文章编号:1671-4598(2016)04-0029-04 DOI:10.16526/j.cnki.11—4762/tp.2016.04.009 中图分类号:TN961 文献标识码:A

基于信噪比测量的欺骗干扰检测方法

曹可劲,彭煊坤,李 豹,朱银兵,李松林
(海军工程大学 导航工程系,武汉 430033)

摘要:在捕获北斗信号的过程中,接收机根据预先设定好的信号搜捕策略和门限值来捕获信号;欺骗干扰源通过产生虚假的相关峰和增加噪声基底,可以有效地干扰普通型北斗接收机正常的捕获工作;针对欺骗信号检测问题,在分析欺骗信号入侵对接收机噪声基底影响的基础上,提出了在捕获阶段利用信噪比(SNR)检测技术识别欺骗干扰信号的方法,并对其有效性进行了分析;仿真结果表明,采用该方法的接收机具有一定程度的欺骗干扰识别能力,为提高GNSS接收机抗干扰能力提供了有益的参考 。

关键词:北斗信号;噪声基底分析;欺骗信号相关峰;信噪比

A Method of Spoofing Jamming Detection Based on SNR Measurement

Cao Kejin, Peng Xuankun, Li Bao, Zhu Yinbing, Li Songlin
(Department of Navigation, Naval University of Engineering, Wuhan 430033, China)

Abstract: The receiver acquires the BD signals according to pre-defined policies and threshold in the acquiring process. Spoofing Jamming sources can effectively interfere with ordinary BD receivers by generating a false correlation peak and increasing noise floor. In order to detect the spoofing signal, based on the analysis of the influence that the intrusion of spoofing signals can increase noise floor of the receiver, a SNR detection method is proposed to identify spoofing signals during the acquiring process and its effectiveness is analyzed. The receiver adopting this approach has a certain degree of detecting and discriminating spoofing sources, providing a useful reference to improving anti-jamming capability of GNSS receivers.

Keywords: BD signals; noise power analysis; spoofing signal correlation peak ; SNR

0 引言

北斗卫星信号由于到达地面已及其微弱,很容易受到窄带干扰。欺骗式干扰是针对卫星系统的人为蓄意干扰,再加上目标接收机并不清楚此类威胁,因而相对于其他类型干扰更具有威胁性。由于民用北斗系统体系结构是公开的,对普通型接收机实施欺骗干扰并不是很困难,欺骗干扰和反干扰是GNSS系统面临的又一大挑战。

在捕获卫星信号过程中,接收机通过预先设定好的信号搜捕策略直接调节载波数控振荡器和C/A码数控振荡器,使它们复制出相应于某一搜索单元的载波和为伪码。假设接收机通过搜索所有的载波频率和码相位单元,得到的某一相关峰值超过检测阈值,便可认为捕获到卫星信号,进而可粗略估计出相应的载波频率和码相位。欺骗干扰可以从两个方面影响接收机捕获信号的过程。一方面欺骗干扰源会产生一组不相关的噪声,进而影响了接收机的噪声基底;另一方面欺骗干扰源可以产生一个或多个幅值超过真实信号相关峰值的虚假相关峰,使接收机捕获跟踪后得到错误的导航信息。

目前文献[1-5]展开了欺骗干扰检测方面的研究,文献[1]从幅值角度提出了欺骗干扰源识别技术,文献[2]从多种途径探讨了针对欺骗干扰检测的方法,但是这些文献都缺乏对欺骗干扰检测的具体方法的分析与研究,本文着重分析了欺骗干扰信号对接收机信号噪声水平的影响,通过讨论发现,欺骗干扰分布可以用一种圆对称高斯分布加上环境附加的高斯白噪声分布来近似。在此基础上又分析了干扰状态下接收机信号的捕获过程,通过研究发现,欺骗干扰会降低真实信号的载噪比,并有可能使其小于信号检测门限,进而导致捕获性能的恶化。此外,欺骗信号功率增强会使接收机信号载噪比增加,进而使接收机捕获到欺骗信号相关峰。

在此基础上,提出了利用信噪比(SNR)检测欺骗干扰信号的方法。

1 系统模型与实验场景

这里假定欺骗信号由欺骗干扰源发射,并且由图1中接收机天线所接收。为便于分析,在这里同样可以认为欺骗信号与真实结构相同,但欺骗信号与真实信号功率、码相位、多普勒频率往往不相同。在捕获过程中,接收机目的是要检测到存在的真实信号,并对其码相位和载波多普勒频率做出粗略的估计。

