doi:10.11887/j.cn.201603008 http://journal.nudt.edu.cn

GNSS 双接收机抗欺骗技术*

肖 岭,唐小妹,李柏渝,孙广富
(国防科技大学 电子科学与工程学院,湖南 长沙 410073)

摘 要:欺骗干扰能使目标接收机得出错误的位置、时间结果,是GNSS应用安全性的一个严重威胁。提出一种利用两个接收机伪距测量值单差的抗欺骗方法,利用方差分析技术推导基于伪距单差的欺骗信号最优检测量,并分析检测量的统计特性。经分析,接收机噪声、接收机基线长度和卫星个数等参数对检测性能的影响较大;在接收机噪声和卫星个数未知的情况下,可以通过增大接收机基线长度来提高检测性能。仿真结果表明,当接收机间的基线长度为10 m时,0.01虚警概率下,欺骗信号的检测概率可达98%。

关键词:欺骗干扰;伪距单差;方差分析
中图分类号:TN95 **文献标志码**:A **文章编号**:1001-2486(2016)03-045-05

A GNSS anti-spoofing technique based on dual-receiver

XIAO Ling, *TANG Xiaomei*, *LI Baiyu*, *SUN Guangfu*
(College of Electronic Science and Engineering, National University of Defense Technology, Changsha 410073, China)

Abstract: The spoofing interference can mislead target receiver in resulting in wrong position and time, which is a serious threat to the security of GNSS applications. An anti-spoofing method using the pseudo-range single-differences of two receivers was proposed. Using the variance analysis technique, the optimal spoofing detection variable based on the pseudo-range single-differences was deduced and the statistical character of the detection variable was analyzed. After analyzing, the parameters such as the receiver noise, the receiver baseline, and the satellite number have a large influence on the detection performance; as the receiver noise and satellite number are uncertain, the detection performance can be improved by increasing the length of baseline. When the length of baseline is 10 meters, the simulation results illustrate that the spoofing detecting probability is up to 98% if the false alarm rate is 0.01.

Key words: spoofing interference; pseudo-range single-differences; analysis of variance

当前,由全球导航卫星系统(Global Navigation Satellite System, GNSS)提供的位置、速度和时间(Position, Velocity and Time, PVT)服务深刻影响着人们的生活,广泛应用于车辆运输导航、飞机导航及着陆系统、电网时间同步、数字通信网络时间同步、银行及股票市场交易时间同步、紧急救援、汽车租赁中的车辆定位等领域。随着应用的深入,人们也越来越关注卫星导航应用的安全性和可靠性;然而由于到达地面的GNSS信号比较微弱,而且民用GNSS信号工作频点及信号体制等是公开的,所以GNSS信号很容易被干扰。

在所有的干扰类别中,欺骗干扰是危害最大的一类干扰。欺骗干扰指通过发射和真实卫星信号相似的模拟信号,使目标GNSS接收机输出欺骗方设计的位置、时间结果,从而达到对目标接收机载体的控制。如果系统使用这些错误的信息,将带来严重的后果。比如:欺骗无人机进行导航使用的GNSS接收机而致无人机偏离航线[1];拉偏移动通信网络的同步时间导致通信阻塞中断[2];拉偏电网系统的同步时间导致电力输送故障[3]等。

鉴于GNSS接收机欺骗干扰的严重危害性,许多学者研究了欺骗干扰的抑制技术,这些技术主要通过分析信号的带内功率[4-5]、相关峰质量[6-7]以及信号来向的空间分布特性[8-12]等特征来检测并抑制欺骗信号。由于带内功率监测不能区分阻塞干扰和欺骗干扰、相关峰质量监测无法区分多径干扰和欺骗干扰,因此这些方法的应用具有局限性。由于欺骗信号一般由同一个天线发射,来自于同一个方向,而真实信号由各个卫星发射,来自于不同的方向,因此信号来向监测是判

