【装备理论与装备技术】　　doi：10.11809/scbgxb2015.08.011

GPS 接收机的一种空时零陷抗欺骗式干扰方法

葛大江，周光彬，胥大川，毛　荣

（78088 部队，重庆　400039）

摘要：针对 GPS 导航系统的欺骗式干扰，比较了几种抗欺骗式干扰方法的优缺点，提出一种空时多天线零陷抗欺骗式干扰算法，利用“门限检测法”改进 OPDA 算法；通过对该算法的建模，研究了该算法的性能；系统仿真表明：该算法能有效的抑制欺骗式干扰，对工程实践具有一定的指导意义。

关键词：空时多天线零陷；GPS；接收机；抗欺骗式干扰

本文引用格式：葛大江，周光彬，胥大川，等. GPS 接收机的一种空时零陷抗欺骗式干扰方法[J]. 四川兵工学报，2015(8)：41－45.

Citation format：GE Da-jiang，ZHOU Guang-bin，XU Da-chuan，et al. GPS Receiver Anti-Deceptive Jamming Method Based on Space-Time Multi-Antenna Null[J]. Journal of Sichuan Ordnance，2015(8)：41－45.

中图分类号：P228.4；TN97　　**文献标识码**：A　　**文章编号**：1006－0707(2015)08－0041－06

GPS Receiver Anti-Deceptive Jamming Method Based on Space-Time Multi-Antenna Null

GE Da-jiang，ZHOU Guang-bin，XU Da-chuan，MAO Rong

（The No. 78088th Troop of PLA，Chongqing 400039，China）

Abstract：According to the deceptive jamming signals of GPS，the merits and demerits of several anti-deceptive jamming methods were compared and a new anti-deceptive jamming method based on space-time multi-antenna null was proposed. OPDA algorithm was improved by the threshold detection method. By modeling this algorithm，the anti-deceptive jamming system performance was studied. Simulation results show deceptive jamming can be suppressed by this algorithm，which has direct engineering practice value.

Key words：space-time multi-antenna null；GPS；receiver；anti-deceptive jamming

GPS 卫星导航信号相对于带内干扰（压制式干扰和欺骗式干扰）是十分脆弱的。欺骗式干扰是一种恶意干扰信号，它的目的就是使 GPS 卫星导航接收机产生错误的定位和导航结果[1]。欺骗式干扰比压制式干扰有更大的危害，因为被干扰接收机不能察觉这种干扰，随着技术的发展，现在欺骗式干扰设备已经用于实际中，它的成本也不高。

近些年来，抗欺骗式干扰的方法也正在研究，归纳起来，抗欺骗式干扰的方法主要分为两类，分别是欺骗式干扰信号发现方法和欺骗式干扰信号消弱方法。欺骗式干扰信号发现方法主要集中在区别欺骗式干扰信号和真实导航信号上，而欺骗式干扰消弱方法目的是抵消欺骗式干扰的威胁。现在大部分方法主要集中在欺骗式干扰发现的方法上而不是欺骗式干扰消弱上。目前，最热门的欺骗式干扰发现方法包括幅度区分法，时间到达区分法，极化区分法和密钥认证法[2－4]等。而欺骗式干扰消弱方法主要有残留信号检测法、多天线零陷法和接收机自主完好性监视法。下面对这 3 种欺骗式干扰信号消弱方法进行详细说明。

1　欺骗式干扰抑制方法

1.1　残留信号检测

在大部分情况下，欺骗式干扰源通常额外产生更高功率的相关峰，这是为了使被干扰目标 GPS 卫星接收机（简称目标接收机）接收和捕获错误的导航信号。然而，真实信号的

收稿日期：2015－01－15

作者简介：葛大江（1976—），男，工程师，主要从事军事装备建设与发展研究。

相关峰仍然存在于互模糊函数中。对于 GPS 卫星导航系统欺骗式干扰源来说抑制这个真实信号相关峰是非常困难的，因为它要求目标接收机天线相位中心位置相对于欺骗式干扰源天线相位中心位置的准确信息。在大多数情况下，信号成功发射后，真实信号的残留仍然保留，它能用于欺骗式干扰的发现和消弱。Humphreys 在 2008 年已经提出了一种针对 GPS 的残留信号发现技术。这种技术是使接收机上应用跟随软件技术。首先接收机将输入的前端数据复制到内存中。其次接收机选择一个已经被跟踪的 GPS 信号，在它附近确定一个伪随机码相位搜索范围，一般是在 ±10 chips 之间。然后在该范围内检测信号，如果测到信号超过门限就进行下一步，否则就测试另一个已经被跟踪的信号的残留信号。最后根据捕获到的欺骗式干扰，提取其参数，重构出干扰波形，用以消除数字通道中的欺骗式干扰。

