doi:10.3772/j.issn.1002-0470.2015.01.002

基于多天线的欺骗式干扰检测技术研究①

罗显志② 范广伟

(中国电子科技集团第54研究所 石家庄 050081)

(河北省卫星导航技术与装备工程技术研究中心 石家庄 050081)

摘 要 根据卫星导航系统抗欺骗式干扰的需要,进行了欺骗式干抗检测技术研究,并针对常规的欺骗式干扰检测方法仅对特定欺骗式干扰检测有效的问题,提出了一种基于多天线的欺骗式干扰检测算法。该算法利用欺骗式干扰信号与本地码解扩后功率增强来实现多阵元信号测向,并与星历解算出来的卫星位置进行比较实现多阵元的欺骗式干扰检测,而且充分利用卫星导航接收系统已有的先验知识,采用高分辨测向的方法实现多种欺骗式干扰的检测。仿真结果表明,该算法对产生式欺骗和转发式欺骗均具有较好的检测性能。

关键词 卫星导航接收系统,波达方向(DOA),欺骗式干扰,解扩

0 引 言

近年来,随着电子技术的发展和一些导航频率保护政策的不断健全,欺骗式干扰(spoofing)逐渐上升为北斗导航系统在民用领域的主要威胁[1],它严重影响了北斗导航系统区域导航定位和系统授时的服务质量,因此有必要对其进行检测与消除。欺骗式干扰是指通过发射与卫星导航信号具有相同参数(只有信息码不同)的假信号来干扰卫星导航接收机,使其产生错误的定位信息。欺骗式干扰分为产生式欺骗干扰[2,3]和转发式欺骗干扰两种形式。欺骗式干扰对导航系统造成的严重影响日益受到国际上的重视,全球卫星导航系统国际委员会(ICG)在每年的会议上都设专题来讨论欺骗式干扰的检测与消除技术,国内外的一些学者也研究了欺骗式干扰的检测,并提出了一些检测方法,例如国内黄龙等[3]对欺骗式干扰的检测方法进行了研究,周轩等[4]对卫星导航系统的反欺骗技术进行了总结和展望;国外 Nielsen 等[5]提出了一种利用手持单天线接收机对欺骗式干扰进行检测的方法,美国德州大学的学者 Montgomery 等[6]提出了利用两个天线接收到的相位差的变化进行欺骗式干扰检测的方法。分析表明,现有方法主要是应用卫星的功率变化速率、载噪比绝对值、不同频点信号的相对功率、伪距变化速率、多普勒频移变化速率、L1 与 L2 的互相关、L1-L2 伪距差分、观测量跳变等参数进行欺骗式干扰的检测与识别。本文在分析总结现有算法的研究基础上,利用导航信号捕获跟踪上的相关增益,提出了一种基于多阵元天线测向的欺骗式干扰检测与识别算法,并给出了设计原理及算法实现过程。该算法的有效性通过实验仿真得到了验证。在仿真过程中假设用户接收机动态和功率动态比较小,能够实现导航信号的捕获和跟踪,并且不考虑算法的处理时延。

1 欺骗式干扰模型

本文以 B1 频点 I 支路的民码信号为参考展开研究。B1 频点发射信号表达式为

① 863 计划(2011BAH05B03, 2012AA121802)资助项目。

② 男,1976 年生,博士,高级工程师;研究方向:卫星导航信号处理;联系人,E-mail: xianzhiluo@tom.con

(收稿日期:2014-09-02)

$$S^j = A_C C^j(t) D_C^j(t) \cos(2\pi f t + \varphi_C^j) + \cdots + A_P P^j(t) D_P^j(t) \sin(2\pi f t + \varphi_P^j) \quad (1)$$

式中:j 表示卫星标号;A_C 表示调制于 B1 频点载波 Q 支路的测距码振幅;C 表示 I 支路的测距码;P 表示 Q 支路的测距码;D_C 表示 I 支路测距码上调制的数据码;D_P 表示 Q 支路测距码上调制的数据码;f 表示 B1 频点的载波频率;φ_C 表示 B1 频点载波 I 支路的初相;φ_P 表示 B1 频点载波 Q 支路的初相。

