DOI:10.13878/j.cnki.jnuist.2023.02.014

唐洪军[1]　黄治磊[2]　曾浩[2]

GNSS 中基于调零天线的欺骗干扰抑制方法

摘要

欺骗式干扰由于实现成本低、干扰能力强,成为 GNSS 中主流干扰来源,但现有 GNSS 抗干扰天线仅仅针对压制式干扰.根据欺骗式干扰检测获得的干扰到达方向信息,采用人为在该角度增加压制式干扰的方法,现有 GNSS 调零天线就可以在欺骗干扰角度形成方向图零陷,实现欺骗干扰抑制.通过对天线方向图和接收机扩频码同步仿真,验证了新方法的有效性.

关键词

欺骗干扰;干扰抑制;调零天线;全球导航卫星系统

中图分类号 TN967.1

文献标志码 A

收稿日期 2022-06-14

资助项目 "十四五"国防预研基金(629010204)

作者简介

唐洪军,男,高级工程师,主要从事高速信号采集、数字阵列信号处理平台等相关研究.a_thj@163.com

曾浩(通信作者),男,博士,教授,主要从事自适应阵列天线技术、软件无线电和宽带移动通信技术研究.haoz@cqu.edu.cn

1　西南电子技术研究所,成都,610036

2　重庆大学 微电子与通信工程学院,重庆,400044

0　引言

全球导航卫星系统(Global Navigation Satellite System,GNSS)因其可为各类军民载体提供全天候高精度的定位、测速和授时(Position Velocity Time,PVT)服务而得到广泛应用.由于卫星导航信号的脆弱性,GNSS 接收机极易受到恶意人为干扰,使得平台导航系统失效[1].一般 GNSS 调零天线针对压制式干扰,但从近几年针对无人武器平台的 GNSS 干扰热门事件来看,欺骗式干扰的威胁越来越大,这是因为欺骗式干扰信号不易被 GNSS 接收机察觉,并且随着软件无线电技术的发展,欺骗干扰设备所需成本也越来越低.转发式欺骗干扰技术上容易实现,成本低,是目前最主要的欺骗干扰方式.抗欺骗式干扰技术可分为欺骗干扰检测和欺骗干扰抑制:欺骗干扰检测主要实现对接收信号中是否存在欺骗干扰信号进行检测[2];欺骗干扰抑制主要实现消除欺骗干扰信号对 GNSS 系统的影响[3].对欺骗干扰抑制方法的研究相对其检测方法要少很多,特别是不改变 GNSS 编码结构下的接收机自主抑制方法尤其困难.目前研究较多的欺骗抑制方法有残留信号检测算法,其根据欺骗干扰源无法将真实卫星信号完全抵消,从 GNSS 接收机接收信号的缓冲样本中将系统重构建的欺骗信号减去,即可实现对欺骗干扰的消除[4],该方法对欺骗干扰抑制的效果属于中等水平,需要额外的存储空间和专门用于重构欺骗信号的通道,并且在欺骗信号功率明显大于真实卫星信号时,因检测不到真实信号而失效.接收机自主完整性监测(Receiver Autonomous Integrity Monitoring,RAIM)是另一种欺骗干扰抑制方法,其把欺骗干扰信号当成故障信号,通过比较伪距测量值而剔除因存在欺骗信号而导致的异常值,从而实现对欺骗干扰的抑制[5],该方法成本低,实现简单,但欺骗信号只能是一个.最可靠的是空域零陷控制算法,由于欺骗干扰大多采用单天线发射,因此信号到达方向(Direction of Arrival,DOA)是区分真实信号和欺骗信号的可靠因素,在判断出欺骗信号来向的基础上[6],可通过零陷形成技术降低欺骗信号方向上的增益,实现对欺骗干扰的抑制[7].该方法虽然能达到良好的抑制效果,但是由于需要进行矩阵求逆运算,算法复杂度较高.针对上述问题,本文提出一种基于调零天线的欺骗干扰抑制算法,能弥补残留信号检测算法和 RAIM 算法的不足,相对于空域零陷控制算法,运算复杂度更低.

本文首先分析欺骗干扰信号模型,然后提出基于调零天线的欺

骗干扰抑制算法,最后通过 MATLAB 仿真验证该算法的可行性.

1 欺骗式干扰信号模型

GNSS 接收机的基本结构如图 1 所示,整体分为天线、射频前端、信号处理、定位 4 个部分.通常,GNSS 接收机射频前端输出为中频信号,中频信号转换为数字信号后,通过各种信号处理算法实现不同功能,包括了干扰信号检测和抑制等[8].而干扰抑制后的信号,则进入接收机,实现载体定位和授时功能[9].