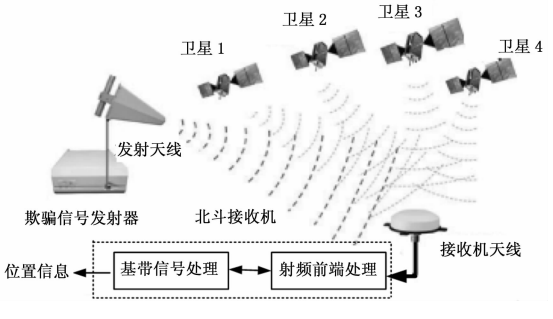

图1 欺骗干扰场景

接收机基带信号处理过程由复杂的相关器组成,结构如图

收稿日期:2015-09-14; **修回日期**:2015-10-23。
基金项目:海军工程大学自然科学基金(HGDQNJJ15021)。
作者简介:曹可劲(1978-),男,湖南娄底人,博士,副教授,主要从事卫星无线电导航技术研究。

2 所示，整个过程包括载波多普勒玻剥离、信号伪码解扩、低通滤波。

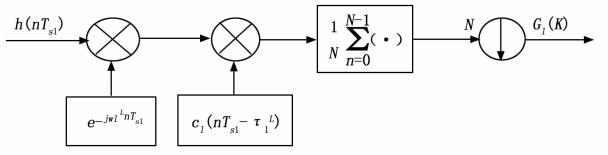

图 2 北斗接收机基带信号相关器结构

在图 2 中，c_l 代表第 l 路本地伪码序列，w_l 和 τ_l 分别代表本地码的载波多普勒和码相位时延，T_{s1} 代表采样间隔。捕获过程中，接收机通过不同载波多普勒频率所调制的伪码信号与接收到的真实信号做相关运算，其运算结果再进行 N 个环节的积分。当本地产生信号多普勒和码相位与接收信号相一致时，积分器输出值便会产生一个相关峰值。在这里我们假设本地载波信号相位和真实信号并不同步，但多普额频率和码相位时延和真实信号参数保持一致，积分时间远小于数据位长. 即可在分析中忽略数据位的影响，整个积分过程输出值可表示为：

$$G_l[f_l,\tau_l,k]=\sqrt{P_l}\exp(j\varphi_l)+\sum_{\substack{m=1\\m\neq l}}^{N_A}\sqrt{P_m}R_{ml}[w_l,\tau_l,K]+\sum_{\substack{m=1\\m\neq l}}^{N_S}\sqrt{P_k}R_{kl}[w_l,\tau_l,K]+\eta(k) \tag{1}$$

这里

$$R_{ml}[w_l,\tau_l,K]=\frac{1}{N}\sum_{n=(k-1)N+1}^{kN}c_m(n-\tau_{mlk})c_l(n)e^{(j\Delta w_{mlk}(n)+j\Delta\varphi_{mlk})} \tag{2}$$

其中：P_m、c_m 分别表示接收的第 m 颗卫星信号的功率和伪码，τ_{mlk}、Δw_{mlk}、$\Delta\varphi_{mlk}$ 分别表示在第 k 个积分环节，接收到的第 m 颗卫星伪码和本地产生的第 l 颗卫星伪码两者之间的码相位时延差值、载波多普勒差值、载波相位差值。

$G_l[f_l,\tau_l,k]$ 表示第 k 个时间间隔对应的积分器输出，公式（1）由四部分组成。第一项表示在捕获过程中目标信号相关积分值；第二项表示由其它伪码信号引起的干扰；第三项表示由欺骗信号伪码引起的干扰；第四项表示方差为 σ^2/N 的圆对称高斯分布，其中 σ^2 表示加性高斯白噪声的方差。

2 欺骗信号对接收机噪声基底影响分析

在接收机捕获过程中，对卫星信号的多普勒频率和码相位进行二维搜索，每一次搜索将得到一个相关值，在这里用 $G_l[f_l,\tau_l,k]$ 表示。然而在这些值中只有一个是在存在卫星信号的单元上获得的，其它都是在信号不存在的单元上所得到，进一步可理解为这些相关值基本上来源于噪声。

一般情况下，BD 接收机天线接收到的欺骗信号比真实信号功率更强，由欺骗信号产生的干扰会抬高接收机信号处理过程中的噪声基底。通过产生一个并不存在于 BD 星座中虚拟的 PRN 与接收到的信号进行相关运算，可以估算出接收机噪声基底的大小。