接收端接收到的民码信号表达式为

$$x(t) = \sum_{j=1}^{M} A_C^j C^j(t-\tau_j) D_C^j(t-\tau_j) \cos(2\pi f_j(t-\tau_j) + \varphi_C^j) + N(t) \quad (2)$$

其中 τ_j 为第 j 颗卫星到接收机的时延,M 为可见卫星数,f_j 为第 j 颗卫星到达接收机含多普勒频移的频率,$N(t)$ 为接收机系统噪声。

产生式欺骗干扰是通过干扰产生器产生高逼真的欺骗信号,它的前提条件是需要知道卫星导航信号的码型和此时刻需要模拟卫星的导航电文,这对于公开码型的民码信号来说是可实现的,但对于加密的军码信号来说,目前实现难度较大。

B1 频点民码的产生式欺骗干扰模型可认为是 B1 频点的民码信号加一定的多普勒频移构成。对于接收端来说,当接收端含有转发式欺骗干扰时,接收端的接收信号可描述为

$$x(t) = \sum_{j=1}^{M} A_C^j C^j(t-\tau_j) D_C^j(t-\tau_j) \cos(2\pi f_j(t-\tau_j) + \varphi_C^j) + \sum_{l=1}^{L} A_C^l C^l(t-\tau_l) D_C^l(t-\tau_l) \cos(2\pi f_v(t-\tau_l) + \varphi_C^l) + N(t) \quad (3)$$

其中 L 表示产生式欺骗干扰的个数,A_C^l 表示第 l 个欺骗干扰的幅度,一般比真实信号高 5 ~ 10dB,$D_C^l(t)$ 为欺骗干扰上调制的数据码,f_v 表示相对 B1 频点有一定多普勒频移的载波频率。

转发式欺骗干扰是利用导航信号的自然延伸,接收天上的卫星导航信号,再通过一定的延迟放大处理,直接发射出去。延迟干扰不需要知道卫星导航信号的编码形式和此时刻的导航电文,因此实现起来较为简单,但是卫星导航信号到达地面的时间一般为 70 ~ 90ms,因此延迟后到达接收机的时间范围不能超过 90ms。当有转发式欺骗干扰时,接收端接收到的信号模型可描述为

$$x(t) = \sum_{j=1}^{M} A_C^j C^j(t-\tau_j) D_C^j(t-\tau_j) \cos(2\pi f_j(t-\tau_j) + \varphi_C^j) + \sum_{j=1}^{M'} A_C^{j'} C^j(t-\tau_j-\tau_{j'}) D_C^j(t-\tau_j-\tau_{j'}) \cos(2\pi f_v(t-\tau_j-\tau_{j'}) + \phi_C^j) + N(t) \quad (4)$$

其中 $A_C^{j'}$ 为转发式欺骗干扰的幅度,$\tau_{j'}$ 为转发式欺骗干扰的时延。

以北斗 B1 信号的民码为例,将接收到的一个伪码周期的信号与期望卫星信号的扩频码 $c_i(t-\tau_i)$ 做相关处理后的信号可描述为

$$y(\tau) = \frac{1}{2046 T_c} \int_{t=0}^{2045} x(t) c_i(t-\tau_i) \cos(2\pi f_i(t-\tau_i) + \varphi_i) \mathrm{d}t \quad (5)$$

其中 T_c 表示伪码中每个码片的时宽,f_i 为与接收信号同频的对应频率。通过上述处理,分别对每颗卫星进行的相关解扩处理,可以有效地提高期望信号的功率。

图 1 是 B1I 支路民码一个周期的伪码信号的相关函数图。图 1(a)是有一定码片时延的自相关函数图,图 1(b)是同一伪码起始相位不同叠加的自相关函数图。图 1(c)是一个周期的伪码和其它支路的伪码的互相关图。从图中可以看出,自相关能够产生一定的增益,同一伪码不同初始相位均能与已知初始相位的同一伪码产生相关峰,不同的伪码不