GNSS 接收机天线为阵列天线.在存在欺骗干扰的情况下,其单元接收信号包括了欺骗干扰、卫星信号、噪声 3 个部分,可以表示为

$$x(t)=\sum_{i=1}^{M}x_{\mathrm{T}i}(t)+\sum_{j=1}^{J}x_{\mathrm{S}j}(t)+n(t),\tag{1}$$

其中:$x_{\mathrm{T}i}(t)$ 表示第 i 个卫星的真实信号,M 表示真实信号的个数;$x_{\mathrm{S}j}(t)$ 表示第 j 个卫星的欺骗式干扰信号,J 表示欺骗信号的个数;$n(t)$ 为噪声信号.由于 GNSS 卫星采用了直接序列扩频技术,所以卫星 i 的信号在接收机处的信号可表示为

$$x_{\mathrm{T}i}(t)=\sqrt{P_{\mathrm{T}i}}C_{\mathrm{T}i}(t-\tau_{\mathrm{T}i})D_{\mathrm{T}i}(t-\tau_{\mathrm{T}i})\cos(2\pi f_0 t+\varphi_{\mathrm{T}i}),\tag{2}$$

其中:$P_{\mathrm{T}i}$ 为接收机接收的卫星 i 信号的功率;$C_{\mathrm{T}i}(t)$ 为接收机接收的卫星 i 信号的伪随机噪声(Pseudo Random Noise, PRN)码;$D_{\mathrm{T}i}(t)$ 为接收机接收的卫星 i 信号的导航数据码;$\tau_{\mathrm{T}i}$ 为接收机接收的卫星 i 信号的码相位;f_0 为中心频率;$\varphi_{\mathrm{T}i}$ 为载波相移.

由于转发式欺骗干扰信号是对真实卫星信号的延时和功率放大,即欺骗信号和真实卫星信号具有相同的信号结构,因此,卫星 i 对应的欺骗信号可以表示为

$$\begin{aligned}x_{\mathrm{S}i}(t)&=kx_{\mathrm{T}i}(t)(t-\Delta t)=\\&k\sqrt{P_{\mathrm{T}i}}C_{\mathrm{T}i}(t-\tau_{\mathrm{T}i}-\Delta t)D_{\mathrm{T}i}(t-\tau_{\mathrm{T}i}-\Delta t)\cdot\\&\cos(2\pi f_0(t-\Delta t)+\varphi_{\mathrm{T}i}),\end{aligned}\tag{3}$$

其中:Δt 即为欺骗干扰相对于真实卫星信号的延时;k 为欺骗信号对真实卫星信号功率放大系数.

根据图 1 所示的接收机结构,欺骗式干扰的检测算法在信号处理阶段完成,输入信号为数字中频信号.另外,天线采用均匀面阵,但为了叙述简便,假设阵列天线为 $L+1$ 个阵元构成的均匀线型阵列,信号处理模块把中频模拟信号经过 ADC 转换为中频数字信号 $\boldsymbol{x}(k)$,其中 $\boldsymbol{x}(k)$ 为 $L+1$ 维列矢量,每个元素对应一个阵元接收信号,k 为采样序号.根据阵列天线基本理论,接收信号表示为

$$\begin{aligned}\boldsymbol{x}(k)&=\begin{bmatrix}x_0(k)\\\vdots\\x_L(k)\end{bmatrix}=\\&\sum_{i=1}^{M}x_{\mathrm{T}i}(k)\boldsymbol{v}(\theta_i)+\sum_{j=1}^{J}x_{\mathrm{S}j}(k)\boldsymbol{v}(\theta_j)+\boldsymbol{n}(k),\end{aligned}\tag{4}$$

式中,$\boldsymbol{v}(\theta)$ 表示入射角度为 θ 的信号或者干扰的方向矢量,$\boldsymbol{n}(k)$ 为噪声矢量.