残留信号检测技术增加了接收机的运算量，因为这项技术要求额外的跟踪通道用于跟踪真实信号和欺骗式干扰信号。此外，目前欺骗式干扰信号的功率高，使得真实信号的残留不可能很容易的被发现。

1.2 多天线波束形成和零陷

多天线接收机应用阵列技术是为了形成有用信号的波束。这种类型的接收机能向着欺骗式干扰源进行零陷，抑制欺骗式干扰的不利影响。如果接收信号乘一个复杂的权向量，那么欺骗式干扰就能被消弱。Daneshmand 提出了一种低复杂度和运算量的多天线欺骗式干扰信号消弱方法，它能用空域天线阵列滤除欺骗式干扰信号。为了形成一个空域相关矩阵，这种方法从不同天线接收的信号进行互相关，因此基于欺骗式干扰信号的功率优势，提取欺骗式干扰的空间特性。在真实信号和欺骗式干扰信号解扩前，以上这些操作都是在原始采样信号上进行的。如果欺骗式干扰源传输几个伪随机码信号，它们每个信号都有一个相对真实信号的功率水平，欺骗式干扰信号的导向矢量就能被提取因为所有的欺骗式干扰信号是从相同的空间区域发射出来的。这种方法不要求对天线阵列进行校准也不需要关于天线阵列朝向的先验信息。它们可以作为内置单独的天线组合模块在传统接收机的信号输入部分消弱欺骗式干扰信号。由于欺骗式干扰信号功率高于平均真实信号功率，这种抗欺骗式干扰信号的方法能成功的消弱欺骗式干扰信号。然而在一些情况下这种技术的应用可能不经意的降低了一些真实信号的功率。

1.3 接收机自主完好性监视

欺骗式干扰信号导致了在 GPS 卫星导航系统中的虚假测试。这些测试不可能是一致的，因此不可能得到一个合理的定位解算。接收机自主完好性监视是接收机利用多出来的观测量测试和判别导航卫星是否出现故障，同时检查出哪颗导航卫星出现了故障。Ledvina 对接收机自主完好性监视方法进行了扩展，这种方法能发现和排除外部测试，在这些外部测试中有欺骗式干扰信号的成分。接收机自主完好性监视能被用作抗欺骗式干扰信号的技术。然而这种方法只有在几个真实伪距测量中有一至两个欺骗式干扰信号的情况下才能有效。

通过以上分析可以看出多天线零陷法是一种比较好的抑制欺骗式干扰信号的方法。

2 多天线零陷抗欺骗式干扰方法

利用多天线零陷法进行抗欺骗式干扰是一种很有发展前景的新方法[5-7]。这种方法是依据欺骗式干扰源用一个天线发射多个伪随机码，而真实信号从不同卫星不同方向发射出来。根据这一事实，进行欺骗式干扰的发现和消弱。

2.1 多天线零陷方法的基本原理

欺骗式干扰消弱模块在接收机的信号输入端。首先设欺骗式干扰源是一个点干扰源，如图 1 所示，它能发射多种伪随机码，每一个功率都高于真实的伪随机码的功率。为了在干扰方向上产生零陷，该方法利用了欺骗式干扰信号和真实信号的不同特性。该方法有一个好处是它不用对天线阵进行调节或知道天线阵的形态和方向。为了进一步改善波束形成，本文要对空域多天线零陷方法进行扩展，实现空时多天线零陷方法。该方法不仅要对欺骗式干扰信号来向进行零陷，而且要对欺骗式干扰信号的多径反射信号进行抑制。用空时多天线零陷方法克服空域多天线零陷方法中不经意降低真实信号功率的缺点。