* **收稿日期**:2015-09-07
基金项目:国家自然科学基金资助项目(61403413)
作者简介:肖岭(1986—),男,河南方城人,博士研究生,E-mail:xiaoling_nudt@163.com;
孙广富(通信作者),男,教授,博士,博士生导师,E-mail:sunguangfu_nnc@163.com

断欺骗信号的有力证据。文献[8－9]利用天线阵,通过测量信号的入射方向来检测欺骗信号。真实信号的入射方向是多样的,而欺骗信号的入射方向是相同的。该方法的实现需要对天线阵进行校准,且用时较长。文献[10]提出了一种基于相位的方差分析(Phase only ANalysis Of VAriance, PANOVA)技术,通过分析信号到达两个接收天线的一致性来检测欺骗信号,该方法在信噪比(Signal Noise Ratio, SNR)大于 10 dB 时能够有效检测欺骗干扰,当 SNR 小于 10 dB 时,检测性能较差。当位于不同位置的接收机同时被欺骗时,这些接收机将得出相同的定位结果,文献[11－12]利用这一特征给出了一种多接收机定位结果校验的抗欺骗技术,但该方法要求接收机之间的距离至少大于两倍定位精度,并且只有当接收机处于相同的欺骗环境下、都被欺骗信号控制时才能有效检测欺骗干扰。因此,本文提出一种基于双接收机伪距单差的抗欺骗方法,利用方差分析(ANalysis Of VAriance, ANOVA)技术分析不同信号伪距单差均值的一致性来检测欺骗信号。

1 测量值模型

本节分析真实信号与欺骗信号存在情况下的伪距单差观测量模型。

1.1 真实信号伪距单差模型

真实信号的空间分布如图 1 所示,此时两接收机的伪距单差为:

$$\begin{aligned}\Delta\rho^i_{\mathrm{BA}} &= \rho^i_{\mathrm{B}} - \rho^i_{\mathrm{A}} \\ &= d \cdot <\boldsymbol{\gamma}^i, \boldsymbol{\gamma}_{\mathrm{BA}}> + c(dt_{\mathrm{B}} - dt_{\mathrm{A}}) + n^i \end{aligned} \quad (1)$$

式中:ρ^i_{A},ρ^i_{B} 分别表示接收机 A 和 B 测得的第 i 颗卫星到达接收机天线的伪距值;d 为接收机 A 和 B 的接收天线之间的距离,在本文的应用中该值小于 1 km,因此可以认为两个接收机测得伪距中电离层和对流层误差相同,且可以认为真实信号到达两个接收机的入射方向相同;$\boldsymbol{\gamma}^i$,$\boldsymbol{\gamma}_{\mathrm{BA}}$ 分别表示在参考坐标系下第 i 颗卫星信号的单位方向矢量和接收天线 A 到天线 B 的单位方向矢量;c 为光速;dt_{A},dt_{B} 分别表示接收机 A 和 B 的钟差;n^i 为接收机噪声量,$n^i \sim N(0,\sigma^2)$,σ^2 为接收机 A 和 B 热噪声差的方差,此量与两个接收机的构造及接收信号功率有关。

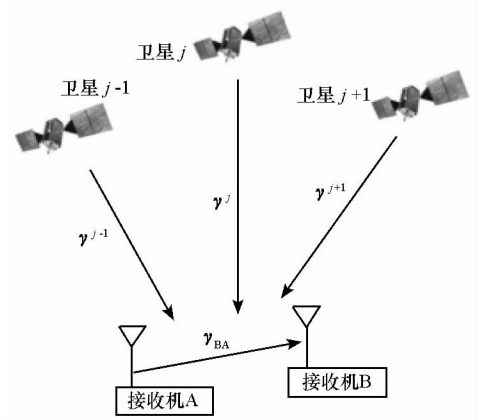

图 1 真实信号的空间分布和双接收机欺骗检测系统示意图

Fig. 1 Illustration of the real signal geometry distribution and dual-receiver spoofing detection system