2 基于调零天线的欺骗干扰抑制方法实现

2.1 算法结构

基于调零天线的欺骗干扰抑制的目的是在欺骗干扰的来波方向上形成零陷来实现对欺骗干扰的抑制.经典文献[10]指出,基于功率倒置(Power Inversion, PI)算法的调零天线能在强干扰处产生零陷,而对微弱的欺骗信号是不适用的.由于 PI 算法的调零天线实现简单可靠,因此,本文所提算法的思想是人为构建大功率信号,模拟其从欺骗信号 DOA 入射,以使调零天线能在该方向生成零陷,从而实现对该

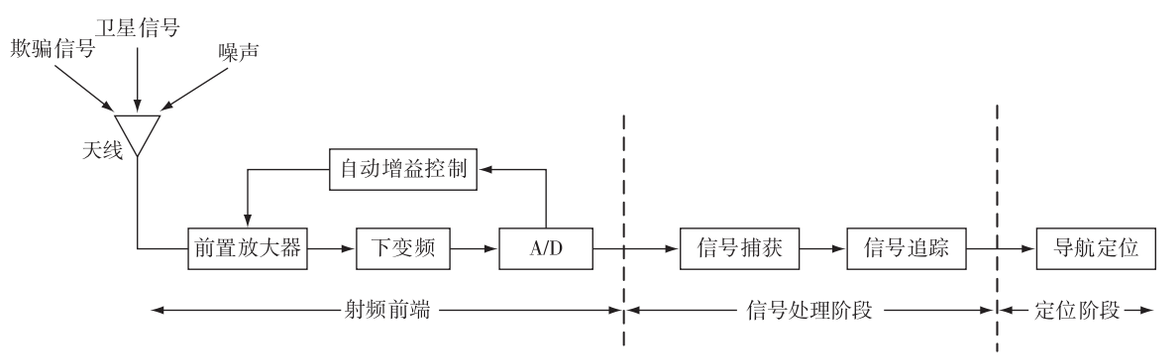

图 1 GNSS 接收机的通用内部结构

Fig. 1 General internal structure of GNSS receiver

方向信号的抑制,即欺骗干扰信号的抑制.欺骗式干扰的入射角度需要通过 DOA 估计方法得到,比如阵列信号处理中的自适应滤波算法[11].

基于调零天线的欺骗干扰抑制算法结构如图 2 所示,主要包含压制式干扰生成模块、信号求和模块和调零天线模块 3 部分,其中压制式干扰生成模块和信号求和模块主要是完成调零天线输入信号的产生.基于调零天线的欺骗干扰抑制算法结构具体实现步骤如下:

1)压制式干扰生成模块根据欺骗干扰的 DOA 信息,人工模拟产生 J 个大功率的带通信号,其中 J 是接收信号中的欺骗干扰个数;

2)信号求和模块将卫星导航接收阵列接收信号和压制式干扰模块产生的人工干扰求和作为调零天线模块的输入;

3)调零天线模块对其输入信号进行权值求解和加权求和,最终将零陷对准欺骗干扰信号,从而实现对欺骗干扰的抑制.

压制式干扰生成模块和信号求和模块是对调零天线模块输入信号的生成.

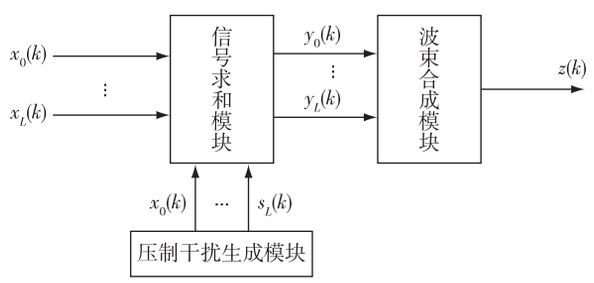

图 2 基于调零天线的欺骗干扰抑制算法结构

Fig. 2 Structure of anti-spoofing algorithm based on nulling antenna

2.2 人工干扰信号生成

根据图 2 所示结构,调零天线新的输入就是真实输入和压制干扰生成模块输出二者的叠加.压制式干扰生成模块根据欺骗式干扰入射角度 θ_j,人工产生任意 J 个不相干的大功率带通信号:

$$\boldsymbol{s}_j(k)=a_j(k)\cdot \mathrm{e}^{\mathrm{j}\omega_c kT_s}\boldsymbol{v}(\theta_j), \tag{5}$$

其中,$a_j(k)$ 为高斯分布随机序列,ω_c 为卫星信号的中频载波频率,T_s 为采样周期,$\boldsymbol{v}(\theta_j)$ 为第 j 个欺骗干扰信号的方向矢量,$j=1,\cdots,J$.将上述 J 个人工生成的压制式干扰信号求和得到

$$\boldsymbol{s}(k)=\sum_{j=1}^{J}\boldsymbol{s}_j(k), \tag{6}$$

其中,$\boldsymbol{s}(k)$ 是 $L+1$ 维列矢量.