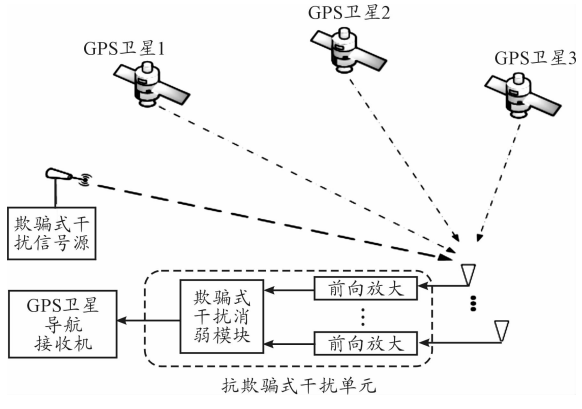

图 1 欺骗式干扰情况

设一均匀线状的天线阵，它有 N 个阵元。几个真实信号和一个欺骗式干扰信号和它的多径反射成分一起被天线阵所接收。为了简化问题，每个码片都被采样。设最大多径延迟为 L_{ch} 码片。在解扩以前信号的数学表达式如下

$$\underset{N\times 1}{r_i} = \sum_{m=0}^{M}\sum_{l=0}^{L_{\mathrm{ch}}} a_l^m s_{i-l}^m + \eta_i \tag{1}$$

式(1)中：s^m 指的是第 m 个信号采样；i 是接收直射信号的第 i 时刻；l 是相对于直射信号多径反射信号的时延；M 是真实卫星导航信号的数量；η_i 是高斯白噪声；a_l^m 是一个 $N\times 1$ 向量表示信号的信道参数。这些信号相比第 m 个信号采样的直射信号是延迟了 l 个码片。事实上，对于第 m 个信号，a_l^m 是和这些信号成分的导向矢量相关的。

设欺骗式干扰信号的几个伪随机码是从相同方向传来

的,所以对于抑制所有的欺骗式干扰的伪随机码来说,找到一个优化的增益向量是关键问题,它由 h 来表示,它必须满足式(2)。

$$\begin{aligned} &h^H a_l^0 = 0 \text{ if } (a_l^0)^H a_l^0 > \lambda_T \quad l = 0,1,\cdots,L_{\text{ch}} \\ &\|h\| = 1 \end{aligned} \tag{2}$$

λ_T 是一个门限,依据 MDL(Minimum Description Length)准则,它能根据信道参数相关值进行设置。这种限制避免了无解的这种情况。将 h 应用到接收机天线阵接收到的信号中,欺骗式干扰信号就能被抑制,输出的波束为

$$h^H r_i = \sum_{m=0}^{M}\sum_{l=0}^{L_{\text{ch}}} h^H a_l^m s_{i-l}^m + h^H \eta_i = \underbrace{\sum_{l=0}^{L_{\text{ch}}} h^H a_l^0 s_{i-l}^0}_{\approx 0} + \sum_{m=0}^{M}\sum_{l=0}^{L_{\text{ch}}} h^H a_l^m s_{i-l}^m + h^H \eta_i \tag{3}$$

2.2 空时多天线零陷方法

本文用一个空时处理的方法,用于估计直射欺骗式干扰源和它的多径反射成分的通道参数,这些参数是用来对欺骗式干扰信号和它的反射信号进行零陷。要做到这些,空时处理方法分为 3 步。首先,从空时数字信号中采集样本形成空时相关矩阵。其次,一种基于二阶统计的盲信号估计技术用于估计信道参数。它显示了通过分析空时相关矩阵欺骗式干扰信号的空间功率谱很容易就能从真实信号中将欺骗式干扰信号的信道参数分离出来。最后,先设置一个门限,通过门限值的比较发现潜在欺骗式干扰信号反射的信道参数。信道参数反应了各种信号的空间信息。因而有了这些参数,欺骗式干扰信号和它们的多路反射成分能通过零陷进行抑制。以上 3 步都是在信号解扩前进行的,这样可以降低处理时间。这种方法不要求进行天线阵校准。这些特征使得这个方法很适合实时的卫星导航信号的处理。下面详细介绍该方法。

2.2.1 空时相关矩阵的形成

在式(1)中,r_i 能表达为下面的形式

$$\underset{N\times 1}{r_i} = \sum_{l=0}^{L_{\text{ch}}} A_l s_{i-l} + \eta_i \tag{4}$$

在式(4)中

$$\underset{N\times(M+1)}{A_l} = [a_l^0 \quad a_l^1 \quad \cdots], \; l = 0,1,\cdots,L_{\text{ch}}$$

$$\underset{(M+1)\times 1}{s_i} = \begin{bmatrix} s_i^0 \\ s_i^1 \\ \vdots \\ s_i^M \end{bmatrix} \tag{5}$$

如果向量 r_i 是从 K_S 连续快拍中形成,那么

$$\vec{r_i} = \begin{bmatrix} r_i \\ r_{i-1} \\ \vdots \\ r_{i-(K_s-1)} \end{bmatrix}_{NK_s\times 1} \tag{6}$$