若 $G_f[f_f,\tau_f,k]$ 表示在时间间隔 k 的复杂相关器输出，那么噪声基底可以认为是 $G_f[f_f,\tau_f,k]$ 的方差，于是有：

$$\delta^2_{Z_f[k]}=var\left[\sum_{m\in J^a}\sqrt{P_m{}^a}R_{mf}{}^a[w_f,\tau_f,K]+\sum_{n\in J^s}\sqrt{P_n{}^s}R_{nl}{}^s[w_f,\tau_f,K]+\eta[k]\right] \tag{3}$$

在这里假设第 f 个 PRN 信号为一个虚拟的伪码，既不存在于真实信号伪码序列，也不存在于欺骗信号伪码序列。因此，相关器输出由三部分组成，由真实信号伪码 PRN 引起的干扰项，欺骗信号伪码 PRN 引起的干扰和高斯信道噪声。

若假设真实信号和欺骗信号 PRN 的多普勒频移与码延迟是相互独立并且是随机分布的，公式可以进一步表示为：

$$\delta^2_{Z_f[k]}=\sum_{m\in J^a}\sqrt{P_m{}^a}var[R_{mf}{}^a[w_f,\tau_f,K]]+\sum_{n\in J^s}\sqrt{P_n^s}var[R^s_{nl}[w_f,\tau_f,K]]+var[\eta[k]] \tag{4}$$

上述公式中的第一项和第二项都包含了 $R_{mf}[w_f,\tau_f,K]\sim[0]$ 的方差，实际上是指由两路信号中随机多普勒频移和相位差分别调制的第 m 个 PRN 和第 f 个 PRN 之间的互相关值。$R_{mf}[w_f,\tau_f,K]$ 的分布可以用数学公式推导出来，在任一 I 支路和 Q 支路均可以近似用一个均值为为零的高斯分布表示出来。对正常功率水平的扩频码序列仿真结果表明，不管是同相还是正交支路，互相关函数值的方差值 $\delta^2_{I,R_{mf}}=\delta^2_{Q,R_{mf}}=0.00033$。进一步分析仿真结果可以得出，$I$ 支路和 Q 支路的协方差可以忽略不计，于是有：

$$R_{mf}[w_f,\tau_f,K]:N_h\left(\begin{bmatrix}0\\0\end{bmatrix},\begin{bmatrix}\delta^2_{I,R_{mf}}&0\\0&\delta^2_{I,Q_{mf}}\end{bmatrix}\right) \tag{5}$$

在这里 $N_h(a,b)$ 表示均值为 a、协方差为 b 的圆对称高斯分布，于是相关输出 $G_f[f_f,\tau_f,k]$ 就是圆对称高斯分布随机变量的和值，这样一来 $G_f[f_f,\tau_f,k]$ 又变成更复杂的高斯变量，并服从以下分布：

$$G_l[f_l,\tau_l,k]:N_c\left(\begin{bmatrix}0\\0\end{bmatrix},\frac{N_0}{2NT_s}\begin{bmatrix}1&0\\0&1\end{bmatrix}+\left(\sum_{m=1}^{N_{Auth}}P_m{}^a+\sum_{j=1}^{N_{Spoof}}P_j{}^s\right)\begin{bmatrix}\delta^2_{I,R_{mf}}&0\\0&\delta^2_{I,Q_{mf}}\end{bmatrix}\right) \tag{6}$$

上述公式表明干扰项的方差直接受真实信号和欺骗信号伪码传输功率的影响，北斗系统设计时规定了真实伪码的干扰功率程度不能超过环境噪声基底。因此欺骗信号的功率可以比真实北斗信号更大，欺骗信号的相应的干扰功率水平可以超过周围高斯噪声基底，于是就降低了传统单用户接收机真实信号的信噪比。为进一步分析欺骗信号对噪声基底方差的影响，考虑到欺骗信号总功率可以定义如下：

$$TP_{dB}=10\log_{10}\left(\sum_{n=1}^{N_{Spoof}}P_n{}^s\right) \tag{7}$$

在图 3 中，分析了当积分时间 T_e 为 1 ms 时噪声基底的变化情况。由图中结果可知，当欺骗信号总功率较低时，环境高斯白噪声是决定接收机噪声基底的主要因素。随着欺骗信号总功率的增加，噪声基底会超过接收到的真实卫星信号的功率。

