DOI:10.13442/j.gnss.1008-9268.2020.01.011

基于功率变化的移动终端欺骗干扰检测方法

范广腾，冉德超，张飞，庹洲慧
（军事科学院国防科技创新研究院，北京 100071）

摘 要：对欺骗信号的功率检测是目前最常用的欺骗检测方法之一，但欺骗源可以通过调整发射的信号功率，仍然可实现对环形范围内所有终端的欺骗攻击. 针对该问题，本文提出了一种基于信号功率变化的移动终端欺骗干扰检测方法，该方法利用了真实卫星和欺骗源与终端在距离上差异的本质属性，通过终端运动情况下真实信号与欺骗信号在相同距离上信号功率变化的不同，实现对近距离欺骗干扰源的有效检测. 本文建立了移动终端导航信号功率变化模型，并在此基础上给出了针对欺骗信号的二元假设检验方法. 通过理论分析和仿真实验，验证了本文提出的基于信号功率变化的移动终端欺骗干扰检测技术的有效性，当干扰源距离终端小于 2 000 m，终端运动距离大于 200 m 即可实现在 1%的虚警概率下实现对 97%以上欺骗攻击的有效检测.

关键词：卫星导航；欺骗攻击；欺骗干扰检测；移动终端；功率变化
中图分类号：TN967.1　　**文献标志码**：A　　**文章编号**：1008-9268(2020)01-0066-05

0 引 言

随着卫星导航定位技术的发展，卫星导航系统用户数量正不断增加，并且已大量进入社会关键应用领域，比如紧急救援、电力、通信、交通运输等领域. 由于目前的导航接收机完全信任所接收到的全球卫星导航系统(GNSS)信号，因此任何组织、个人都可以通过发射虚假的欺骗干扰信号使接收机得出错误的定时定位信息，从而瘫痪诸如电力系统、银行金融系统、无线通信系统等社会关键基础设施，甚至在军事应用中改变敌方无人机、导弹等自主导航载体的运动轨迹，使其到达欺骗干扰方指定的位置[1]. 如何对敌方实施有效的欺骗干扰攻击以及保护己方导航接收机不受欺骗干扰影响，以满足强对抗条件下的导航战的需求，是 GNSS 领域的一大研究热点[2].

目前现有文献都是针对欺骗信号与真实信号在某一特定属性上的区别进行设计. 这些属性包括信号到达角[3]、伪距[4]、信号载噪比[5]、信号功率[6]、导航电文[7]等. 其中信号功率是区别真实信号与欺骗信号的重要属性[6]，现有利用信号功率进行欺骗信号检测的方法，只是通过接收信号的绝对功率大小进行判断，高级的欺骗源可以根据被欺骗终端的位置调整发射功率，从而实现环形范围内，所有导航终端无法通过功率大小检测判断欺骗信号.

针对该问题，本文给出了一种基于信号功率变化的欺骗信号检测方法. 该方法利用现有的欺骗信号生成器与真实导航卫星在距离属性上的本质差别，移动终端在接收真实信号时功率变化较小，而接收欺骗信号时功率变化较大，从而通过检测功率变化值，实现对欺骗信号的有效检测. 该方法理论上，可以检测所有距离较近的欺骗干扰源，大大增加了欺骗干扰的难度.

1 针对功率检测的欺骗信号生成

目前基于信号功率检测的欺骗干扰检测方法，已经广泛运用于导航接收机中，因此欺骗者为实现一次成功的欺骗干扰，必须通过信号功率检测. 高级的欺骗者可以根据需要欺骗的区域，调整发射信号功率，从而使终端接受到的欺骗信号功率在检测

收稿日期：2019-10-08
资助项目：国家自然科学基金(61801503)
通信作者：冉德超 E-mail：18061962@qq.com

门限以内[8-9].

假设导航接收机功率检测门限的上限为 P_u，下限为 P_l，那么欺骗信号可成功欺骗的区域为圆环形，即欺骗半径 $R_l < R < R_u$，其中，R_l 为圆环的内测半径，R_u 为圆环的外侧半径，如图 1 所示.