它能证实

$$\vec{r_i} = \alpha \vec{s_i} + \vec{\eta_i} \tag{7}$$

α 是一个 Toeplitz 矩阵,其定义为

$$\underset{NK_s\times(M+1)(L_{\text{ch}}+K_s)}{\alpha} = \begin{bmatrix} A_0 & A_1 & \cdots & A_{L_{\text{ch}}} & 0 & \cdots & \cdots & 0 \\ 0_{N\times(M+1)} & A_0 & A_1 & \cdots & A_{L_{\text{ch}}} & \ddots & \ddots & 0 \\ 0 & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & 0 & A_0 & \cdots & A_{L_{\text{ch}}-1} & A_{L_{\text{ch}}} & 0 \\ 0 & \cdots & \cdots & 0 & A_0 & \cdots & A_{L_{\text{ch}}-1} & A_{L_{\text{ch}}} \end{bmatrix} \tag{8}$$

$$\vec{s_i} = \begin{bmatrix} s_i \\ s_{i-1} \\ \vdots \\ s_{i-L_{\text{ch}}-K+1} \end{bmatrix}_{(M+1)(L_{\text{ch}}+K_s)\times 1} \qquad \vec{\eta_i} = \begin{bmatrix} \eta_i \\ \eta_{i-1} \\ \vdots \\ \eta_{i-L_{\text{ch}}-K_s+1} \end{bmatrix}_{NK_s\times 1} \tag{9}$$

设噪声和接收信号是相对独立的。因此空时相关矩阵能表示成下面的形式

$$\underset{NK_s\times NK_s}{R_{\vec{r}}} = E\{\vec{r_i}\vec{r_i}^H\} = \alpha E\{\vec{s_i}\vec{s_i}^H\}\alpha^H + \sigma^2 \underset{NK_s}{I} \tag{10}$$

在式(10)中 σ^2 是噪声的方差。式(10)中的 $R_{\vec{r}}$ 能用接收空时样本的连续快拍进行近似估计

$$R_{\vec{r}} \approx \frac{1}{K_s}\sum_{i=0}^{K_s-1} \vec{r_i}\vec{r_i}^H \tag{11}$$

2.2.2 欺骗式干扰信道参数估计

为了识别欺骗式干扰信号的信道参数和它的多径成分,比较好的技术是基于 SOS(二阶统计;second-order statistics)的盲信道估计。有很多基于 SOS 的方法,其中线性预测算法是十分特别的,因为它对信道阶数过估计不是很敏感。它是进行欺骗式干扰信号多径识别和消弱的最好方法之一,因为信道阶数常常是不知道的。Slock 在 1994 年首先提出线性预测算法。后来 Ding、Tong & Zhao、Tsatsanis & Xu 等人对这种算法进行了改进。本文中将外积分解算法应用于消弱欺骗式干扰信号和它的多径成分,并对该算法进行改进。

为了简单,余下的分析都是在欺骗式干扰信号和真实信号不相关的条件下进行的。因而,由于伪随机码的自相关和互相关特性,真实信号和欺骗式干扰信号之间的相关被忽略。外积分解算法的基本思想是构造信道参数矩阵 $[A_0 \quad A_1 \quad \cdots \quad A_{L_{\text{ch}}}]^H$ 的外积,利用该外积矩阵的奇异值分解来产生信号参数的估计。该算法是基于信道输出数据的二阶统计量来构造信道参数的外积。设信道阶数 L_{ch} 已知,定义一个大小为 $K_sN\times(L_{\text{ch}}+K_s)(M+1)$ 的矩阵

$$\underset{K_sN\times(L_{\text{ch}}+K_s)(M+1)}{A_h} \triangleq \begin{bmatrix} A_0 & A_1 & \cdots & A_{L_{\text{ch}}-1} & 0 & \cdots & 0 & \\ A_1 & A_2 & \cdots & A_{L_{\text{ch}}} & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & & & & & \\ A_{L_{\text{ch}}-1} & A_{L_{\text{ch}}} & & \ddots & & & \vdots & \\ A_{L_{\text{ch}}} & 0 & & & \ddots & & & \\ 0_{N\times(M+1)} & 0 & & & & \ddots & & \\ \vdots & \vdots & & \vdots & & & \ddots & \\ 0 & 0 & & & & & & 0 \end{bmatrix} \tag{12}$$