3 在欺骗攻击时 BD 系统捕获的脆弱性分析

接收机捕获过程中主要是检测真实信号的相关峰值，并对多普勒频率和码延迟进行估计。但是有欺骗信号引起的干扰同

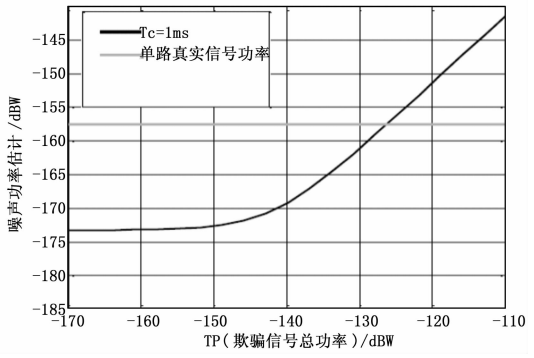

图 3　噪声功率（$2\sigma^2$）随欺骗信号总功率变化分析

时会增加接收机的噪声基底。

通过前面章节讨论可知，相关器输出可以写成 M_0（信号不存在时），M_1（真实信号存在时）和 M_2（欺骗信号存在时）3 种形式的分布。

$$M_{l,0}: y(f_l,\tau_l,k] = N_c(0,\delta^2 I_2) \tag{8}$$

$$M_{l,1}: y(f_l,\tau_l,k] = N_c(\mu^1,\delta_1^2 I_2) \tag{9}$$

$$M_{l,2}: y(f_l,\tau_l,k] = N_c(\mu^2,\delta_2^2 I_2) \tag{10}$$

其中：

$$u^{1|2} = \sqrt{P_L{}^{1|2}}\exp(j\phi_L) \tag{11}$$

$$\delta^2 = \frac{N_0}{2NT_s} + \delta_{I,R_{mf}}^2\left(\sum_{m=1}^{N_{Auth}} P_m{}^{\alpha} + \sum_{j=1}^{N_{Spoof}} P_j{}^{s}\right) \tag{12}$$

$$\delta_1{}^2 = \frac{N_0}{2NT_s} + \delta_{I,R_{mf}}^2\left(\sum_{\substack{m=1\\m\neq 1}}^{N_{Auth}} P_i{}^{\alpha} + \sum_{\substack{j=1\\j\neq 1}}^{N_{Spoof}} P_j{}^{s}\right) \tag{13}$$

$$\delta_2{}^2 = \frac{N_0}{2NT_s} + \delta_{I,R_{mf}}^2\left(\sum_{\substack{m=1\\m\neq 1}}^{N_{Auth}} P_j{}^{\alpha} + \sum_{j=1}^{N_{Spoof}} P_j{}^{s}\right) \tag{14}$$

由前面讨论可知，真实信号的干扰远远小于高斯白噪声干扰程度。因此，可以认为 $\delta^2 = \delta_1{}^2$。同时，若欺骗信号足够多（比如超过 10 路），可以认为单独的一路信号并不改变噪声基底大小。综上所述，以上 3 个方差项实际上非常接近，可以认为 $\delta^2 = \delta_1{}^2 = \delta_2{}^2$。

接收机捕获信号的过程可以看做一个广义最大似然比检测问题（Generalized Likelihood Ratio Test，GLRT），不妨假设一路伪码信号存在，于是有：

$$L_G(y_l) = \frac{P_{y_l|\theta_{l,1}}(y_l \mid \theta_{l,1}^{\Delta};M_{l,1})}{P_{y_l;M_{l,0}}(y_l;M_{l,0})} > \gamma_{th} \tag{15}$$

其中：y_l 代表第 l 路 PRN 信号相关器的输出，$M_{l,0}$ 代表 PRN 信号不存在时的假设条件，$M_{l,1}$ 代表 PRN 信号存在时的假设条件，$\theta_{l,1}^{\Delta}$（$f_l{}^{\Delta}$，$\tau_l{}^{\Delta}$，$\alpha_l{}^{\Delta}$）表示对第 l 路 PRN 信号多普勒频移、码延迟和接收的信噪比等相关参数变量的最大似然估计，γ_{th} 代表 $M_{l,1}$ 情况下的检测阈值，$P_{y_l|\theta_{l,1};M_{l,1}}$ 和 $P_{y_l;M_{l,0}}$ 表示在和 $M_{l,1}$ 假设条件下，各自对应的相关器输出是一种复杂的高斯分布。由于在实际应用中，对于大多数接收机而言，经常提取相关器输出值的平方（$M_{l,0}D = u_l u_l^* = |y_l[f_l,\tau_l,k]|^2$）作为检测量，因此和 $P_{D_l;M_{l,0}}$ 可进一步表示成两个自由度的中心和非中心卡方分布。