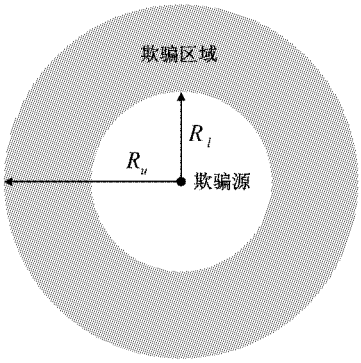

图 1　基于信号功率检测的欺骗区域

由图 1 可知，采用信号功率检测方法后，欺骗成功率变为 η，即：

$$\eta = \frac{R_u^2 - R_l^2}{R_u^2}. \tag{1}$$

因此，由上面分析可知，即便使用功率检测的欺骗检测方法，欺骗生成器通过设置合理的发射功率，仍然可以欺骗圆环区域内的所有导航终端[8].

2　基于信号功率变化的检测方法

真实导航卫星与欺骗干扰源的本质区别是到达导航接收机的距离不同，导航卫星为中圆地球轨道(MEO)以上轨道卫星，距离接收机 20 000 km 以上；而欺骗干扰源距离接收机通常为 1 ～ 10 km，远远小于真实导航卫星，如图 2 所示.

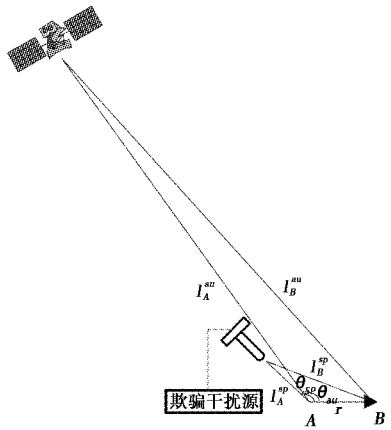

图 2　终端接收真实信号与欺骗信号的几何关系

图中，假设导航接收机从 A 点运动到 B 点，运动距离为 r，真实卫星到 A 和 B 点的距离分别为 l_A^{au} 和 l_B^{au}，欺骗干扰源到 A 和 B 点的距离分别为 l_A^{sp} 和 l_B^{sp}，真实卫星到接收机运动方向的夹角为 θ_{au}，欺骗干扰源到接收机运动方向的夹角为 θ_{sp}，接收机在 A 点接收到真实信号和欺骗信号功率分别为 P_A^{au} 和 P_A^{sp}，在 B 点接收到真实信号和欺骗信号功率分别为 P_B^{au} 和 P_B^{sp}，真实信号功率变化为 δ_B^{au}(dB)：

$$\begin{aligned}\delta_B^{au} &= \left| 10\lg\left(\frac{l_B^{au\,2}}{l_A^{au\,2}}\right) \right| \\ &= \left| 10\lg\left[1 + \frac{2r\cos\theta_{au}}{l_A^{au}} + \left(\frac{r}{l_A^{au}}\right)^2\right] \right|. \end{aligned} \tag{2}$$

同理可得欺骗信号功率变化为 δ_B^{sp}(dB)：

$$\delta_B^{sp} = \left| 10\lg\left[1 + \frac{2r\cos\theta_{sp}}{l_A^{sp}} + \left(\frac{r}{l_A^{sp}}\right)^2\right] \right|. \tag{3}$$

由于真实卫星距离接收机的距离 $l_A^{au} \gg r$，因此式(2)中 $\delta_B^{au} \approx 0$，而欺骗干扰源距离接收机较近，因此 δ_B^{sp} 存在较大幅度变化，从而可以根据这一区别，实现对欺骗信号的检测.

令功率变化的比值为检测量 δ，根据文献[10]可知，在接收真实卫星信号(假设 $H0$)以及欺骗干扰信号(假设 $H1$)条件下 δ 的概率分布为

$$\begin{cases} H0: \delta_{au} \sim \dfrac{1}{\sqrt{2\pi}\,x\sigma} \mathrm{e}^{-\frac{(\lg x)^2}{2\sigma^2}}, \\ H1: \delta_{sp} \sim \dfrac{1}{\sqrt{2\pi}\,x\sigma} \mathrm{e}^{-\frac{[\lg x - \mu(l,r,\theta)]^2}{2\sigma^2}}. \end{cases} \tag{4}$$

式中：x 为功率变化比值的观测量；σ 为功率变化比值的均方差；检测量均值 $\mu(l,r,\theta)$ 是欺骗干扰源到终端距离 l，接收机运动距离 r 以及运动方向夹角 θ 的函数

$$\mu(l,r,\theta) = \left| 10\lg\left[1 + \frac{2r\cos\theta}{l} + \left(\frac{r}{l}\right)^2\right] \right|. \tag{5}$$

由图 3 可以看出，检测量均值越大，欺骗信号检测的成功率越高，图 4～6 示出了不同情况下的检测量均值，可以看出，基于信号功率变化的移动终端欺骗干扰检测方法对欺骗干扰的检测性能与欺骗源到终端距离 l，终端位移距离 r 和欺骗信号的入射角 θ 有关. 当 $H1$ 条件下检验统计量的均值越大，其概率密度分布函数与 $H0$ 条件下间隔越大，欺骗干扰检测性能越好.