再定义一个转移矩阵 J

$$J = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \ddots & 1 \\ 0 & 0 & 0 & \cdots & 0 \end{bmatrix} \tag{13}$$

进而能得到自伴矩阵

$$\Delta = A_h A_h^H - J^N A_h A_h^H (J^N)^H = \begin{bmatrix} A_0 \\ A_1 \\ \vdots \\ A_{L_{\text{ch}}} \end{bmatrix} \begin{bmatrix} A_0^H & A_1^H & \cdots & A_{L_{\text{ch}}}^H \end{bmatrix} \tag{14}$$

J^N 是 J 的 N 次方。这样就构造了一个信号参数矩阵的外积矩阵,对它进行奇异值分解就可以得到信道参数的估计值。由此可以看出外积分解算法的关键是得到 $A_h A_h^H$,由他可算出信道参数的外积。因此,关键步骤是通过信道输出信号来估计外积 $A_h A_h^H$。通过推导,$A_h A_h^H$ 可由下式表示

$$A_h A_h^H = R_h (R_r - \sigma^2 I)^{\#} R_h^H \tag{15}$$

$(\cdot)^{\#}$指的是求伪逆。式(15)中 R_r是信道输出的自相关矩阵

$$R_r = \begin{bmatrix} R_0 & R_1 & \cdots & R_{K_s-1} \\ {\scriptstyle N\times N} & & & \\ R_1^H & R_0 & \cdots & R_{K_s-2} \\ \vdots & \ddots & \ddots & \vdots \\ R_{K_s-1}^H & R_{K_s-2}^H & \cdots & R_0 \end{bmatrix} \tag{16}$$

R_h 可以从 R_r得到

$$\underset{K_sN\times NK_s}{R_h} = \begin{bmatrix} R_0 - \sigma^2 I & R_1 & \cdots & R_{K_s-1} \\ R_1 & R_2 & \underset{N\times N}{0} & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ R_{K_s-1} & 0 & \cdots & 0 \end{bmatrix} \tag{17}$$

这样对外积矩阵的奇异值分解就能得到信道的估计值

$$SVD(A_h A_h^H - J^N A_h A_h^H (J^N)^H) = U \Sigma V^H \tag{18}$$

可以注意到Σ的第一个元素明显比其他对角线元素要高。这是由于在实际中所有的欺骗式干扰信号的伪随机码都是从相同的区域发射出来的而真实信号的伪随机码是从不同卫星上发射出来的。Σ的对角线元素都是每个信号和它反射成分的功率总和。因而对应欺骗式干扰信号和他反射的第一个对角线元素是高于其他元素的。因而,接收机在受到欺骗式干扰攻击的时候,$U\Sigma V^H$ 能近似表示为

$$U \Sigma V^H \simeq \begin{bmatrix} a_0^0 \\ a_1^0 \\ \vdots \\ a_{L_{\text{ch}}}^0 \\ \underset{N\times 1}{0} \\ \vdots \\ 0 \end{bmatrix} \sigma_{\text{sp}}^2 \begin{bmatrix} a_0^0 \\ a_1^0 \\ \vdots \\ a_{L_{\text{ch}}}^0 \\ \underset{N\times 1}{0} \\ \vdots \\ 0 \end{bmatrix}^H \tag{19}$$

式(19)中 σ_{sp}^2是欺骗式干扰信号的功率。因此,$a_l^0, l = 0, 1, \cdots, L_{\text{ch}}$能通过矩阵中最大的列向量来估计得到。

线性预测类算法的优点是对信道阶数有很好的估计。而人们更关心的是信道阶数过估计的情况下信号均衡的结果。在信道阶数未知的情况下,虽然外积分解算法与子空间算法相比较能更好的估计出信道参数,但这种均衡的效果并不是十分好。当被过估计的阶数较大时"信号均衡"的效果对"信噪比"的要求就比较高,这在实际中是很难实现的。因此,找到一种尽可能少的依赖"信道阶数过估计"的"信号均衡"算法变得十分的重要。

当阶数被过估计为 $L'_{\text{ch}}(L'_{\text{ch}} > L_{\text{ch}})$时,信道参数矩阵为

$$\bar{A} = \begin{bmatrix} A_0 & A_1 & \cdots & A_{L_{\text{ch}}} & \underbrace{0 \quad \cdots \quad 0}_{L'_{\text{ch}}-L_{\text{ch}}-1} \end{bmatrix}^H \tag{20}$$