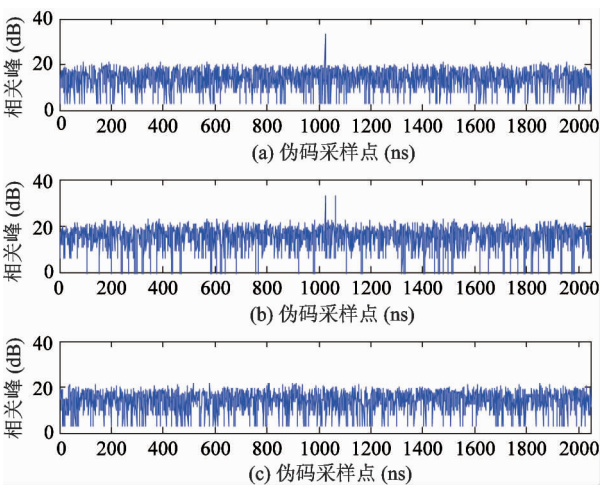

图 1　伪码相关函数

会产生相关峰。欺骗式干扰就是利用伪码能够与接收机不同通道本地码相关解扩之后的扩频增益实现对接收机的欺骗的,一般情况下,转发式欺骗干扰是转发接收机能够接收到的卫星信号,再通过一定的时延,放大处理发射出去,因此,受干扰接收机通道相关处理后会出现两个峰值,而产生式欺骗干扰是模拟接收机目前无法接收到的卫星导航信号和星历,不该捕获到信号的通道会出现相关峰。

2 相关后的阵列测向算法

假设北斗接收机的接收阵列采用均匀线阵,均匀线阵的 P 个相同的全向阵元均匀地分布在一条直线上,则 P 阵元的均匀线阵阵列导向矢量可描述为

$$a(\theta_i) = [1, e^{-j\omega_i}, \cdots, e^{-j(p-1)\omega_i}]^{\mathrm{T}} \tag{6}$$

其中 $\omega_i = \dfrac{2\pi \sin\theta_i d}{\lambda}$, θ_i 为波达方向, λ 为信号波长, d 为阵元间距,一般情况下 $d \leqslant \lambda/2$。

如果欺骗信号加正常导航信号总共有 M 个,则在第 p 个阵元上的接收信号为

$$x_p(t) = \sum_{i=1}^{M} a_p(\theta_i) s_i(t) + n_p(t) \tag{7}$$

式中 s_i 为来波信号, $a_p(\theta_i)$ 为目标信号 i 的导向矢量。与本地码做相关处理后的接收信号可表示为

$$h_p(\tau) = \sum_{i=1, i\neq j}^{M} a_p(\theta_i) q_i(t) + a_p(\theta_j) y_j(t) + n_p(t) \tag{8}$$

其中 j 对应接收机的第 j 个相关通道,由于 $q_i(t)$ 表示接收到的其它卫星信号与第 j 个通道的本地码相关的结果, $y_j(t)$ 表示第 j 通道的本地码与第 j 颗卫星信号的相关结果。

由于接收信号与本地码相关后,其它卫星信号与本地码相关结果相对第 j 颗卫星信号与本地码相关结果可以忽略不计,即 $q_i(t) << y_j(t)$, 所以式(8)又可简化为

$$h_p^j(\tau) = a_p(\theta_j) y_j(t) + n_p(t) \tag{9}$$

一般相关积分的长度选一个伪码周期,如果选择多个伪码周期则需要非相干积累。

将 P 个阵元第 i 个通道相关处理后的数据组成一个数据向量,可表示为:

$$\boldsymbol{H}^j(\tau) = [h_1^j(\tau), \cdots, h_p^j(\tau)]^{\mathrm{H}} \tag{10}$$

相关处理之后的协方差矩阵为

$$\boldsymbol{R}_{hh}^j = E[\boldsymbol{H}^j(t)\boldsymbol{H}^j(t)^{\mathrm{H}}] = A\boldsymbol{R}_{yy}A^{\mathrm{H}} + \sigma_N^2\boldsymbol{I} \tag{11}$$

其中 $\boldsymbol{R}_S = E[y_j(t) y_j(t)^{\mathrm{H}}]$ 为信号复包络协方差矩阵,$\boldsymbol{I}$ 为 P 维单位阵, σ_N^2 为阵元噪声功率。

