymbol{X}_{N\mathrm{ref}}=[x(k-D),x(k-D-1),\cdots,x(k-D-N+1)]\end{cases} \tag{9}$$

其中,D 表示一个码周期内的采样点数,N 表示数据块采样点长度。为了提高采样协方差矩阵的估计精度,采用 G 对数据块 $\boldsymbol{X}_N$ 和 $\boldsymbol{X}_{N\mathrm{ref}}$ 循环相关结果的平均值:

$$\hat{\boldsymbol{R}}_{xx}^{(G)}\approx\frac{1}{G}\sum_{g=1}^{G}\frac{1}{N}\boldsymbol{X}_N^g(\boldsymbol{X}_{N\mathrm{ref}}^g)^{\mathrm{H}} \tag{10}$$

其中,$1\leqslant g<20$,$\boldsymbol{X}_N^g$ 和 $\boldsymbol{X}_{N\mathrm{ref}}^g$ 分别为:

$$\begin{cases}\boldsymbol{X}_N^g=[x(k-gD),x(k-1-gD),\cdots,x(k-N+1-gD)]\\ \boldsymbol{X}_{N\mathrm{ref}}^g=[x(k-(g+1)D),x(k-1-(g+1)D),\cdots,\\ \qquad x(k-N+1-(g+1)D)]\end{cases} \tag{11}$$

2.2 虚拟信号稀疏重构

为了充分利用互质阵列提供的自由度,突破

物理阵元个数对自由度的限制,本文通过虚拟域信号处理以实现自由度性能的提升。具体而言,扩展互质阵列的原始接收信号 $x(t)$ 与虚拟域等价信号 $\boldsymbol{z}$ 之间的映射关系可通过对循环相关协方差矩阵向量化实现,其数学表示为:

$$\boldsymbol{z} \triangleq vec(\boldsymbol{R}_{xx}^{(G)}) = \boldsymbol{B}\boldsymbol{p} \tag{12}$$

其中,$vec(\cdot)$ 为向量化操作,即将矩阵中的各列堆叠以形成一个列向量。向量 $\boldsymbol{z}$ 可视为虚拟阵列对应的等价信号,其对应的阵列流型矩阵为 $\boldsymbol{B} \in \mathbb{C}^{(2M+N-1)^2 \times K}$,信号源为 $\boldsymbol{p}$,具体表示为:

$$\begin{aligned}\boldsymbol{B} = [&(\boldsymbol{a}_1^{\mathrm{A}})^* \otimes \boldsymbol{a}_1^{\mathrm{A}}, (\boldsymbol{a}_2^{\mathrm{A}})^* \otimes \boldsymbol{a}_2^{\mathrm{A}}, \cdots,\\ &(\boldsymbol{a}_L^{\mathrm{A}})^* \otimes \boldsymbol{a}_L^{\mathrm{A}}, (\boldsymbol{a}^{\mathrm{S}})^* \otimes \boldsymbol{a}^{\mathrm{S}}]\end{aligned} \tag{13}$$

$$\boldsymbol{p} = \left[\boldsymbol{R}_{s_1^{\mathrm{A}}s_1^{\mathrm{A}}}, \boldsymbol{R}_{s_2^{\mathrm{A}}s_2^{\mathrm{A}}}, \cdots, \boldsymbol{R}_{s_L^{\mathrm{A}}s_L^{\mathrm{A}}}, \sum_{q=1}^{Q} \boldsymbol{R}_{s_q^{\mathrm{S}}s_q^{\mathrm{S}}}\right]^{\mathrm{T}} \tag{14}$$