1.2 欺骗信号伪距单差模型

欺骗信号的空间分布如图 2 所示,此时两接收机的伪距单差为:

$$\begin{aligned}\Delta\rho^i_{\mathrm{BA}} &= (d_{\mathrm{B}} - d_{\mathrm{A}}) + c(dt_{\mathrm{B}} - dt_{\mathrm{A}}) + n^i \\ &= \beta_s + n^i \end{aligned} \quad (2)$$

式中:d_{A},d_{B} 分别表示欺骗信号发射天线到接收机 A,B 的接收天线之间的距离;β_s 整合了所有相同的分量,其关系如式(3)所示,式中等号右端各个分量都由两个接收机决定,而与发射欺骗信号的卫星无关。

$$\beta_s = (d_{\mathrm{B}} - d_{\mathrm{A}}) + c(dt_{\mathrm{B}} - dt_{\mathrm{A}}) \quad (3)$$

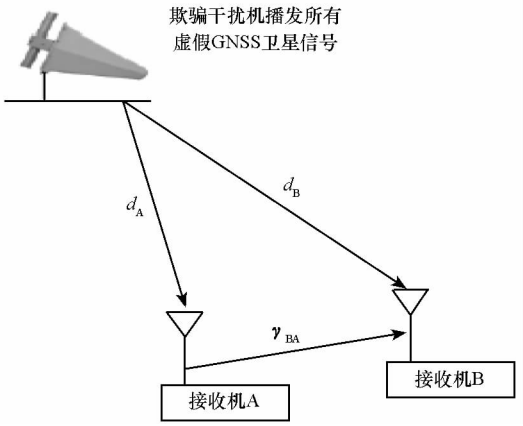

图 2 欺骗信号的空间分布和双接收机欺骗检测系统示意图

Fig. 2 Illustration of the spoofing satellite signal geometry distribution and dual-receiver spoofing detection system

2 欺骗信号检测量

由式(1)和式(2)可见,真实信号不同卫星的伪距单差观测量的均值是不同的,而欺骗信号不同卫星的伪距单差观测量的均值是相同的,这是真实信号与欺骗信号之间一个显著的差别,因此可以根据这一特征来检测欺骗信号。

ANOVA 是一种区分不同集合均值差异的技术[13],本文将该技术扩展到欺骗信号检测方面的

应用,通过利用该技术分析伪距单差观测量的均值特性来检测欺骗干扰。下面简要介绍 ANOVA 技术,推导广义似然比检测(Generalized Likelihood Ratio Test, GLRT)准则下的最优检测量,并给出基于伪距单差的欺骗信号检测量。

2.1 ANOVA 技术简介

假设来自 K 个集合的观测的模型有如式(4)所示:

$$\begin{aligned} &p_{i,j}=\mu_i+v_{i,j},\\ &i=0,1,\cdots,K-1;\quad j=0,1,\cdots,N_i-1 \end{aligned} \tag{4}$$

式中:N_i 为第 i 集合的观测量个数;μ_i 为第 i 集合的均值;$v_{i,j}$ 为观测噪声。经典的 ANOVA 技术中噪声分量 $v_{i,j}$ 具有如下假设:

(Ⅰ)$v_{i,j}$ 服从 0 均值高斯分布,即:

$$v_{i,j}\sim N(0,\sigma_i^2) \tag{5}$$

式中,σ_i^2 为第 i 集合的方差。

(Ⅱ)$v_{i,j}$ 相互独立且所有集合的方差相等,即:

$$\sigma_i^2=\sigma^2,\forall i\in\{0,1,\cdots,K-1\} \tag{6}$$

在上述模型下,ANOVA 的目的是区分如式(7)所示的假设检验问题:

$$\begin{cases} H_0:\forall i,k,\quad \mu_i=\mu_k\\ H_1:\exists i,k,\quad \mu_i\neq\mu_k \end{cases} \tag{7}$$