$$P_{D_l|\theta_{l,1};M_{l,1}|2} = \frac{1}{2\sigma_{1|2}^2}e^{-\frac{D_l+P_l}{2\sigma_{1|2}^2}}I_0\left(\frac{\sqrt{D_l P_l}}{\sigma_{1|2}^2}\right) \quad (D_l > 0) \tag{16}$$

其中：$I_0(x)$ 为第一类修正零阶贝塞尔函数，$M_{l,1|2}$ 代指真实信号或者欺骗信号对应的假设条件。若定义检测门限阈值定义为 D_Y，相应的单次检测概率和单次虚警率可以定义如下：

$$P_{D_l-\text{单次}} = \int_{D_Y}^{+\infty} = \int_{D_Y}^{+\infty}\frac{1}{2\sigma^2}e^{-\frac{D_l+P_l}{2\sigma_1^2}}I_0\left(\frac{\sqrt{D_l P_l}}{\sigma^2}\right)\mathrm{d}D_l = \exp\left(-\frac{D_Y}{2\sigma^2}\right) \tag{17}$$

$$P_{FA-\text{单次}} = \int_{D_Y}^{+\infty} P_{D_l;M_{l,0}}\,\mathrm{d}D_l = \int_{D_Y}^{+\infty}\frac{1}{2\delta^2}\exp\left(\frac{-D_l}{2\delta^2}\right)\mathrm{d}D_l \tag{18}$$

最大似然比（GLRT）检测过程表明，接收机通过搜索所有相应可能码时延和多普勒范围来判断相关器输出值，然后选中最大平方幅值的单元。如果幅度超出阈值，就认为卫星信号已经检测到，进而对检测到的卫星信号参数进行大致分析，相应单元的多普勒频率和码相位就可以得出。因此，对于正确的检测过程来讲，应该只有一个相关峰值在检测阈值之上。

显然如果给定一个虚警率，便可有单次虚警率计算出系统虚警率，不妨设 N_c 为搜索单元总数目，相应的检测阈值计算过程如下：

$$P_{FA-\text{系统}} = 1-(1-P_{FA-\text{单次}})^{N_c} \tag{19}$$

因此有：

$$P_{FA-\text{单次}} = 1-(1-P_{FA-\text{系统}})^{\frac{1}{N_c}} \tag{20}$$

结合上述公式于是有：

$$D_Y = -2\sigma^2\ln(1-(1-P_{FA})^{\frac{1}{N_c}}) \tag{21}$$

这里 N_c 代表搜索单元的数目。显然，第 i 路 PRN 信号的信噪比可以用以下信号表示出来：

$$\alpha_i = \frac{P^{1|2}}{2\delta_{1|2}{}^2} \tag{22}$$

相应的信噪比检测阈值就可以定义如下：

$$\alpha_Y = \frac{D_Y}{2\delta^2} = \ln(1-(1-P_{FA})^{\frac{1}{N_c}}) \tag{23}$$

由该公式可知，给定一个可能的虚警率，接收机就能够检测出信噪比超过检测阈值 α_Y 的卫星信号。

图 4 显示了在 matlab 仿真环境下真实信号和欺骗信号相对于信号总功率的变化，图中分别有 10 路等功率真实信号和 10、20、30 路等功率欺骗信号。其中每一路真实 PRN 信号功率约为 −158 dBW，积分时间 T_c = 1 ms，经典虚警率 $P_{FA} = 10^{-3}$，于是可计算出此时的信噪比检测阈值。由图可知，随着欺骗信号总功率增加，真实信号的信噪比降低，欺骗信号的信噪比却增加到一定程度后缓慢变化。显然欺骗信号的信噪比与欺骗信号的支路数量和欺骗信号的总功率有关。图中右侧纵轴表示 1 ms 积分时间内接收机噪声基底的变化。