其中,$\otimes$ 为克罗内克积,$(\,)^*$ 为共轭操作。$\boldsymbol{B}$ 的列向量代表虚拟阵列对应的导向矢量。由于 $\boldsymbol{B}$ 中含有多个相同的相位延迟,因此将 $\boldsymbol{B}$ 去冗余处理,即去除 $\boldsymbol{B}$ 中的重复行构成一个新的阵列流型矩阵 $\boldsymbol{B}_1 \in \mathbb{C}^{(3MN+M-N)\times K}$,对应得到的新等价虚拟阵列信号 $\boldsymbol{z}_1 = \boldsymbol{B}_1\boldsymbol{p}$。也就是说,$\boldsymbol{z}_1$ 可以看作由 $3MN+M-N$ 个虚拟阵元接收的等价信号,其阵元数由原始互质阵列的 $2M+N-1$ 增加到 $3MN+M-N$,利用该虚拟阵列信号进行统计信号处理能够扩展测向的自由度,克服实际物理阵元个数对自由度的限制。值得注意的是,$\boldsymbol{z}_1$ 为二阶统计量,与一阶统计量 $\boldsymbol{x}(t)$ 中所包含的信号波形信息 $s(t)$ 所不同的是,$\boldsymbol{z}_1$ 表征的是信号源的功率特征。

然后,本文将根据虚拟阵列信号稀疏重建的思想设计优化问题,以获得用于测向的稀疏空间谱。其核心思想是将信号稀疏重建的思想推广至虚拟域,在稀疏性约束条件下,最小化虚拟域等价信号 $\boldsymbol{z}_1$ 和其理论值之间的拟合误差:

$$\begin{cases}\hat{\boldsymbol{p}} = \arg\min_{\boldsymbol{p}} \|\boldsymbol{p}\|_0\\ \text{s.t.} \quad \|\boldsymbol{z}_1 - \boldsymbol{B}_1\boldsymbol{p}\|_2 < \epsilon\end{cases} \tag{15}$$

其中,$\|\ \|_0$ 和 $\|\ \|_2$ 分别表示 l_0 范数和 l_2 范数,ϵ 为拟合误差上限。可见,所构造的优化问题旨在寻找能够使虚拟域等价信号 $\boldsymbol{z}_1$ 和重建的理论值之间拟合误差最小的最优化稀疏空间谱 $\hat{\boldsymbol{p}}$。然而,式(15)中包含非凸项 l_0 范数,使其成为一个 NP 难(NP hard)问题。为了解决这一问题,考虑将 l_0 凸松弛替换 l_1 范数,通过最小绝对收缩和选择算子(least absolute shrinkage and selection operator, LASSO)进行求解。进一步,利用入射信号相对于整个空间域的稀疏性,将波达方向 $\boldsymbol{\theta} = [\theta_1, \theta_2, \cdots, \theta_K]$ 进行过完备表示 $\{\theta_1^g, \theta_2^g, \cdots, \theta_K^g\}$,可以得到对应于过完备基的增广矩阵 $\boldsymbol{B}_1^g$,则 LASSO 目标函数可表示为:

$$\hat{\boldsymbol{p}}^g = \arg\min_{p^g}\left(\frac{1}{2}\|\boldsymbol{z}_1 - \boldsymbol{B}_1^g\boldsymbol{p}^g\|_2 + \xi\|\boldsymbol{p}^g\|_1\right) \tag{16}$$

其中:l_2 范数项表示虚拟阵列等价信号 $\boldsymbol{z}_1$ 的拟合误差;l_1 范数项为重建的空间谱凸松弛化稀疏约束;ξ 是正则化参数,用于权衡拟合误差和稀疏度。求解上述的凸优化问题,可获得过完备表示的 $\{\theta_1^g, \theta_2^g, \cdots, \theta_K^g\}$ 对应的空间谱 $\hat{\boldsymbol{p}}^g$,通过搜索其谱峰值对应的角度即可获得所有信号的到达角。由于空间谱响应的大小可以表征空间信号的功率强弱,在检测到欺骗信号的基础之上,最大空间谱响应值对应的信号来向即为欺骗信号的来向。由于式(16)设计的优化问题是基于二阶虚拟域等价信号构建的,所以测向的自由度可以有效地提升。