所有观测量 $p_{i,j}$ 的联合概率分布为:

$$f(\boldsymbol{p})=\frac{1}{(2\pi\sigma^2)^{N/2}}\cdot\exp\left\{-\frac{1}{2\sigma^2}\sum_{i=0}^{K-1}\sum_{j=0}^{N_i-1}(p_{i,j}-\mu_i)^2\right\} \tag{8}$$

式中:$\boldsymbol{p}$ 为观测量矢量,$\boldsymbol{p}=\{p_{i,j}\}$;$N$ 为所有观测量的个数,$N=\sum_{i=0}^{K-1}N_i$。

则在 GLRT 准则下的最优检测统计量为:

$$l(\boldsymbol{p})=\frac{\max_{\mu_o,\mu_1,\cdots,\mu_{K-1}}f(\boldsymbol{p}\mid H_1)}{\max_{\mu}f(\boldsymbol{p}\mid H_0)} \tag{9}$$

经计算,可得:

$$l(\boldsymbol{p})=\sum_{i=0}^{K-1}\sum_{j=0}^{N_i-1}(p_{i,j}-\hat{\mu})^2-\sum_{i=0}^{K-1}\sum_{j=0}^{N_i-1}(p_{i,j}-\hat{\mu}_i)^2 \tag{10}$$

式中:$\hat{\mu}$ 为所有观测量的均值估计量,$\hat{\mu}=\frac{1}{N}\sum_{i=0}^{K-1}\sum_{j=0}^{N_i-1}p_{i,j}$;$\hat{\mu}_i$ 为第 i 集合的均值估计量,$\hat{\mu}_i=\frac{1}{N_i}\sum_{j=0}^{N_i-1}p_{i,j}$。

2.2 欺骗检测统计量

由式(1)和式(2)知,不同卫星的伪距单差满足式(4)的模型,且噪声特性满足 ANOVA 要求的式(5)、式(6)假设,因此上小节得出的最优检测量式(10)可直接应用于欺骗检测。

在基于伪距单差欺骗信号检测的 ANOVA 应用中,每颗卫星对应一个集合,每个集合的观测量个数都是 1,则式(10)中的 $\hat{\mu}_i=\Delta\rho_{\mathrm{BA}}^i$,从而最优检测量变为:

$$l(\Delta\boldsymbol{\rho}_{\mathrm{BA}})=\sum_{i=0}^{K-1}(\Delta\rho_{\mathrm{BA}}^i-\hat{\mu})^2 \tag{11}$$

式中,$\Delta\boldsymbol{\rho}_{\mathrm{BA}}=\{\Delta\rho_{\mathrm{BA}}^i\}$,$\hat{\mu}=\frac{1}{K}\sum_{i=0}^{K-1}\Delta\rho_{\mathrm{BA}}^i$。

3 统计特征分析

为了表述方便,记 $d_i=E(\Delta\rho_{\mathrm{BA}}^i-\hat{\mu})$。下面分析 H_0,H_1 条件下式(11)所示检测量的统计特性。

在 H_0 条件下(欺骗干扰),由式(2)易知 $d_i=0,\forall i\in\{0,1,\cdots,K-1\}$,则 $l(\Delta\boldsymbol{\rho}_{\mathrm{BA}})/\sigma^2$ 服从自由度为 $K-1$ 的中心 χ^2 分布(所有式(11)的相同分量 $\hat{\mu}$ 导致 1 个自由度的损失),其概率密度函数为:

$$f(x\mid H_0)=\begin{cases}\dfrac{x^{\frac{K-3}{2}}\exp(-\frac{x}{2})}{2^{\frac{K-1}{2}}\Gamma(\frac{K-1}{2})}, & x>0\\ 0, & x\leqslant 0\end{cases} \tag{12}$$

式中,$\Gamma(\cdot)$ 为伽马函数。进一步可得 H_0 条件下 $l(\Delta\boldsymbol{\rho}_{\mathrm{BA}})$ 的均值和方差为:

$$\begin{cases}\mu_{H_0}=E[l(\Delta\boldsymbol{\rho}_{\mathrm{BA}})\mid H_0]=(K-1)\sigma^2\\ \sigma_{H_0}^2=D[l(\Delta\boldsymbol{\rho}_{\mathrm{BA}})\mid H_0]=2(K-1)\sigma^4\end{cases} \tag{13}$$