根据子空间分解理论,如果信号源的个数少于阵列阵元个数,那么阵列数据的信号分量位于阵列协方差矩阵 $\boldsymbol{R}$ 的 1 个低秩空间上。分通道相关处理后,如果不存在欺骗干扰仅存在导航信号或仅存在产生式欺骗干扰,则只有一个大的信号分量;如果存在转发式欺骗干扰,则有可能存在两个大的信号分量。理论上,只要阵元个数大于 2 就能够通过特征分解把大的特征分量提取出来,因此,对 $\boldsymbol{R}$ 进行特征分解,并将其特征向量按照特征值的大小降序排列得到:

$$\begin{aligned}\boldsymbol{R} &= \boldsymbol{U}_s \sum\nolimits_s \boldsymbol{U}_s^{\mathrm{H}} + \boldsymbol{U}_n \sum\nolimits_n \boldsymbol{U}_n^{\mathrm{H}} \\ &= \sum_{m=1}^{K} \zeta_m e_m e_m^H + \sum_{m=K+1}^{M} \zeta_m e_m e_m^H \end{aligned} \tag{12}$$

R 中较大的特征值 $\zeta_1, \cdots, \zeta_K$ 对应于信号项,而 $P-K$ 个小的特征值对应于噪声项。因此,可以将 K 个特征向量 $e_1, e_2, \cdots, e_K$ 构成信号子空间;另外 $P-K$ 个特征向量 $e_{K+1}, \cdots, e_M$ 构成噪声子空间。由于信号的方向矢量 $a_i(\theta)$ 所张成的空间和特征向量 $\boldsymbol{U}_s$ 张成的空间相同,而信号子空间和噪声子空间正交,因此 $a_i(\theta)$ 和噪声子空间 $\boldsymbol{U}_n$ 正交, 利用信号子空间在噪声子空间上投影为零的性质,通过构造谱峰搜索来得到对信号波达方向的超分辨估计。

最后利用下面的公式进行空间谱估计:

$$P_{\mathrm{MUSIC}} = \frac{1}{a^H(\theta)(I - \boldsymbol{U}_n\boldsymbol{U}_n^{\mathrm{H}})a(\theta)} \tag{13}$$

其中 $a(\theta)$ 为信号波达方向矢量,$\boldsymbol{U}_n$ 为噪声子空间矢量, P_{MUSIC} 为估计的空间谱。

3 欺骗式干扰检测识别算法

欺骗式干扰检测识别算法多阵元的欺骗式干扰检测技术也是利用欺骗式干扰跟踪相关处理之后,有 60 ~ 70 分贝的相关增益,利用接收机跟踪上卫星

的伪码剥离后较高相关增益,可实现多阵元通道的欺骗式干扰测向,与星历解算出来的卫星位置进行对比即可实现欺骗式干扰的检测与识别。

检测与识别的流程如图 2 所示。多阵元接收机接收了来自空中的导航信号和欺骗式干扰,通过射频链路将信号放大到合适的幅度并将频率转换到需要的输出频率上,再通过模数转换器将输出信号转化为数字信号,然后每一路接收机相对每一路接收通道分别做捕获跟踪处理,接收机内部能同时复制出相应的载波和伪码信号,并且两者又分别与接收到该卫星信号中的载波和伪码保持同步一致,那么复制载波与接收信号进行混频可以实现载波剥离和信号解扩,这时在接收信号中剩下的便只是数据码,这时利用相关处理之后的增益,综合多个接收机对应卫星通道相关后的数据,采用 MUSIC 算法进行测向处理,测向得到的角度信息与接收机定位解算出的卫星位置信息进行对比,实现欺骗式干扰的检测与识别。

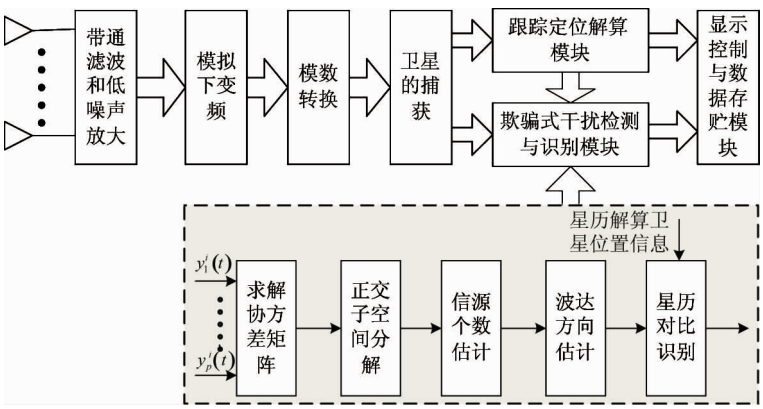

图 2　欺骗式干扰检测与识别流程图

为了验证相关后测向检测的性能,本研究对接收机捕获跟踪的流程进行了简化处理,并假定接收信号的频率和伪码起始相位已知,在这种情况下,在多阵元接收中实现欺骗式干扰检测与识别的算法的流程可描述如下:

(1) 初始化所有的参数设置。

(2) 利用式(8)解扩相应的通道接收到的信号。

(3)利用式(10)和式(11)求相关后的协方差矩阵。

(4)分解协方差矩阵得到信号子空间和噪声子空间。

(5)利用式(13)计算信号的波达方向。

(6)测出方向与星历解算出的卫星位置进行对比,确定此信号是欺骗式干扰还是导航信号。

(7)重复步骤(2) ~ (6),遍历所有接收通道,检测出接收信号中存在的所有欺骗式干扰。

4　算法仿真与性能分析

为了验证算法的性能,以北斗 B1 频点的民码信号作为参考进行了如下仿真验证。仿真中, B1 频点的导航信号调制的扩频码采用长度为 2046 的 Gold 码,调制方式为 BPSK,噪声为加性高斯白噪声,码速率为 2.046MHz/s,选取输入信噪比为 -25dB,接收机阵列模型采用 12 阵元的线阵模型,仿真模型中不考虑相同通道欺骗式干扰和真实卫星信号不同频的影响。

假设多天线接收机 1、2、3 通道有卫星信号进入,入射方位角分别为 10°、30°和 -60°。1、2 通道的卫星信号受到了 -70°方向的一个转发式欺骗干扰源的干扰,干扰的功率相对于噪声功率比为 -20dB,4 通道有一个产生式欺骗干扰进入,入射方向角为 60°,干噪比为 -20dB。对各个通道相关处理后分别做多阵元联合测向处理,得到的测向结果如图 3 所示。

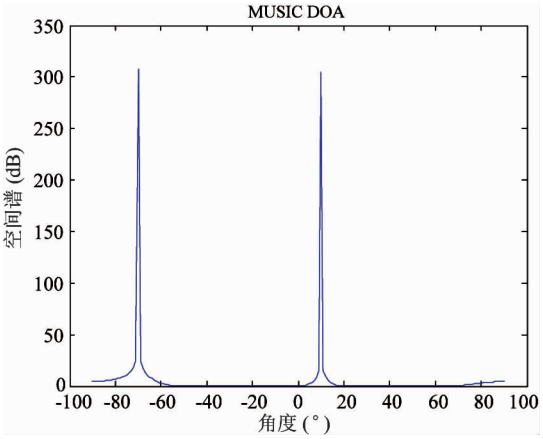

图 3　相关后 1 通道的测向

图 3 是 1 通道相关后的测向,从图中看出:在 10°和 -70°方向有检测到两个入射信号。因与接收机通道本地码相关后才有较高相关增益,而其它通道的信号与本通道本地码的互相关增益很小,可以忽略不计。一个通道收到两个不同方向的同一个相关信号,说明这个通道受到了转发式欺骗干扰的影响。与卫星星历解算出来的星历信息进行对比就可以确认哪个方向的信号是转发式欺骗干扰。

图 4 是通道 2 相关处理后的测向。从图中可以看出:即使转发式欺骗干扰与卫星信号的入射方向较近,本文提出的相关后测向的算法也能较好地把两个信号的方向检测出来,从而实现欺骗式干扰的识别。