3　仿真验证

在已检测到欺骗信号存在的基础之上,对所提基于虚拟信号稀疏重构的欺骗源测向方法的有效性进行验证。具体而言,选用目前典型的子空间类欺骗源测向方法:循环多重信号分类[14](cyclic multiple singal classification, Cyclic MUSIC)算法和特征空间多重信号分类[22](eigenspace multiple signal classification, ESMUSIC)算法为对比算法,在仿真试验中分别用 Cyclic MUSIC 算法和 ESMUSIC 算法进行标识,分别从空间谱特性和精度这两方面,对所提算法性能进行验证。在仿真实验中,使用的扩展互质阵列由一对包含 $2M=2\times3=6$ 个阵元和 $N=5$ 个阵元的均匀线性阵列(uniform linear array, ULA)构成,因此,实际阵列一共包含 $2M+N-1=10$ 个物理阵元,这些阵元传感器分别位于 $[0\ d,\ 3\ d,\ 5\ d,\ 6\ d,\ 9\ d,\ 10\ d, 12\ d,\ 15\ d,\ 20\ d,\ 25\ d]$ 的位置处。预定义的空间网格点以 0.1°的间隔均匀分布于 −90°到 90°的范围内。正则化参数设置为 0.8。选取 20 ms 数据进行仿真分析,数据块长度为 37 000,每个码周期的样本数为 37 个,此外,使用了 2 对数据块和参考数据块估计采样循环相关协方差矩阵。采样频率为 37.851 MHz,中频频率为 4.092 MHz。假设噪声为零均值高斯白噪声,真实卫星信号的信噪比设为 −20 dB,而欺骗信号的 SNR 可以根据不同的仿真场景而改变。欺骗信号和真实信号码相位对齐在第 100 个采样点处。

3.1　空间谱特性比较

本小节将针对两种不同的场景,对所提估计算法的空间谱特性进行仿真分析。为了公平比

较，Cyclic MUSIC 算法和 ESMUSIC 算法都采用和互质阵列相同阵元数（10 个物理阵元）的 ULA。其中，ULA 的阵元间距 d 设置为半波长，即 $d=\lambda/2$。由于子空间类算法需要信号源数量的先验信息，所以假设执行 Cyclic MUSIC 算法和 ESMUSIC 算法时信号源的个数是精确已知的。

场景 1：在第一个仿真实验中，假设 5 个真实的卫星信号 PRN2、PRN6、PRN8、PRN13 和 PRN19 分别从 −40°、−20°、−10°、10° 和 20° 的方向入射。一个欺骗源来自 40° 方向，欺骗信号的 PRN 码与真实信号相同。为了成功欺骗目标接收机，欺骗信号相比于真实信号具有功率优势，但为了欺骗过程的隐蔽性，过高的欺骗功率会导致欺骗信号容易被接收机检测。因此，在本小节中，假设每个欺骗信号的 SNR 比真实信号高 3 dB。而不同欺骗信号功率下的测向效果将在 3.2 小节进行进一步分析。图 2 给出了所提基于虚拟阵列信号稀疏重建算法与基于 ULA 的 Cyclic MUSIC 算法和 ESMUSIC 算法的归一化空间谱估计结果。从图 2 可以看出，三种算法都可以对所有信号来向进行估计，但两种对比算法峰值响应不如所提算法那样尖锐。此外，三种算法都显示 40° 方向对应空间谱响应的最大值，所以欺骗信号的波达角为 40°，这与仿真设置一致。