信号求和模块将卫星导航接收机天线阵面的接收信号 $\boldsymbol{x}(k)$ 和压制式干扰模块产生的人工干扰 $\boldsymbol{s}(k)$ 进行求和:

$$\boldsymbol{y}(k)=\boldsymbol{s}(k)+\boldsymbol{x}(k)=[y_0(k)\quad\cdots\quad y_L(k)]^{\mathrm{T}}. \tag{7}$$

以上求和结果 $\boldsymbol{y}(k)$ 作为调零天线的输入.显然,$\boldsymbol{y}(k)$ 也是 $L+1$ 维列矢量.

2.3 调零天线结构

同样采用 $L+1$ 个阵元构成的均匀线阵,阵元间距为载波波长的一半的阵列结构对调零天线进行介绍.可用图 3 表示调零天线的原理结构组成,其主要采用功率倒置算法实现抗干扰功能.调零天线模块输入信号为

$$\boldsymbol{y}(k)=[y_0(k)\quad\cdots\quad y_L(k)]^{\mathrm{T}}, \tag{8}$$

其中,输入信号包含真实卫星信号、欺骗干扰信号和噪声信号.为了将其形式化表达,将阵元 0 对应信号 $y_0(k)$ 作为调零天线参考阵元接收到的信号 $d(k)$,假设其接收真实卫星信号为 $s_{\mathrm{T}}(k)$,空间存在 J 个欺骗干扰信号 $s_{\mathrm{S}j}(k)$,噪声信号表示为 $n_0(k)$,则参考信号 $d(k)$ 可用下式表示:

$$d(k)=s_{\mathrm{T}}(k)+\sum_{j=1}^{J}s_{\mathrm{S}j}(k)+n_0(k). \tag{9}$$

其余 L 个阵元对应信号作为辅助阵元信号 $\boldsymbol{y}_a(k)=[y_1(k)\quad\cdots\quad y_L(k)]^{\mathrm{T}}$,其接收信号矢量可写为

$$\boldsymbol{y}_a(k)=[y_2(k)\quad y_3(k)\quad\cdots\quad y_L(k)]^{\mathrm{T}}=$$

$$s_{\mathrm{T}}(k)\boldsymbol{v}_a(\theta_m)+\sum_{j=1}^{J}s_{\mathrm{S}j}(k)\boldsymbol{v}_a(\theta_j)+\boldsymbol{n}(k), \tag{10}$$

式中:$\boldsymbol{v}_a(\theta_m)$,$\boldsymbol{v}_a(\theta_j)$ 分别为真实卫星信号和欺骗干

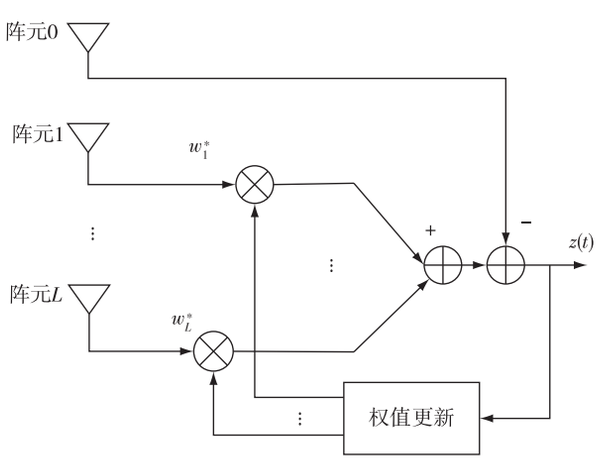

图 3 调零天线结构

Fig. 3 Structure of nulling antenna

扰信号的方向矢量;$\boldsymbol{n}(k)$ 为辅助阵元阵列接收到的噪声信号.

由于真实卫星信号本身强度就相对较弱,再经过扩频调制之后,其信号强度甚至会远低于噪声信号的强度.那么,式(9)可近似表示成

$$d(k) \approx \sum_{j=1}^{J} s_{Sj}(k) + n_0(k). \tag{11}$$

式(10)可写为

$$\boldsymbol{y}_a(k) = [y_1(k) \quad y_2(k) \quad \cdots \quad y_L(k)]^{\mathrm{T}} \approx \sum_{j=1}^{J} s_{Sj}(k)\boldsymbol{v}_a(\theta_j) + \boldsymbol{n}(k). \tag{12}$$

经过自适应滤波之后,非参考阵元阵列的权矢量可表示成

$$\boldsymbol{w}_a = [w_1 \quad w_2 \quad \cdots \quad w_L]^{\mathrm{T}}. \tag{13}$$