由图 4 可知，在欺骗信号功率一定的情况下，随着欺骗信号支路数的增加，每一路欺骗信号所获得的功率就变小，相应的信号 SNR 就降低。

接收机捕获的伪码信号并不在欺骗信号伪码和真实信号伪码之间。欺骗信号入侵导致真实信号载噪比降低，最终使其降至接收机检测阈值之下。此时欺骗信号对于接收机而言仅仅相当于一种宽带干扰，使接收机捕获检测性能恶化。

当捕获信号伪码位于真实信号伪码和欺骗信号伪码之间时，分析如图 5 所示，图中有 10 路真实信号和 10 路欺骗信号，按照实验载噪比和绝对功率变化过程，可以将欺骗信号干扰影响过程划分为 3 个阶段：

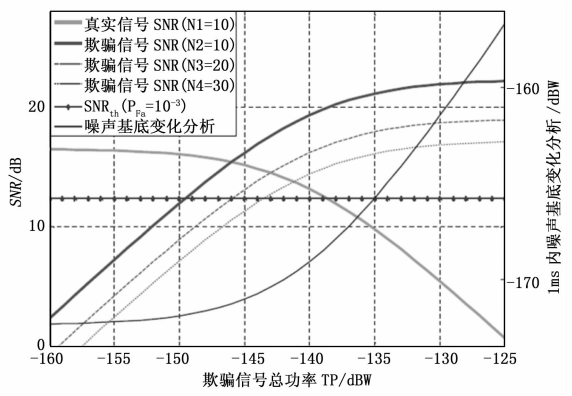

图 4 真实信号和欺骗信号信 SNR 变化

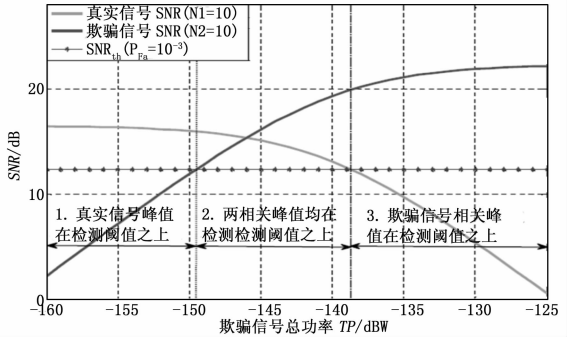

图 5 存在欺骗干扰时信号相关峰值的捕获

1）总功率小于－150 dBW 时属于第一类区域：欺骗信号的信噪比在检测阈值之下，此时接收机仍然能够捕获到真实信号，欺骗信号只是导致真实信号的信噪比出现下降；

2）当功率位于－150 dBW 与－139 dBW 之间时，真实信号和欺骗信号相关峰均位于捕获程序检测阈值之上，接收机会捕获到两个相关峰，这种情形如图 6 所示。此时，若欺骗信号的信噪比高于真实信号的信噪比，接收机可能会错误检测到欺骗信号相关峰，进而捕获到欺骗信号。在这个区域，欺骗信号源并没有大幅度增加噪声基底，接收机面对欺骗攻击十分脆弱。

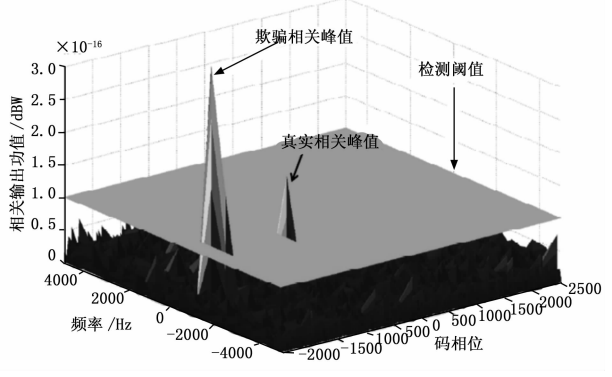

图 6 欺骗信号产生幅值超过检测阈值的更强功率相关峰值

3）总功率大于－139 dBW 时，真实信号信噪比降至检测阈值之下，接收机只能检测到欺骗信号产生的相关峰值，此时欺骗信号对接收机噪声基底影响较大，如图中观察可知，随着欺骗总功率的增加，欺骗信号相关峰成为占据接收机噪声基底的主要部分，欺骗信号的信噪比达到新的上限。换句话说，由于欺骗信号和本地码复制产生的相关峰引起噪声基底升高之后，欺骗信号产生更强的相关峰。