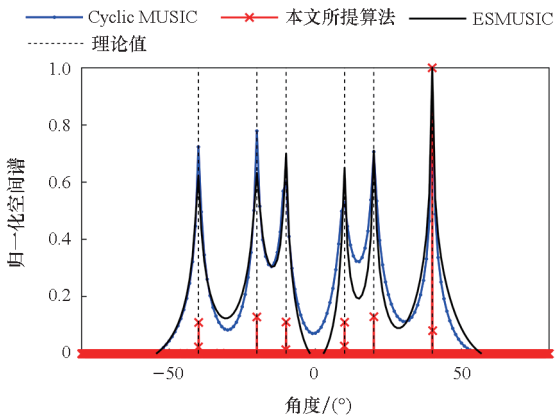

图 2　场景 1 的空间谱比较

Fig. 2　Spatial spectrum comparison in scenario 1

场景 2：在这一场景下，假设信号源的数量大于天线传感器的数量即欠定场景，随着可见卫星数量的增加和日益复杂的电磁环境，这更符合实际的 GNSS 应用场景。10 个真实信号 PRN1、PRN2、PRN5、PRN8、PRN9、PRN13、PRN19、PRN21、PRN26 和 PRN29 分别来自 −50°、−40°、−30°、−20°、−10°、0°、10°、30°、40° 和 50° 方向。欺骗源发送 4 个伪信号，伪信号的 PRN 与真实卫星信号 PRN2、PRN5、PRN8、PRN9 相同。假设每个欺骗信号的信噪比 SNR 比真实信号高 2 dB，欺骗信号的来向为 20°。由于采用 ULA 的 Cyclic MUSIC 算法和 ESMUSIC 算法的空间谱自由度受限于实际物理阵元的个数，10 个物理阵元的 ULA 其自由度为 9，无法对 11 个信号源进行有效分辨，所以图 3 中无法绘制两种基于 ULA 的对比算法的空间谱；相反地，所提算法能够在使用 10 个物理阵元的情况下对 11 个入射信号源进行有效分辨（如图 3 所示），这显示了其在自由度提升上的优势。除此之外，根据所提算法的空间谱估计结果，可以看出欺骗源的方向为 20°。因此，所提算法在实际物理传感器数量不足的情况下，仍可以对欺骗源的来向进行准确估计。

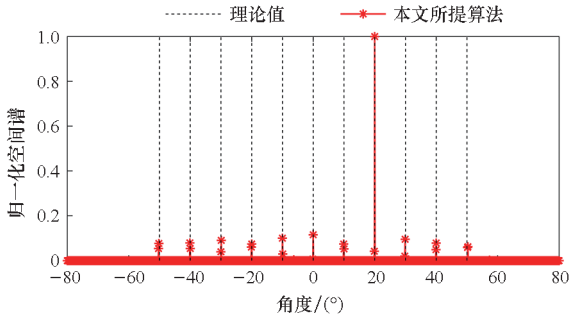

图 3　场景 2 的空间谱比较

Fig. 3　Spatial spectrum comparison in scenario 2

3.2　测向精度比较

本小节将比较所提算法与两种对比算法的测向性能，测向性能由均方根误差（root mean square error，RMSE）进行评估，性能结果均通过 1 000 次 Monte-Carlo 试验求平均值获得。三种算法 RMSE 随数据块采样点长度 N 的变化曲线如图 4 所示，其中每个欺骗信号的 SNR 为 −17 dB，其他参数设置与 3.1 小节中的仿真场景 1 一致。图 5 则给出了三种算法 RMSE 随欺骗信号信噪比的变化曲线，以考察欺骗信号的信噪比对测向精度的影响。其中 $N=37\ 000$，其他参数与 3.1 小节中的仿真场景 1 一致。

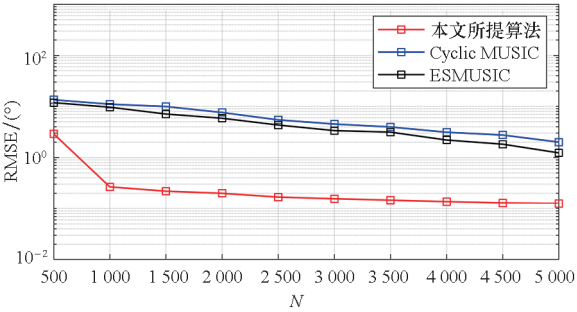

图 4　RMSE 与 N 的关系曲线

Fig. 4　RMSE versus N curve

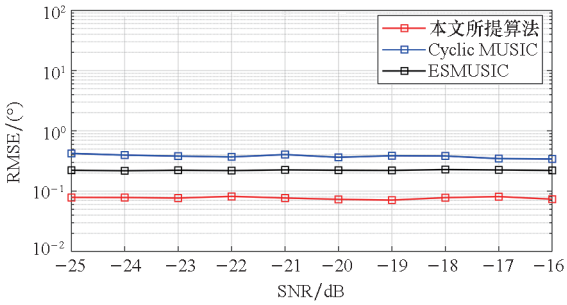

图 5　RMSE 与 SNR 的关系曲线

Fig. 5　RMSE versus SNR curve

图 4 和图 5 显示了本文所提算法在测向精度上的优越性。具体而言,如图 4 所示,三种算法的 RMSE 随着 N 的增加均表现出下降的趋势,但所提算法在 N 较小时也可以具有较为理想的性能,当 $N = 500$ 时,所提测向算法的 RMSE 优于 Cyclic MUSIC 算法和 ESMUSIC 约 10°。由图 5 可知,本文所提算法的测向性能在所考虑的整个 SNR 范围内均优于 Cyclic MUSIC 算法和 ESMUSIC 算法。以上仿真对比结果表明,通过求解式(16)所构建的优化问题,测向精度得到了有效的提升。