经过加权处理后的调零天线输出信号为

$$z(t) = d(t) - \boldsymbol{w}_a^{\mathrm{H}}\boldsymbol{y}_a(t). \tag{14}$$

阵列方向图可以表示为

$$B(\theta) = |\boldsymbol{w}^{\mathrm{H}}\boldsymbol{v}(\theta)|. \tag{15}$$

式(15)中的权值和方向矢量包含了第 0 个阵元的信息,所以

$$\boldsymbol{w} = [-1 \quad \boldsymbol{w}_a]^{\mathrm{T}}. \tag{16}$$

2.4 权值求解方法

调零天线图 3 中的权值更新模块通常采用最小均方(Least Mean Square, LMS)算法计算权值.LMS 算法的工作原理是使参考阵元和非参考阵元阵列接收信号的均方误差最小化,并通过当前时间的权矢量与调零天线输入迭代计算后一时刻的权矢量值,重复以上运算直到权矢量收敛[12].该算法具体实现步骤如下:

1)设置初始取值为 0 的权矢量 $\boldsymbol{w}_a(0)$ 与迭代步长 μ,$0 < \mu < 2/\lambda_{\max}$,其中 $\lambda_{\max}$ 为调零天线输入信号协方差矩阵的最大特征值;

2)计算此时非参考阵元阵列输出信号 $u(k) = \boldsymbol{w}_a^{\mathrm{H}}\boldsymbol{y}_a(k)$;

3)利用参考阵元接收信号,计算阵列输出信号 $z(k) = d(k) - u(k)$;

4)依据快拍数 k,对权矢量进行更新 $\boldsymbol{w}_a(k+1) = \boldsymbol{w}_a(k) + \mu\boldsymbol{y}_a(k)z^*(k)$;

5)回退执行 2),直到权矢量收敛;

6)权矢量收敛后,将最后的 $z(k)$ 作为调零天线输出信号.

3 算法性能分析

空域零陷控制算法和本文提出的基于调零天线的欺骗干扰抑制算法都能达到较好的欺骗抑制效果,但是二者算法复杂度存在区别.

空域零陷控制算法满足以下条件即可实现对欺骗干扰的抑制.

$$\begin{cases} \boldsymbol{w}^{\mathrm{H}}\boldsymbol{v}_0 = 1, \\ \text{s.t.} \quad \boldsymbol{w}^{\mathrm{H}}\boldsymbol{v}_i = 0, \quad i = 1, \cdots, K, \end{cases} \tag{17}$$

其中:$\boldsymbol{v}_0$,$\boldsymbol{v}_i$ 分别为真实信号和欺骗信号的方向矢量;K 为接收信号中存在的欺骗信号来向个数.若矩阵

$$\boldsymbol{T} = [\boldsymbol{v}_0 \quad \boldsymbol{v}_1 \quad \cdots \quad \boldsymbol{v}_K], \tag{18}$$

则式(17)可写为

$$\boldsymbol{w}^{\mathrm{H}}\boldsymbol{T} = \boldsymbol{e}_1^{\mathrm{T}} = [1 \quad 0 \quad \cdots \quad 0]. \tag{19}$$

因此,求得最优权矢量表达式为

$$\boldsymbol{w}_{\mathrm{null}}^{\mathrm{H}} = \boldsymbol{e}_1^{\mathrm{T}}\boldsymbol{T}^{-1} = \boldsymbol{e}_1^{\mathrm{T}}\boldsymbol{T}^{\mathrm{H}}(\boldsymbol{T}\boldsymbol{T}^{\mathrm{H}})^{-1}. \tag{20}$$

由式(20)可知,空域零陷控制算法对权矢量的求解涉及到矩阵求逆 $\boldsymbol{T}^{-1}$ 运算,而通常仅矩阵求逆算法的复乘计算量就能达到 L^4 的数量级,其中 L 是阵元数.而采用 LMS 算法计算权值的调零天线只需对权值简单地进行迭代即可确定最优权矢量值,复乘计算量最高达到 L^3 的数量级.当然,两种算法的具体复杂度还跟采样快拍有关.但从以上推导可以得出:基于调零天线的欺骗干扰抑制算法复杂度比空域零陷控制算法复杂度有所降低.