而在实际中由于一些干扰因素使得信道参数矩阵的尾部并不都为零,而是会出现一些小的波动。过估计的阶数增大,只是尾部的小波动变长,而信道的其他部分不会发生变化。在实际中由于接收机采用了脉冲成形滤波器以及常数媒质的色散效应,有效的信道阶数一般只选取包含信道冲激相应大部分能量的采样。根据这种情况,本文对外积分解算法进行改进,提出一种"门限检测法"。因为过估计信道的能量主要集中在前部,所以可以设一个门限值,从尾部进行搜索,当遇到大于门限的采样点时停止搜索,只保留该点之前的数值,从而形成新的信道冲激响应,并用此信道进行均衡。但要注意的是:

1)在进行截尾时,如果某一时刻内有一个采样点被舍弃,则其余 $L_{\text{ch}} - 1$ 个点丢弃,以保证采样时刻的同步。

2)由于构造出的新的冲激响应只需要包含信道的大部分能量就可以了,因此新的冲激响应的阶数可以在真实的信道阶数左右浮动。

3)选取门限如果过大,则会造成信道尾部扰动,如果门限选取过小就会造成丢掉部分信号响应。通过实验统计,该门限值可选取信号归一化能量的 84% ~88% 之间[8]。

2.2.3 零陷控制

在估计 $a_l^0, l = 0, 1, \cdots, L_{\text{ch}}$后,通过每一个 a_l^0 的绝对值和 λ_T 这个门限进行比较,延迟和它们对应的信道参数能够被发现。从估计信道参数的相对值中能发现这个门限值 λ_T。如果$(a_l^0)^H a_l^0 > \lambda_T \quad l = 0, 1, \cdots, L_{\text{ch}}$,则在实际中 a_l^0 被认为是一个信号导向矢量或是几个相同时延的接收信号导向矢量。如果潜在延迟 M_{sp}被发现,那么信道参数就构成 $N \times M_{\text{sp}}$矩阵,这个矩阵被定义为 B。欺骗式干扰信号的正交投影矩阵是 $P_\perp$,它由下式获得

$$P_\perp = I - B(B^H B)^{-1} B^H \tag{21}$$

因此,如果这个正交投影矩阵应用到接收信号向量中,欺骗式干扰信号和它的反射信号将从接收机天线阵接收的信号中消弱。数学表达式如下

$$\bar{r_i} = P_\perp^H r_i = \sum_{m=0}^{M} \sum_{l=0}^{L_{\text{ch}}} P_\perp^H a_l^m s_{i-l}^m + P_\perp^H \eta_i = \sum_{l=0}^{L_{\text{ch}}} P_\perp^H a_l^0 s_{i-l}^0 + \sum_{m=0}^{M} \sum_{l=0}^{L_{\text{ch}}} P_\perp^H a_l^m s_{i-l}^m + P_\perp^H \eta_i \tag{22}$$

欺骗式干扰信号被消弱。式中第一部分为零可以忽略。因而最优权向量是 $P_{\perp}\beta$,β 是任意单位向量。

现在对这项欺骗式干扰消弱方法进行如下总结:构建空时相关矩阵;通过原始 OPDA 算法对信道冲激响应 A 进行估算(信道阶数 L_{ch} 可被任意阶过估计);用"门限检测法",调整信道冲激响应;计算 Δ;进行 Δ 的奇异值分解得到最大列向量,这是为了估计欺骗式干扰信号的信道参数;将估计出来的欺骗式干扰信号信道参数和门限值比较,构建矩阵 B;计算正交投影 $P_{\perp}$,把它应用到接收信号向量中。

3 仿真实验

将真实信号和欺骗式干扰信号的伪随机码取为相同,但码延和多普勒频移随机产生。真实信号的平均功率为 -140 dBW。所有的欺骗式干扰信号都从同一方向发射。每个欺骗式干扰信号功率为 -122 dBW。采样频率为 10 MHz。天线阵为均匀线阵,阵间距为 GPSC/A 信号波长的一半。所有仿真的时间都是 1 ms。K_s 选为 10 码片。

为了显示该方法的改进效果,在不同的欺骗式干扰信号功率情况下,进行了 100 次蒙特卡洛实验。图 2 显示了用该欺骗式干扰信号消弱方法时真实信号、欺骗式干扰信号和欺骗式干扰信号多径成分的平均信噪比。信噪比是由接收的真实信号和欺骗式干扰信号的功率与噪声基底估计器输出的功率比得出的,噪声基底是与 1 ms 内接收信号的虚假伪随机码有关。在每次实验时多径延迟在 0 ~ 5 个码片间自由选择。欺骗式干扰信号要比它的多径成分在功率上高出 3 个 dB。真实信号和欺骗式干扰信号伪随机码的传输距离、码延和多普勒平移都是随机改变的。