在 H_1 条件下(真实信号),由式(1)知 $\exists i\in\{0,1,\cdots,K-1\}$,$d_i\neq 0$,则 $l(\Delta\boldsymbol{\rho}_{\mathrm{BA}})/\sigma^2$ 服从自由度为 $K-1$ 非中心参量 $\lambda=\sum_{i=0}^{K-1}d_i^2$ 的非中心 χ^2 分布,其概率密度为[14]:

$$f(x\mid H_1)=\begin{cases}\dfrac{1}{2}\left(\dfrac{x}{\lambda}\right)^{(K-3)/4}\exp\left(-\dfrac{x+\lambda}{2}\right)I_{(K-3)/2}(\sqrt{\lambda x}), & x>0\\ 0, & x\leqslant 0\end{cases} \tag{14}$$

式中,$I_n(\cdot)$ 为第一类 n 阶修正贝塞尔函数。经计算可得 H_1 条件下 $l(\Delta\boldsymbol{\rho}_{\mathrm{BA}})$ 的均值和方差为:

$$\begin{cases}\mu_{H_1}=E[l(\Delta\boldsymbol{\rho}_{\mathrm{BA}})\mid H_1]=(K-1)\sigma^2+\lambda\\ \sigma_{H_1}^2=D[l(\Delta\boldsymbol{\rho}_{\mathrm{BA}})\mid H_1]=2(K-1)\sigma^4+4\lambda\sigma^2\end{cases} \tag{15}$$

本文采用 Neyman-Pearson 准则确定判决门

限，鉴于 $f(x|H_1)$ 中的 λ 值与卫星位置有关，不方便计算，而 $f(x|H_0)$ 只与接收机的热噪声有关，便于计算，故可通过 H_0 的漏检概率来确定门限，如式(16) 所示：

$$P[l(\Delta\boldsymbol{\rho}_{\mathrm{BA}}) > T|H_0] = \alpha \tag{16}$$

式中，α 为 H_0 的漏检概率。当检测量小于 T 时，接受 H_0(即判决当前接收机被欺骗)；否则拒绝 H_0 接受 H_1(即判决信号为真实信号)。欺骗信号检测概率和虚警概率如式(17) 所示：

$$\begin{cases} P_d = \int_0^T f(x|H_0)\mathrm{d}x = 1-\alpha \\ P_f = \int_0^T f(x|H_1)\mathrm{d}x \end{cases} \tag{17}$$

4 仿真验证与分析

定义检测量在 H_0，H_1 条件下分布的隔离度 S 如式(18)所示，S 越大，则检测性能越好。

$$S = (\mu_{H_1} - \sigma_{H_1}) - (\mu_{H_0} + \sigma_{H_0}) \tag{18}$$

将式(13)、式(15)代入式(18)可得：

$$S = \lambda - \sigma^2\left[\sqrt{2(K-1)} + \sqrt{2(K-1) + \frac{4\lambda}{\sigma^2}}\right] \tag{19}$$

由式(19)可见主要有三个参数影响检测性能：①热噪声方差 σ^2；②接收机之间的基线长度 d 导致的非中心参量 λ；③卫星个数 K。

为了验证分析上述参数对检测性能的影响，利用蒙特卡洛方法仿真了不同参数下的接收机特性(Receiver Operation Character, ROC)曲线。针对这三个参数设计了三组仿真验证，每组仿真的参数配置如表 1 所示。

表 1 仿真参数配置

Tab. 1 Simulation parameter configurations

编号	σ^2/m^2	d/m	K
1	1,2,4①	10	6
2	2	5,10,15	6
3	2	10	4,6,8

注：①当接收机设计完成后，伪距测量值的测量噪声主要与信号类型及信号功率有关，GPS L1 C/A 信号在 38 dB-Hz 时的测量噪声方差约为 1 m^2[15]，假设两个接收机设计完全相同，仿真中 σ^2 选择 1,2,4 分别模拟信号质量较好、一般、较差的情况。