4 仿真分析

下面对本文提出的欺骗干扰抑制方法进行仿真分析,假设接收机阵列为 8 阵元均匀线阵,阵元间距为 0.5 倍波长,仿真假设接收机接收信号包括了一个卫星信号,信号来向分别为 30°,两个转发式欺骗干扰信号,信号来向为-40°和 60°,以及噪声信号.为了简单,GNSS 接收机仅仅研究 L1 频段的 GPS 信号,PRN 码为长度是 1 023 的 GOLD 码,码速率为 1.023 MHz,接收信号通过射频前端转换为中频信号,中频频率 4.092 MHz,采样频率为 37.851 MHz,信号信噪比 SNR = -20 dB,干噪比 INR = -19 dB.噪声为功率为 1 的高斯白噪声.

用大功率带通信号 $s(k) = a(k) \cdot \mathrm{e}^{j\omega_c kT_s}$ 模拟两个压制式干扰,其中 $a(k)$ 为均值为 0,功率为 INR = 10 dB 的高斯分布随机序列.两个人为干扰的区别是基带信号 $a(k)$ 独立生成,彼此不相关.其时域波形和频谱图分别如图 4、5 所示,两个人为干扰时域波形不同,但频谱是相同的.

然后,根据式(7)和式(14)对 GNSS 接收机接收

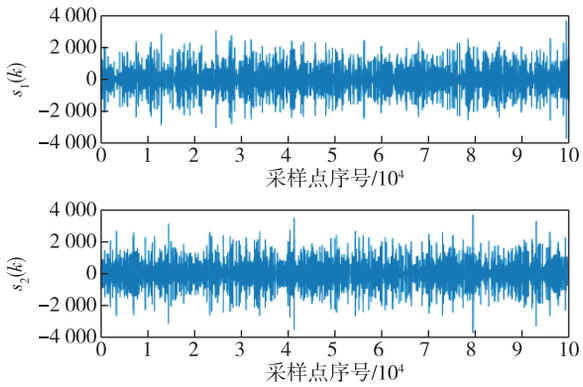

图 4　带通信号时域波形

Fig. 4　Time domain waveform of bandpass signal

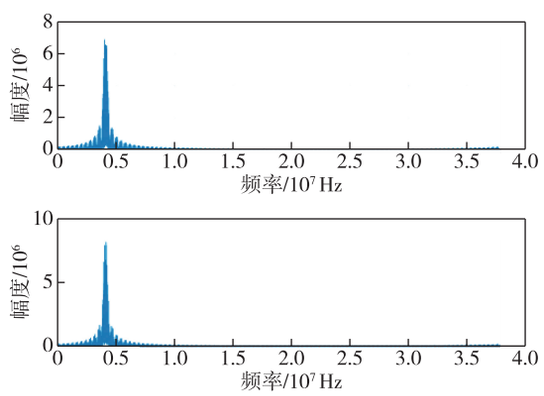

图 5　带通信号频谱

Fig. 5　Spectrum of bandpass signal

信号进行调零天线抗干扰处理.采用 LMS 算法计算最优权矢量,图 6 为根据式(15)计算的调零天线方向图.当不增加人为干扰时,由于欺骗信号功率太弱,无法形成零陷,方向图是水平实线.当采用本文方法后,在-40°和 60°两个干扰信号方向,都能够形成零陷.

欺骗干扰通常和真实卫星信号功率相当,都较弱.调零天线主要目的是减小欺骗干扰功率,保持真实信号功率不变,这些都可以从干扰和真实信号 DOA 对应的方向图上看出.为此,在相同假设条件下改变阵元数量和人为干扰功率,对真实信号、两个干扰信号天线增益进行仿真,如图 7、图 8 所示.仿真结果说明,真实信号功率和天线数量、人为干扰功率大小没有显著关系.图 7 显示,欺骗式干扰抑制度在天线数量满足自由度要求后,维持在-55 dB 左右,不随天线数量增加而增加.图 8 显示,干扰功率对干扰抑制度影响显著,干扰功率越大,抑制越多.