4　结论

本文从稀疏重建的角度提出了一种欠定场景下的欺骗源测向方法,该方法无须信号源数作为先验信息,在自由度增加的同时,可以实现高精度欺骗源测向。本文所提方法首先构造循环相关矩阵以去除协方差矩阵中的噪声信号,然后对去噪后的协方差矩阵矢量化处理获得等效虚拟阵列信号,利用 GNSS 信号相对于整个空间域的稀疏特性,通过预定义网格点对虚拟阵列信号进行过完备表示,将信号稀疏重建的思想扩展到虚拟域,设计了一个优化问题,在保证最小化拟合误差的同时实现对虚拟域等效信号进行稀疏化重建,通过空间谱分析对欺骗信号源的来向进行了有效估计。仿真结果表明,本文所提算法不仅适用于入射信号总数大于阵元数目的欺骗场景,而且具有较高精度的测向结果。

虽然所提算法具有明显的性能优势,在一定程度上可以推动新型天线在卫星导航领域的应用,但稀疏配置的互质阵列必然会导致天线体积增大,从而限制其使用范围。因此,在接下来的研究中,需要进一步优化阵列结构,突破阵列天线尺寸和体积的限制,使其有望应用于小型化的导航场景中。

参考文献(References)

[1] 史鹏亮, 王晓宇, 薛瑞. 无人机位置欺骗诱导策略[J]. 国防科技大学学报, 2021, 43(2): 40 – 46.
SHI P L, WANG X Y, XUE R. Induction strategy for unmanned aerial vehicle position spoofing[J]. Journal of National University of Defense Technology, 2021, 43(2): 40 – 46. (in Chinese)

[2] 鲁祖坤, 郭海玉, 宋捷, 等. 抗干扰型卫星导航接收机的最优前端增益[J]. 系统工程与电子技术, 2022, 44(7): 2270 – 2275.
LU Z K, GUO H Y, SONG J, et al. Optimal front-end gain of anti-jamming satellite navigation receiver[J]. Systems Engineering and Electronics, 2022, 44(7): 2270 – 2275. (in Chinese)

[3] 吴忠望, 胡彦逢, 徐龙威. 导航战中 GNSS 信号干扰技术特征研究[J]. 无线电工程, 2021, 51(10): 1031 – 1036.
WU Z W, HU Y F, XU L W. Research on technical characteristics of GNSS signal jamming in navigation warfare[J]. Radio Engineering, 2021, 51(10): 1031 – 1036. (in Chinese)

[4] 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.
REN B B, NI S J, CHEN F Q, et al. Analysis of anti-spoofing performance of GNSS nulling anti-jamming antenna[J]. GNSS World of China, 2021, 46(6): 30 – 36. (in Chinese)

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

[6] 付栋, 彭竞, 马明, 等. 基于钟差检验的 GNSS 授时欺骗检测与识别[J]. 系统工程与电子技术, 2022, 44(3): 948 – 955.
FU D, PENG J, MA M, et al. GNSS time spoofing detection and discrimination based on clock bias hypothesis test[J]. Systems Engineering and Electronics, 2022, 44(3): 948 – 955. (in Chinese)

[7] GASPAR J, FERREIRA R, SEBASTIÃO P, et al. Capture of UAVs through GPS spoofing using low-cost SDR platforms[J]. Wireless Personal Communications, 2020, 115(4): 2729 – 2754.