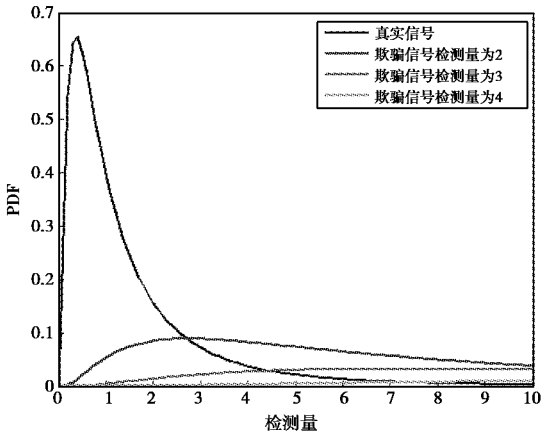

图 3 接收真实信号($H0$)和欺骗信号($H1$)下的概率分布

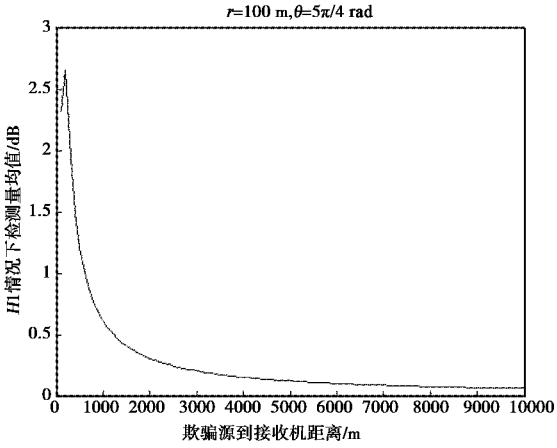

图 4 $H1$ 条件下检测量均值与欺骗源到终端距离的关系

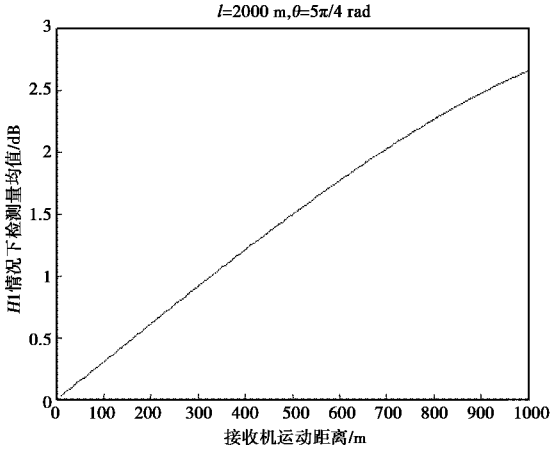

图 5 $H1$ 条件下检测量均值与终端运动距离的关系

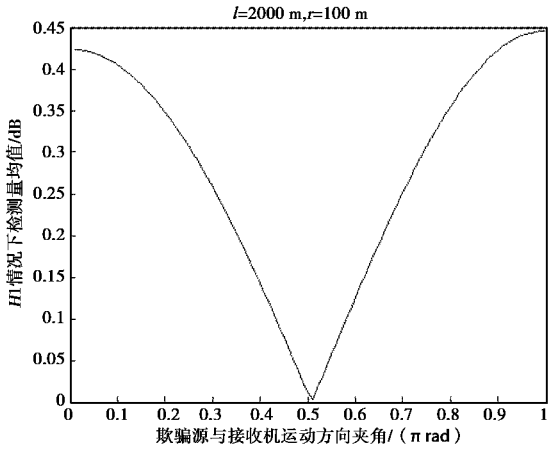

图 6 $H1$ 条件下检测量均值与夹角的关系

3 性能分析

针对不同的欺骗源到接收机距离,接收机位移距离和欺骗信号的入射角,进行蒙特卡洛仿真验证. 每种条件下,仿真次数为 10 000 次,得到基于信号功率变化的移动终端欺骗干扰检测方法的 ROC 曲线如图 7～9 所示.