抗干扰模块在抑制干扰时,不能对真实信号产

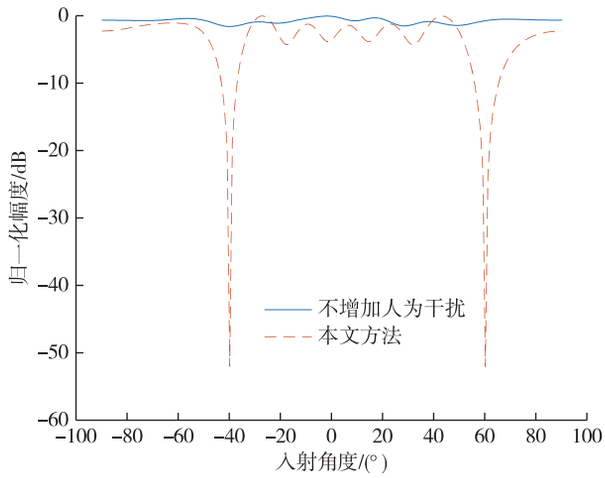

图 6　两种情况调零天线方向图

Fig. 6　Directional diagram of nulling antenna in two cases

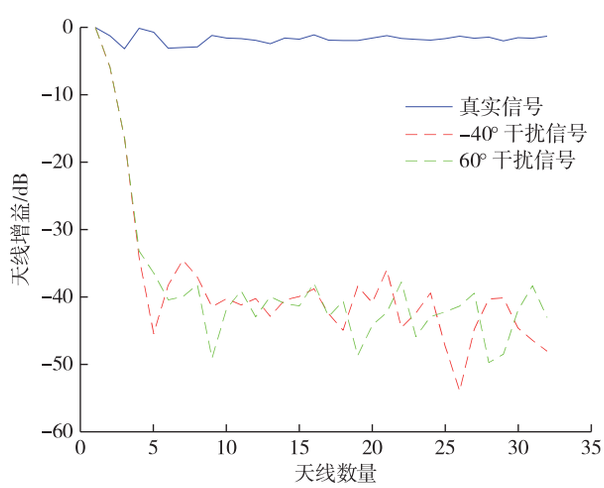

图 7　天线增益与天线数量关系

Fig. 7　Relationship between antenna gain and antenna number

生较大影响,至少要保证真实信号能够被 GNSS 接收机中 PN 码检测器正常检测到相关峰.根据扩频通信接收中相关峰检测方法,对抗干扰前后信号进行分析.图 9 为未进行欺骗干扰抑制接收机捕获的相关峰,仿真中可以看到接收机捕获到 3 个相关峰,说明接收信号中存在 2 个欺骗干扰信号.干扰抑制后,同样进行相关峰检测,如图 10 所示,则只有一个相关峰,说明干扰信号被有效抑制,并且真实卫星信号得到了有效保护.