一个典型的信噪比发现门限在图 2 中也有表示。它是在真实信号接收过程中为了发现虚警率而设置的。就单天线接收机来说,当欺骗式干扰信号的功率加强时,真实信号的信噪比在降低。这是由于更高的欺骗式干扰信号功率使接收机噪声基底增加而导致的。同时,当欺骗式干扰信号的功率增加时欺骗式干扰信号的伪随机码功率也增加。这样 GPS 卫星导航接收机将错误的接收欺骗式干扰信号的相关峰。当用了本文的方法后,可以看出当欺骗式干扰信号功率增加时,真实信号的平均信噪比保持不变而欺骗式干扰信号的信噪比一直在门限下。因此本文介绍的方法不仅消弱了欺骗式干扰的相关峰而且降低了欺骗式干扰信号的影响。从图 2 中可以看出,在功率增大后,真实信号的平均信噪比远高于其他信号的信噪比。

图 3 显示了在使用抗欺骗式干扰信号方法前后真实信号和欺骗式干扰信号中的第 1 号卫星伪随机码的互模糊函数。欺骗式干扰信号的功率要高出真实信号的功率大约 3 dB。图 3(a)显示的是在使用抗欺骗式干扰信号方法前,真实信号相关峰要比欺骗式干扰信号的相关峰弱。图 3(b)显示的是在使用抗欺骗式干扰信号方法后,欺骗式干扰信号的相关峰被抑制,而真实信号的相关峰被加强了。

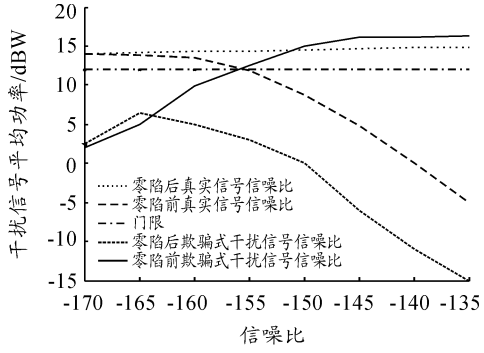

图 2 用抗欺骗式干扰方法前后真实信号和欺骗式干扰信号信噪比情况

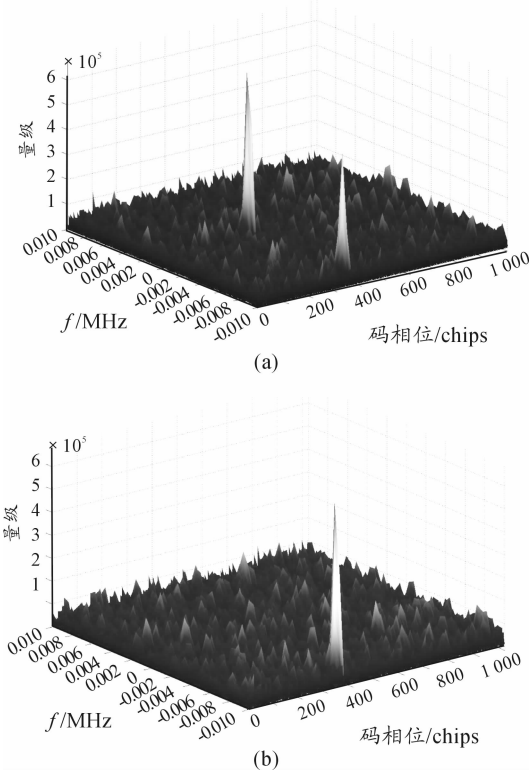

图 3 抗欺骗式干扰方法使用前后信号相关峰捕获情况

4 结束语

本文论述了抗欺骗式干扰的研究现状,分析了欺骗式干扰与真实信号间的差别。依据这种差别,提出基于空时多天线的零陷法来发现与抑制欺骗式干扰信号。通过仿真实验验证了该方法的可行性。

(下转第 50 页)

经过2.5 ms后,混凝土靶在聚能射流作用下形成一个漏斗状的孔洞。4点起爆时,射流穿靶深度约为980 mm;8点起爆时,射流穿靶深度约为1 060 mm;16点起爆时,射流穿靶深度约为1 100 mm;32点起爆时,射流穿靶深度约为1 150 mm,射流穿靶深度随着起爆点的增加而加深。