仿真中每组验证的仿真次数为 10^6；设置两个接收机之间的方向矢量为 $\boldsymbol{\gamma}_{\mathrm{BA}} = [1\ 0\ 0]$，则：

$$<\boldsymbol{\gamma}^i, \boldsymbol{\gamma}_{\mathrm{BA}}> = \cos\varepsilon_i\cos\alpha_i \tag{20}$$

式中，ε_i 和 α_i 分别为入射信号的方位角和俯仰角。真实卫星信号的入射方向是等可能随机的，因此仿真中 $\{\varepsilon_i\}$ 建模为 $[0,360°]$ 上面的均匀分布，$\{\alpha_i\}$ 建模为 $[0,90°]$ 上面的均匀分布。

由仿真结果图 3、图 4、图 5 可以得出以下结论：

1)在固定其他参数只考虑一个参数时，热噪声越小、接收机距离越大、卫星个数越多则检测性能越好；

2)鉴于热噪声及卫星个数随环境和时间变化，不是恒定值，因此可以通过增大接收机基线长度来提高检测性能；

3)由图 4 可见当两接收机距离为 10 m 时，虚警概率为 0.01 时的检测概率可达 98%。

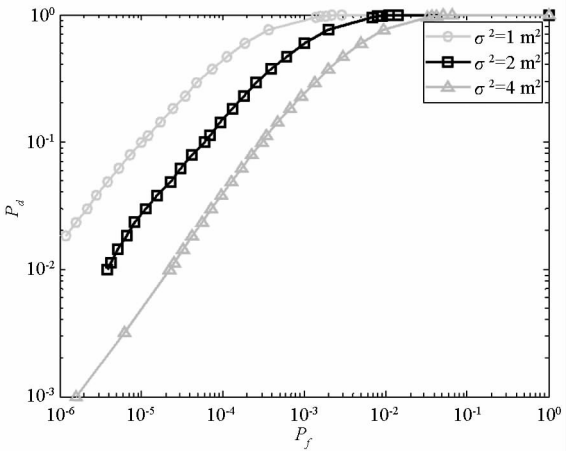

图 3 参数配置 1 仿真结果

Fig. 3 Simulation result of parameter configuration 1

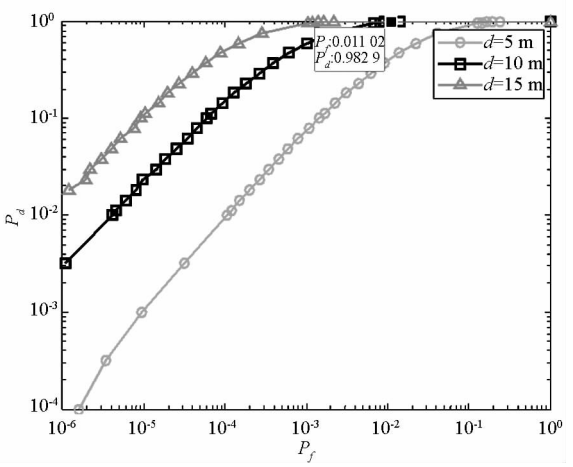

图 4 参数配置 2 仿真结果

Fig. 4 Simulation result of parameter configuration 2

5 结论

欺骗干扰是 GNSS 服务安全使用的一个严重威胁，故提出一种利用双接收机伪距单差的抗欺骗技术，将两个普通的接收机置于一个合适的距

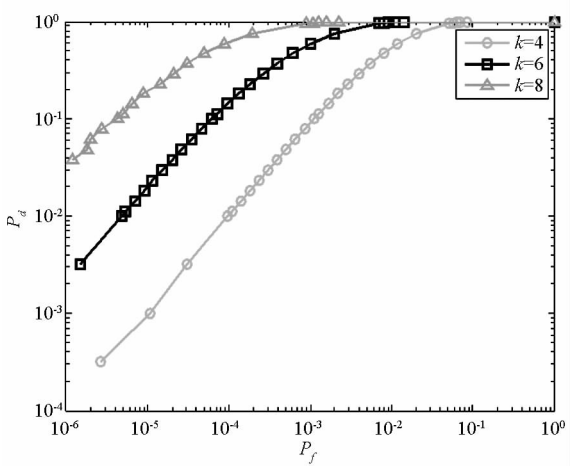

图 5　参数配置 3 仿真结果

Fig. 5　Simulation result of parameter configuration 3

离(约 10 m)即可有效地检测欺骗信号。该技术可以应用于数字通信、输电网络等所使用 GNSS 时间服务的安全防护,也可以应用于载体长度不小于 10 m 的交通运输所使用的 GNSS 导航服务的安全防护。

参考文献(References)

[1] Humphreys T. UAVs vulnerable to civil GPS spoofing[EB/OL]. [2014 - 12 - 11]. http://www. insidegnds. com/node/3131.

[2] 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.
HUANG Long, GONG Hang, ZHU Xiangwei, et al. Research of reradiating spoofing technique to GNSS timing receiver [J]. Journal of National University of Defense Technology, 2013, 35(4): 93 - 96. (in Chinese)

[3] Zhang Z, Gong S, Dimitrovski A D, et al. Time synchronization attack in smart grid: impact and analysis[J]. IEEE Transactions on Smart Grid, 2013, 4(1): 87 - 98.

[4] Akos D M. Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC)[J]. Journal of the Institute of Navigation, 2012, 59(4): 281 - 290.

[5] Jafarnia-Jahromi A, Broumandan A, Nielsen J, et al. Pre-despreading authenticity verification for GPS L1 C/A signals[J]. Journal of the Institute of Navigation, 2014, 61 (1): 1 - 11.