4 基于 SNR 测量的欺骗信号检测方法

欺骗信号入侵过程中会产生异常高值信噪比，基于此可以通过判断相关峰值来鉴别是否是真实信号。通过前面章节讨论可知，可以设置两个不同的检测阈值来判断所讨论的的 3 种分布。我们可以根据阈值公式设置第一道信噪比阈值，这样可以把 M_0 与 M_1、M_2 区别开来；紧接着可以设置第二道信噪比检测阈值，进一步在超过第一道检测阈值的所有相关峰值中检测出异常高值信噪比的相关峰。

为此，我们不妨假设真实信号的信噪比服从统一的数学分布，进而可得出真实信号功率服从一种边缘分布：

$$P_{D_l|\theta'_{l,1};M_{l,1}}(D_l \mid \theta'_{l,1};M_{l,1}) = \frac{1}{\alpha_{\max}-\alpha_{\min}} \times \int_{\alpha_{\min}}^{\alpha_{\max}} P_{D_l|\theta_{l,1};M_{l,1}}(D_l \mid \theta_{l,1};M_{l,1})\mathrm{d}\alpha_l \tag{24}$$

这里 $\theta'_{l,1}=[f_l{}^a,\ \tau_l{}^a]$ 表示对 l 路 PRN 信号多普勒频移、码延迟等相关参数变量的最大似然估计，$\alpha_{\max}$ 和 $\alpha_{\min}$ 分别表示真实信号信噪比最大值和最小值，考虑到一定的虚警率情况下我们有：

$$P_{FA}{}^{A|S} = \int_{\alpha_{th}}^{+\infty} P_{D_l|\theta'_{l,1};M_{l,1}}(D_l \mid \theta'_{l,1};M_{l,1})\mathrm{d}D_l \tag{25}$$

$P_{FA}{}^{A|S}$ 代表欺骗信号鉴别实验中设置的虚警率，$\alpha_{th}{}^{A|S}$ 代表欺骗信号鉴别中设置的信噪比检测阈值，图 7 展示了欺骗检测方法的性能，基于这种方法，如果一个相关峰值位于两个检测阈值之间，那么该信号就会被认为是真实信号。基于 SNR 的欺骗鉴别方法是一种较好的检测途径，但这种方法却有一定的局限性。显然当接收机噪声基底被欺骗信号抬高时，其鉴别有效性就会下降。例如上图所示，欺骗信号可以设置。

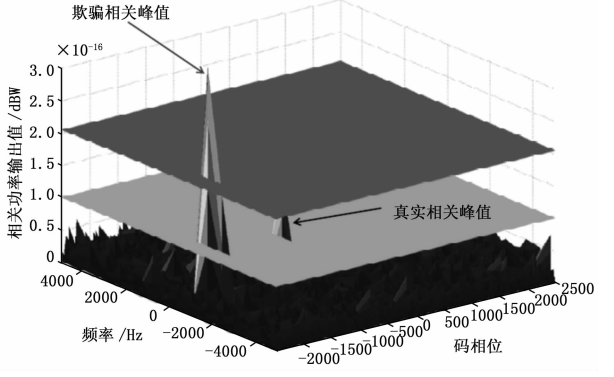

图 7 基于 SNR 的欺骗识别检测方法

5 结论

本文从分析欺骗信号对接收机捕获过程的影响出发，发现欺骗信号会增加噪声基底使得真实的卫星信号埋没，同时欺骗信号相关峰可以诱导接收机捕获到欺骗信号。在此基础上，提出了在捕获阶段利用信噪比（SNR）检测方法识别欺骗干扰信号的方法。

（下转第 35 页）

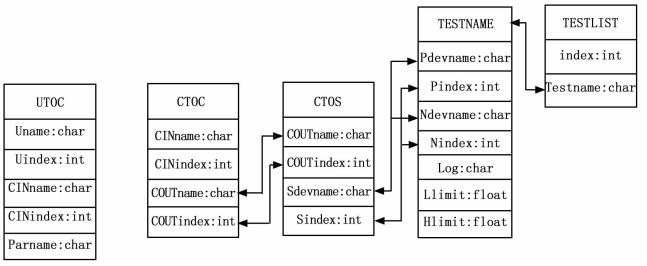

图 4　试验配置数据模型

- if $x=0, y \leqslant f(x,y,z) \leqslant z$;
- if $x=1, f(x,y,z) \geqslant y$;
- if $x=2, f(x,y,z) \leqslant y$;
- if $x=3, f(x,y,z)=y$。