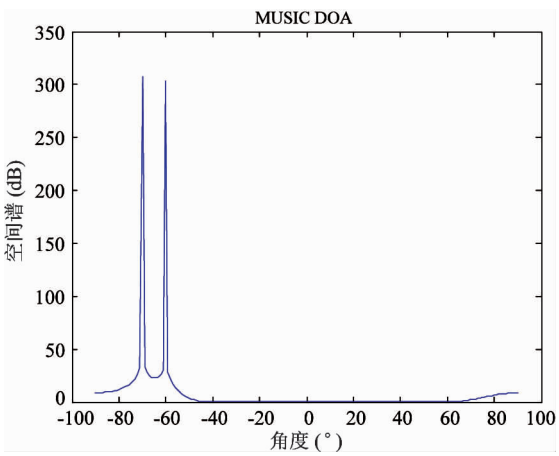

图 4　相关后 2 通道的测向

图 5 是通道 3 相关后的测向检测,从图中可以看出,如果没有针对此通道的欺骗式干扰,则针对其它通道的欺骗式干扰不会对该通道造成干扰。

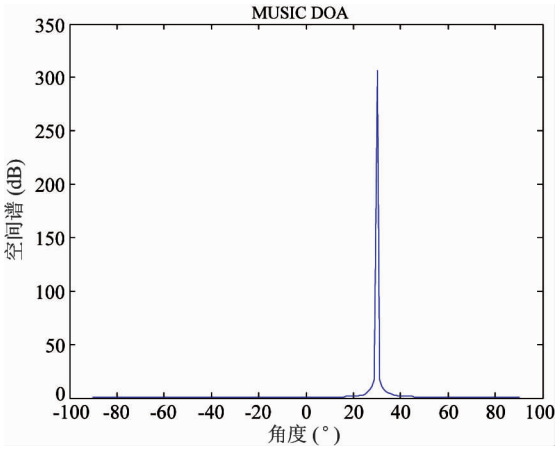

图 5　相关后 3 通道的测向

图 6 是通道 4 中相关测向后在 60°方向有一个信号进入,由于产生式欺骗干扰的入射方向星历很难做到与它模拟的卫星信号星历一致,因此可以依靠星历对比检测和识别是产生式欺骗干扰还是真实卫星信号。

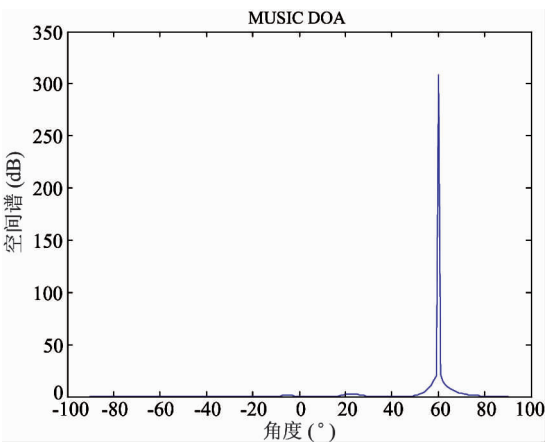

图 6　相关后 4 通道的测向

为验证本文提出的相关后测向检测识别算法估计性能,用均方根误差(RMSE)来描述算法的测向性能。均方根误差定义为

$$RMSE = \sqrt{E\{(\bar{\theta}' - \theta)^2\}} \tag{14}$$

其中 $\bar{\theta}'$ 为估计信号方向,θ 为真实信号方向。

仿真不同阵元数对相关后测向性能的影响。信号的入射方向为 30°,信噪比为 -20dB,采用线阵模型,阵元数从 6 个变换到 12 个,取 100 次平均,仿真

结果如图7所示。

图7是阵元数变化对测向精度的影响曲线。从图中可以看出:随着阵元数的增加,相关后的测角性能逐渐提高,且在6个阵元时的相关后测角性能已经能够达到0.15°左右,能够满足欺骗式干扰检测识别的要求。

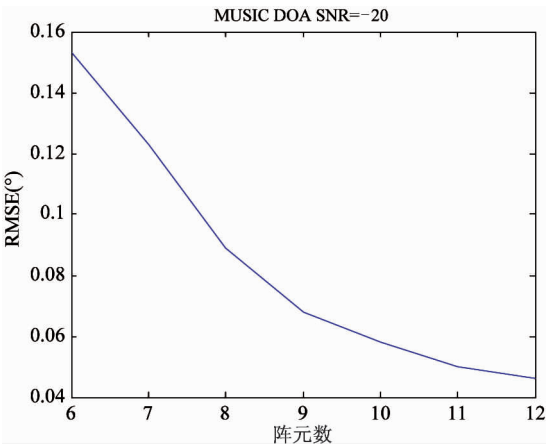

图7　阵元个数对测角误差的影响

仿真不同信噪比对相关后测向性能的影响。信号的入射方向为30°,信噪比为-20dB,采用12阵元的线阵模型,信噪比变化从-40dB开始,变化到-10db,每隔5dB取一个点,取100次平均,仿真结果如图8所示。