[8] 边少峰, 胡彦逢, 纪兵. GNSS 欺骗防护技术国内外研究现状及展望[J]. 中国科学: 信息科学, 2017, 47(3): 275 – 287.
BIAN S F, HU Y F, JI B. Research status and prospect of GNSS anti-spoofing technology [J]. Scientia Sinica Informationis, 2017, 47(3): 275 – 287. (in Chinese)

[9] 周薏, 李洪, 王楚涵, 等. 全球导航卫星系统诱导式欺骗检测[J]. 国防科技大学学报, 2019, 41(4): 129 – 135.
ZHOU M, LI H, WANG C H, et al. Induced spoofing detection of global navigation satellite system[J]. Journal of National University of Defense Technology, 2019, 41(4): 129 – 135. (in Chinese)

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

[11] 王晓宇, 吴舜晓, 王亚锋, 等. 一种基于阵列天线的卫星导航欺骗干扰检测与抑制方法[J]. 现代导航, 2022, 13(3): 163 – 169.

WANG X Y, WU S X, WANG Y F, et al. Spoofing interference detection and suppression method based on array antenna for satellite navigation [J]. Modern Navigation, 2022, 13(3): 163 – 169. (in Chinese)

[12] FALCO G, NICOLA M, FALLETTI E, et al. An algorithm for finding the direction of arrival of counterfeit GNSS signals on a civil aircraft[C]//Proceedings of the 32nd International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS + 2019), 2019: 3185 – 3196.

[13] APPEL M, KONOVALTSEV A, MEURER M. Robust spoofing detection and mitigation based on direction of arrival estimation [C]//Proceedings of the 28th International Technical Meeting of the Satellite Division of the Institute of Navigation(ION GNSS +2015), 2015: 3335 – 3344.

[14] ZHANG J Q, CUI X W, XU H L, et al. A two-stage interference suppression scheme based on antenna array for GNSS jamming and spoofing[J]. Sensors, 2019, 19(18): 3870.

[15] DANESHMAND S, JAFARNIA-JAHROMI A, BROUMANDAN A, et al. A GNSS structural interference mitigation technique using antenna array processing[C]//Proceedings of the 2014 IEEE 8th Sensor Array and Multichannel Signal Processing Workshop (SAM), 2014: 109 – 112.

[16] 王仲潇, 李洪, 周子恒, 等. 一种面向商用接收机的GNSS欺骗干扰源测向方法[J]. 中国科学: 信息科学, 2022, 52(4): 658 – 674.
WANG Z X, LI H, ZHOU Z H, et al. A direction finding method of the GNSS spoofer for commercial receivers[J]. Scientia Sinica Informationis, 2022, 52(4): 658 – 674. (in Chinese)

[17] 关刚强. 阵列天线卫星导航接收机关键技术研究[D]. 长沙: 国防科学技术大学, 2017.
GUAN G Q. Research on key techniques of GNSS receiver with antenna arrays[D]. Changsha: National University of Defense Technology, 2017. (in Chinese)

[18] MAGIERA J, KATULSKI R. Detection and mitigation of GPS spoofing based on antenna array processing[J]. Journal of Applied Research and Technology, 2015, 13(1): 45 – 57.

[19] 孙兵, 阮怀林, 吴晨曦, 等. 非均匀噪声条件下的互质阵列欠定DOA估计方法[J]. 电子与信息学报, 2021, 43(12): 3687 – 3694.
SUN B, RUAN H L, WU C X, et al. Underdetermined direction of arrival estimation for coprime array in the presence of nonuniform noise[J]. Journal of Electronics & Information Technology, 2021, 43(12): 3687 – 3694. (in Chinese)

[20] SHI Z G, ZHOU C W, GU Y J, et al. Source estimation using coprime array: a sparse reconstruction perspective[J]. IEEE Sensors Journal, 2017, 17(3): 755 – 765.

[21] AMIN M G, WANG X R, ZHANG Y D, et al. Sparse arrays and sampling for interference mitigation and DOA estimation in GNSS[J]. Proceedings of the IEEE, 2016, 104(6): 1302 – 1317.

[22] XU G H, SHEN F, AMIN M, et al. DOA classification and CCPM-PC based GNSS spoofing detection technique[C]//Proceedings of the 2018 IEEE/ION Position, Location and Navigation Symposium (PLANS), 2018: 389 – 396.