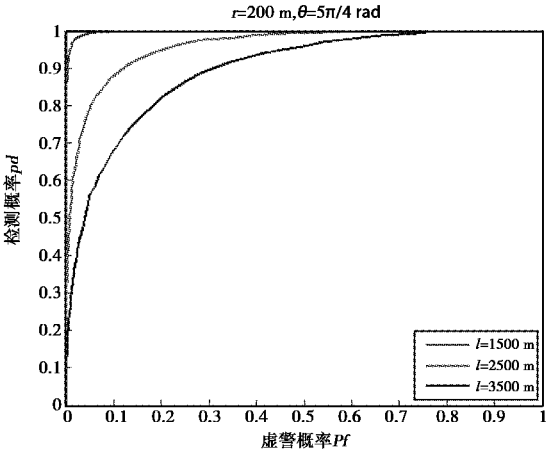

图 7 不同欺骗源距离的 ROC 曲线

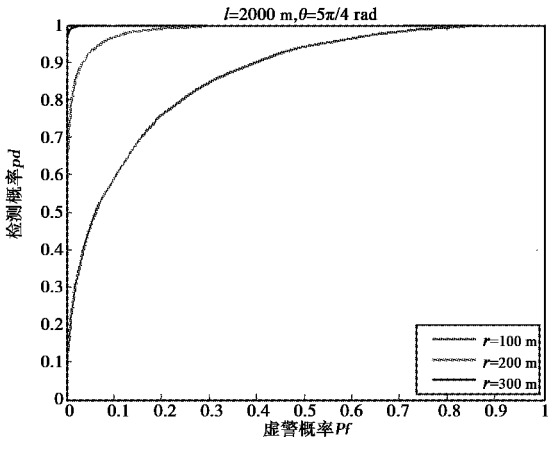

图 8 不同终端运动距离的 ROC 曲线

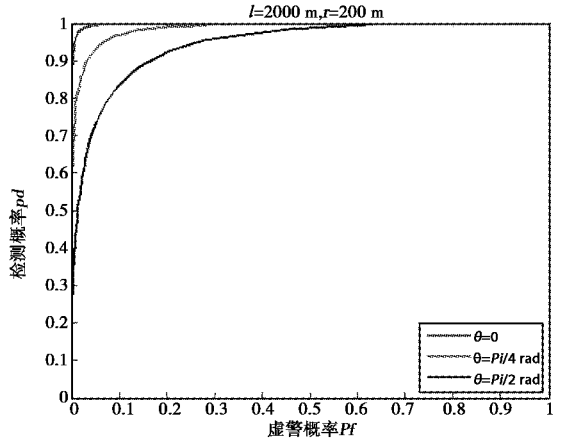

图 9　不同运动方向下的 ROC 曲线

根据图 7～9 的仿真结果，令虚警概率为 5%，则不同参数下的检测概率如表 1 所示.

表 1　不同参数下的检测概率

参数选择	检测概率		
$r=200$ m，$\theta=5\pi/4$ rad	$l=1500$ m	$l=2500$ m	$l=3500$ m
	99%	80%	56%
$l=2000$ m，$\theta=5\pi/4$ rad	$r=100$ m	$r=200$ m	$r=300$ m
	51%	94%	99%
$l=2000$ m，$r=200$ m	$\theta=0$ rad	$\theta=\pi/4$ rad	$\theta=\pi/2$ rad
	99%	93%	76%

由图 9 和表 1 可以看出：

1）欺骗源距离终端越近，基于信号功率变化的欺骗干扰检测技术的检测性能越优；

2）终端运动距离越远，基于信号功率变化的欺骗干扰检测技术的检测性能越优；

3）欺骗信号入射方向与终端运动方向夹角越小，基于信号功率变化的欺骗干扰检测技术的检测性能越优.

4）当终端运动距离超过 200 m，可以有效检测 2 km 范围内的欺骗源.

以上结论与第 2 节中理论分析结论一致.

为进一步说明基于功率变化的移动终端欺骗干扰检测方法相比与传统基于绝对功率的检测方法的优势，下面通过仿真比较在不同欺骗源发射功率下，仿真参数如表 2 所示，两种方法的检测概率如图 10 所示.