[6] Cavaleri A, Pini M, Presti L L, et al. Signal quality monitoring applied to spoofing detection[C]// Proceedings of the 24th International Technical Meeting of the Satellite Division of the Institute of Navigation, 2011: 1888 - 1896.

[7] Kuusniemi H, Bhuiyan M Z H, Kröger T. Signal quality indicators and reliability testing for spoof-resistant GNSS receivers [J]. European Journal of Navigation, 2013, 11(2): 12 - 19.

[8] 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 [C]//Proceedings of the International Technical Meeting of the Institute of Navigation, 2009: 124 - 130.

[9] Trinkle M, Zhang Z, Li H, et al. GPS anti-spoofing techniques for smart grid applications[C]//Proceedings of the 25th International Technical Meeting of the Satellite Division of the Institute of Navigation, 2012: 1270 - 1278.

[10] Borio D. PANOVA tests and their application to GNSS spoofing detection [J]. IEEE Transactions on Aerospace and Electronic Systems, 2013, 49(1): 381 - 394.

[11] Swaszek P F, Hartnett R J, Kempe M V, et al. Analysis of a simple, multi-receiver GPS spoof detector[C]//Proceedings of the International Technical Meeting of the Institute of Navigation, 2013: 884 - 892.

[12] Heng L, Makela J J, Dominguez-Garcia A D, et al. Reliable GPS-based timing for power systems: a multi-layered multi-receiver architecture[C]//Proceedings of Power and Energy Conference at Illinois (PECI), 2014: 1 - 7.

[13] Barnard G A. Comparing the means of two independent samples[J]. Journal of the Royal Statistical Society, 1984, 33(3): 266 - 271.

[14] 何选森. 随机过程[M]. 北京:人民邮电出版社, 2009: 199 - 201.
He Xuansen. Stochastic processes[M]. Beijing: Posts & Telecom Press, 2009: 199 - 201. (in Chinese)

[15] Kaplan E D, Hegarty C J. Understanding GPS: principles and applications[M]. 2nd ed. USA: Artech House, 2006.