参数 x 为判剧逻辑关系映射，其中 $x=0$ 时，参数 y,z 都有效，且 $y \leqslant z$；在 $x=1,2,3$ 时，仅参数 y 有效。

3　试验结果与分析

3.1　功能性验证

根据上述软、硬件设计方法，基于 PXI 总线设计了一种遥测系统自动化测试平台。该平台可以完成多达数百路参数的巡检测试与激励输出，也可完成多路相关参数的同时测试，完全满足系统的测试需求。测试平台可根据不同的测试项目需求编制不同的测试流程，图 5 所示为某巡检测试项目中系统的运行界面。在该测试项目中，测试流程按照事先编制好的流程进行通道的控制切换和数据解析，测试结果依据参考值的不同表达方式自动识别与判读，整个测试过程系统自主完成，无须人工干预。

3.2　通用性验证

与以往遥测系统测试设备采用面向仪器的设计方法不同，该平台在设计时采用面向信号的设计方法。在面对不同的测试需求时，只需要添加试验配置模块中的测试对象模型（UTOC）数据库和测试流程模型（TESTNAME）数据库，不同测试流程与测试对象的映射通过添加测试流程列表模型（TESTLIST）数据库完成。

目前该测试平台在软硬件未做任何更改的前提下，仅通过配置不同的数据库文件和测试电缆，已在多型运载火箭遥测系统集成验证中进行了应用。

图 5　运行界面

4　结论

本文针对运载火箭遥测系统的测试需求，设计了一种遥测系统自动化测试平台。该平台不仅可以完成多参数的巡检测试和相关参数的同时测试，而且整个测试过程完全实现了自动化测试与判读，无须人工干预。目前已在多个型号取得了较好的应用效果。

参考文献：

[1] 方心虎，等. 液体弹道导弹与运载火箭总体设计 [M]. 北京：宇航出版社，1991.

[2] National Instrument Corporation，LabVIEW Measurement Manual [Z]. 2012.

[3] 陈锡辉，张银鸿. LabVlEW 8.20 程序设计从入门到精通 [M]. 北京：清华大学出版社，2007.

[4] 黄晓晴，王纬国，梁　岳，等. 自动测试系统软件技术通用型研究综述 [J]. 测控技术，2012，20 (2)：1－4.

[5] 吕晓峰，马　羚，冯小南. ATS 软件平台的通用性研究与设计 [J]. 计算机测量与控制，2012，20 (2)：538－540.

(上接第 32 页)

参考文献：

[1] 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 [A]. ION 2009 International Technical Meeting [C]. Anaheim，CA，2009.

[2] Humphreys T E. Detection strategy for cryptographic GNSS anti－spoofing [J]. IEEE Transactions on Aerospace and Electronic Systems，2013，49 (2)：1073－1090.

[3] Nielsen J，Broumandan A，Lachapelle G. GNSS spoofing detection for single antenna handheld receivers [J]. Journal of the Institute of Navigation，2011，58 (4)：335－344.

[4] Jafarnia－Jahromi A，Lin T，Broumandan A，et al. Detection and mitigation of spoofing attacks on a vector based tracking GPS receiver [A]. Proceedings of the International Technical Meeting of The Institute of Navigation [C]. New － port Beach，CA，United states. 2012：790－800.

[5] Wesson K，Shepard D，Humphreys T E. Straight talk on anti－spoofing：securing the future of PNT [J]. GPS World，2012，23 (1)：32－39.

[6] Humphreys T E，Ledvina B M，Psiaki M L，et al. Assessing the spoofing threat：development of a portable GPS civilian spoofer [A]. ION GNSS 2008. Savannah [C]. GA，USA，2008：1198－1209.

[7] 胡彦逢，卫星导航欺骗式研究 [D]. 海军工程大学，2014.

[8] 胡彦逢，边少锋，曹可劲，等. GNSS 接收机欺骗干扰功率控制策略 [J]. 中国惯性技术学报，2015，23 (2)：207－209.

[9] 黄　龙，吕志成，王飞雪. 针对卫星导航接收机的欺骗干扰研究 [J]. 宇航学报，2012 (07)：884－890.

[10] 黄　龙，龚　航，朱祥维，等. 针对 GNSS 授时接收机的转发式欺骗干扰技术研究 [J]. 国防科技大学学报，2013，35 (4)：93－96.

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

[12] 王茂锋，王少华. GNSS 抗欺骗干扰技术解析 [J]. 通信设计与应用，2015 (07)：56－57.