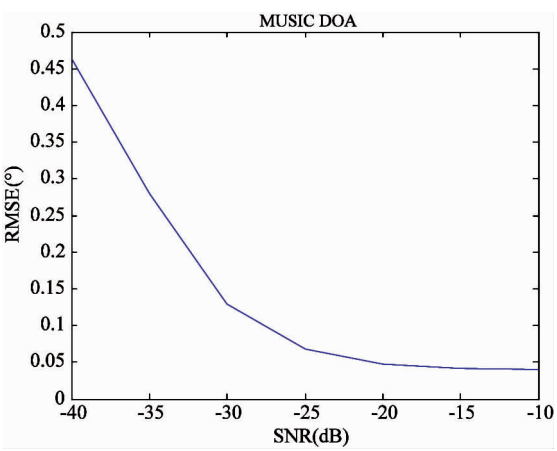

图8　信号功率对测角误差的影响

图8是信号功率对测角误差的影响曲线。从图中可以看出:随信噪比的增大,测角精度逐渐提高,在-25db的时候已经达到0.1°以下,一般的导航信号的信噪比集中在-25dB ~ -20dB左右,欺骗式干扰相对于导航信号功率略高,因此,本文提出的相关后测向的算法对欺骗式干扰和卫星信号均具有较好的测向性能,能够实现各种欺骗式干扰和卫星导航信号的检测与识别。

5　结　论

本文以北斗B1频点民码信号为基础,介绍了转发式和产生式欺骗干扰的接收模型,结合高分辨测向算法,利用接收信号相关解扩后的扩频增益,提出了一种基于多天线检测的欺骗式干扰检测与识别算法。本算法在信号相关解扩后完成来波信号方向的估计,并与星历解算出的卫星位置进行对比,来区分欺骗式干扰和正常的导航信号。仿真结果表明:本算法有较好的普适性,在导航信号功率范围内,对于转发式和产生式欺骗干扰均具有较好的检测性能;在较少的接收通道的情况下仍然具有较高的测量精度。该算法能有效地提高欺骗式干扰的检测性能。

参考文献

[1] Basker S. Jamming: A clear and present danger. *GPS World*, 2010,21(4):8-9

[2] 何四华,李天伟,韩云东. 导航战中GPS干扰技术研究. 舰船电子对抗,2004,27(1):24-27

[3] 黄龙,唐小妹,王飞雪. 卫星导航接收机抗欺骗干扰方法研究. 武汉大学学报(信息科学版),2011,36(11):1344-1347

[4] 周轩,李广侠,蔡定波等. 卫星导航系统反欺骗技术:回顾与展望. 见:第四届中国卫星导航学术年会论文集-S7 北斗/GNSS用户终端技术,湖北武汉,2013

[5] Nielsen J, Broumandan A, Lachapelle G. GNSS spoofing detection for single antenna handheld receivers. *Navigation*, 2012, 58(4): 335-344

[6] Montgomery P Y, Humphreys T E, Ledvina B M. A multi-antenna detection. *Inside GNSS*, 2009,4(2):40-46

Research on a multi-antenna based spoofing detection technique

Luo Xianzhi, Fan Guangwei

(The 54 Research Institute of China Electronics Technology Group Corporation, Shijiazhuang 050081)

(Hebei Satellite Navigation Technology and Equipment Engineering Technology Research Center, Shijiazhuang 050081)

Abstract

The spoofing detection was studied to meet the needs of satellite navigation systems' anti-spoofing, and a multi-antenna based spoofing detection algorithm was put forward to solve the problem that conventional spoofing detection methods are only used to deal with specific spoofing detections. The algorithm estimates the multi-array element signal direction by the power amplifying of the dispreading signal of the spoofing signal & local code, and realizes the multi- array elements spoofing detection by comparing to the satellite position from the ephemeris. Furthermore, based on the priori knowledge of the satellite navigation receiver system, this algorithm can realize a spoofing detection with high precision. The simulation results showed that the algorithm achieved a good detection result for spoofing and transmitting interference.

Key words: satellite navigation receiver system, direction of arrival (DOA), spoofing, dispread