仿真计算结果表明:聚能药经环形起爆后形成喇叭状爆轰波,爆炸点越多,波阵面应力越大,爆轰波输出能量越强,32点起爆波阵面中心最大压力约为单点起爆的2.2倍,爆轰波对药型罩的压垮方向向中心线会聚,提高了罩壁微元的压垮速度,形成速度更快、能量更高的射流;在2.5 ms时间内,射流穿靶深度随着起爆点的增加而加深,32点起爆后射流穿混凝土靶板深度为单点起爆的1.69倍,对目标毁伤效果较单点起爆更好,最终提高了聚能装药的侵彻威力。

4 结论

本文提出了聚能战斗部柔性分流索环形起爆方法,是将引信传爆药柱改为多条柔性分流索环起爆装置,各分流索将爆轰能量同步传递到爆轰输出端子,爆轰输出端子在聚能装药末端面起爆后形成起爆炸环并引爆聚能药,爆轰波形成超高压力的喇叭波阵面压垮药型罩会形成速度更快、能量更大地射流。仿真结果表明:分流索环起爆装置的隔爆座体能可靠地隔离导爆药、扩爆药柱的爆轰能量,可以作为隔爆元件;聚能装药多点均布起爆能够提高射流的侵彻能力。不足之处,仿真分析是在简化模型、理想工况的基础上得到的,结果有一定的误差。

参考文献:

[1] 周义,王永良,王自焰.地下堡垒可行—美国钻地弹的应用与发展[J].飞航导弹,2005(4):41-45.

[2] 徐蓬朝,黄惠东,张龙山,等.垫片提高抗冲击能力的应力波衰减机理[J].探测与控制学报,2012,34(2):1-6.

[3] 徐蓬朝,黄惠东,聂峥.前级爆轰过载信息作为后级计时起爆起点[C]//2012年212所学术交流论文集,2012:70-74.

[4] 张龙山.引信技术概论[Z].西安:西安机电信息技术研究所,2004.

[5] 方向,张卫平,高振儒,等.武器弹药系统工程与设计[M].北京:国防工业出版社,2012.

[6] 赵白露,高炜.模糊本体中的模糊相似度计算[J].重庆工商大学学报:自然科学版,2014,31(9):60-62.

[7] Schwalbe L A,Wingate C A,Stofleth J H,et al. Experiment and computation studies of rod—deployment mechanisms [C]//16th International Symposium on Ballistcs. September,1996:347.

[8] 何涛,杨竞,金鑫,等.ANSYS10.0/LS-DYNA非线性有限元分析实例指导教程[M].北京:机械工业出版社,2007.

[9] 聂峥,徐蓬朝,周平,等.有限元方法在串联引信结构强度计算中的应用[J].探测与控制学报.2012,34(3):42-46.

(责任编辑 周江川)

(上接第45页)

参考文献:

[1] 卜长江,罗跃生.矩阵论[M].哈尔滨:哈尔滨工程大学出版社,2003.

[2] Humphreys T E,Ledvina B M,Psiaki M L. Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer[J]. ION GNSS 21st International Technical Meeting of the Satellite Division,2008,2314-2325.

[3] Ledvina B M,Bencze W J,Galusha B. An In-Line Anti-Spoofing Device for Legacy Civil GPS Receivers[J]. Institute of Navigation ITM,2010,698-712.

[4] Montgomery P Y,Humphreys T E,Ledvina B M. Receiver-Autonomous Spoofing Detection: Experimental Results of a Multi-antenna Receiver Defense against a Portable Civil GPS Spoofer[J]. ION 2009 International Technical Meeting,2009:124-130.

[5] Wen H,Huang P Y,Dyer J. Countermeasures for GPS Signal Spoofing[J]. ION GNSS 18th International Technical Meeting of the Satellite Division,2005:1285-1290.

[6] Daneshmand,Jafarnia S A,Broumandan A. A Low Complexity GNSS Spoofing Mitigation Technique Using a Double Antenna Array[J]. GPS World magazine,2011,22(12):44-46.

[7] Nielsen J,Broumandan A,Lachapelle G. Spoofing Detection and Mitigation with a Moving Handheld Receiver[J]. GPS World magazine,2010,21(9):27-32.

[8] 刘媛涛,葛临东,王彬.一种改进的外积分解(OPDA)算法[J].系统仿真学报,2007,19(20):4835-4839.

(责任编辑 周江川)