5　结论

通过阵列天线接收信号在空域的处理,可以确定干扰信号角度,然后人为把欺骗式干扰转换为压

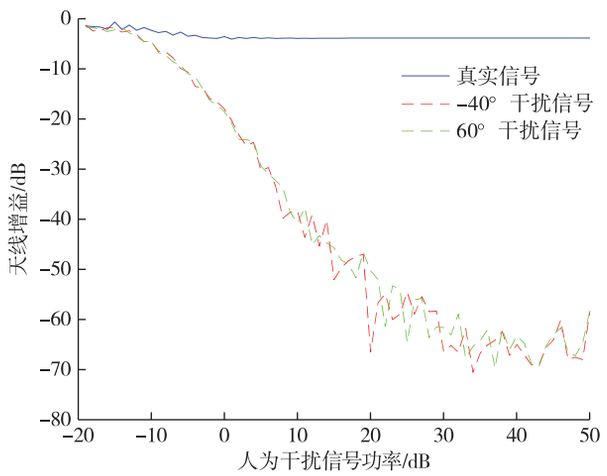

图 8　天线增益与干扰功率关系

Fig. 8　Relationship between antenna gain and interference power

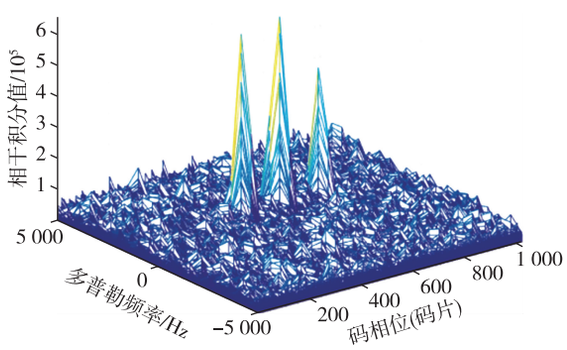

图 9　干扰抑制前接收机捕获相关峰

Fig. 9　Correlation peak captured by receiver before interference suppression

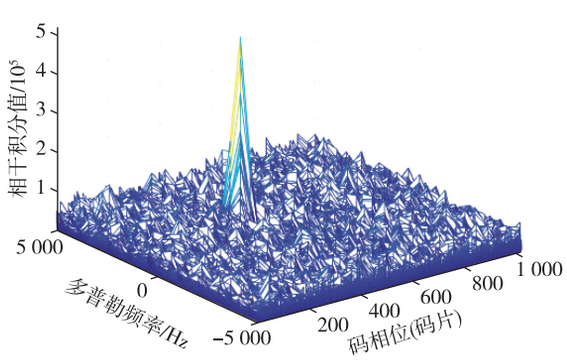

图 10　干扰抑制后接收机捕获相关峰

Fig. 10　Correlation peak captured by receiver after interference suppression

制式干扰,再采用传统调零天线算法在欺骗干扰方向形成天线方向图零陷,从而实现对欺骗干扰抑制.通过 MATLAB 仿真实验验证了算法的可行性,对于 GNSS 抗干扰天线工程设计具有参考价值.

参考文献

References

[1] Lu Q, Feng X Z, Zhou C. A detection and weakening method for GNSS time-synchronization attacks[J]. IEEE Sensors Journal, 2021, 21(17): 19069-19077

[2] Li J Z, Zhu X W, Ouyang M J, et al. Research on multi-peak detection of small delay spoofing signal[J]. IEEE Access, 8: 151777-151787

[3] Feng W K, Friedt J M, Goavec-Merou G, et al. Software-defined radio implemented GPS spoofing and its computationally efficient detection and suppression[J]. IEEE Aerospace and Electronic Systems Magazine, 2021, 36(3): 36-52

[4] Wesson K, Shepard D, Humphreys T, et al. Straight talk on anti-spoofing securing the future of PNT[J]. GPS World, 2012, 3(4): 65-70

[5] Sun Y, Fu L. A new threat for pseudorange-based RAIM: adversarial attacks on GNSS positioning[J]. IEEE Access, 2019, 7: 126051-126058

[6] 孙凤林,尹继亮,李凤,等.GNSS 欺骗干扰的空时联合检测算法[J].计算机仿真,2022,39(5):60-65
SUN Fenglin, YIN Jiliang, LI Feng, et al. Space-time joint detection algorithm for GNSS spoofing interference[J]. Computer Simulation, 2022, 39(5): 60-65

[7] Hu Y F, Bian S F, Li B, et al. A novel array-based spoofing and jamming suppression method for GNSS receiver[J]. IEEE Sensors Journal, 2018, 18(7): 2952-2958

[8] 刘丁浩,吕晶,马蕊,等.卫星导航系统欺骗与抗欺骗技术研究与展望[J].通信技术,2017,50(5):837-843
LIU Dinghao, LÜ Jing, MA Rui, et al. The research and prospect of spoofing and anti-spoofing technology in the satellite navigation system[J]. Communications Technology, 2017, 50(5): 837-843

[9] Rychlicki M, Kasprzyk Z, Rosiński A. Analysis of accuracy and reliability of different types of GPS receivers[J]. Sensors (Basel, Switzerland), 2020, 20(22): 6498-6511

[10] Compton R T. The power-inversion adaptive array: concept and performance[J]. IEEE Transactions on Aerospace and Electronic Systems, 1979, 15(6): 803-814

[11] Zeng H, Ahmad Z, Zhou J W, et al. DOA estimation algorithm based on adaptive filtering in spatial domain[J]. China Communications, 2016, 13(12): 49-58

[12] Meng D W, Feng Z M, Lu M Q. Anti-jamming with adaptive arrays utilizing power inversion algorithm[J]. Tsinghua Science & Technology, 2008, 13(6): 796-799

南京信息工程大学学报(自然科学版),2023,15(2):237-243
Journal of Nanjing University of Information Science & Technology(Natural Science Edition),2023,15(2):237-243

Anti-spoofing via nulling antenna in GNSS

TANG Hongjun[1] HUANG Zhilei[2] ZENG Hao[2]
1 Southwest Institute of Electronic Technology, Chengdu 610036
2 School of Microelectronics and Communication Engineering, Chongqing University, Chongqing 400044

Abstract Nowadays spoofing is the dominant threats for GNSS receiver due to its low cost and high efficiency. However, the nulling antenna, which is widely used in GNSS receiver, can only mitigate the interference via high power. According to the DOA information of spoofing, some pseudo interferences are added to the received signal and imping on the antenna array from the same DOAs as the spoofing. Then the following traditional nulling antenna can suppress the spoofing since the beam pattern generate nulls at the DOAs of spoofing. Finally, the simulations of beam pattern and PN code synchronization illustrate the performance of the proposed method.

Key words spoofing; jamming mitigation; nulling antenna; global navigation satellite system(GNSS)