表 2　仿真参数

仿真参数	数值
欺骗源距离	1500 m
终端运动距离	300 m
欺骗信号入射角度	$\pi/4$ rad
终端功率检测精度	0.7 dB
虚警概率	5%

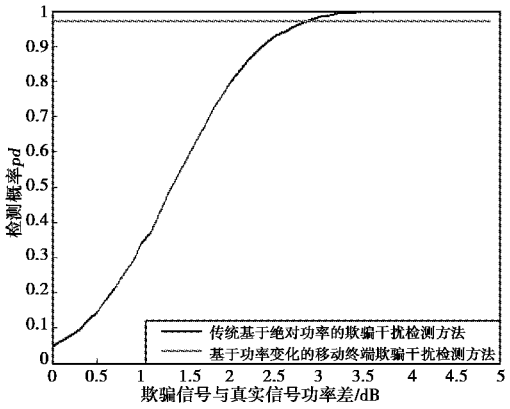

图 10　不同运动方向下的 ROC 曲线

由图 10 可知，传统基于绝对功率的欺骗干扰检测方法当欺骗信号相比真实信号高出 2.5 dB 以上时，可以得到 90%以上的检测概率，但当欺骗信号与真实信号功率比较接近时，检测性能急剧恶化，而基于功率变化的移动终端欺骗干扰检测方法的检测性能与欺骗信号的绝对功率无关，只要移动终端运动较长距离即可获得 95%以上的检测性能.

4　结束语

针对运动状态下的导航终端，本文提出了一种通过检测终端接收导航信号功率变化进行欺骗干扰检测的方法. 理论分析和仿真实验结果表明，只要干扰源距离终端小于 2000 m，天线运动距离大于 200 m，欺骗信号与终端运动方向夹角满足正负 45°内的条件，本文提出的基于信号功率变化的欺骗干扰检测算法即可在 1%的虚警概率下实现对 97%以上欺骗攻击有效检测，该方法可以有效解决只利用信号功率大小进行欺骗信号检测的局限性.

参考文献

[1] 张瑞华，贾琼琼，吴仁彪. 利用矢量跟踪环路的欺骗干扰检测与抑制方法[J]. 信号处理，2018，34(6)：688-696.

[2] 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，2012，33(7)：884-890.

[3] DANESHMAND S，JAFARNIA-JAHROMI A，BROUMANDON A，et al. A low-complexity GPS anti-spoofing method using a multi-antenna array[C]// Proceedings of the 25th International Technical Meeting of the Satellite Division of The Institute of Navigation，Nashville，Tennessee，USA，2012：1233-1243.

[4] LEDVINA B M, BENCZE W J, GALUSHA B, et al. An in-line anti-spoofing device for legacy civil GPS receivers[C]//Proceedings of the Institute of Navigation International Technical Meeting, San Diego, Calif, USA, 2010: 698-712.

[5] JAHROMI J A, BROUMANDAN A, NIELSEN J, et al. GPS spoofer countermeasure effectiveness based on signal strength, noise power, and C/N0 observables[J]. International Journal of Satellite Communications and Networking, 2012, 30(4): 181-191. DOI: 10.1002/sat.1012.

[6] DEHGHANIAN V, NIELSEN J, LACHAPELLE G. GNSS spoofing detection based on signal power measurements: Statistical analysis[J]. International Journal of Navigation and Observation, 2012(7): 1-8. DOI: 10.1155/2012/313527.

[7] CHENG X J, XU J N, CAO K J, et al. An authenticity verification scheme based on hidden messages for current civilian GPS signals[C]//Fourth International Conference on Computer Sciences and Convergence Information Technology, 2009: 345-352. DOI: 10.1109/ICCIT.2009.91.

[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): 207-210, 218.

[9] JAFAMIA. JAHROMI A, LIN T, BROUMANDAN A, et al. Detection and mitigation of spoofing attacks on a vector based tracking GPS receiver[C]//Proceedings of the International Technical Meeting of the Institute of Navigation, Newport Beach, CA, United States, 2012: 1-11.

[10] JOVANOVIC A, BOTTERON C, FARINE P A. Multi-test detection and protection algorithm against spoofing attacks on GNSS receivers[C]//IEEE/ION Position, Location and Navigation Symposium-Plans, PLANS2014, 2014. DOI: 10.1109/PLANS.2014.6851501.

作者简介

范广腾 (1988—),男,博士,助理研究员,主要研究方向为卫星导航技术.

冉德超 (1987—),男,博士,助理研究员,主要研究方向为卫星控制技术.

张飞 (1988—),男,博士,助理研究员,主要研究方向为云计算技术.

Detection method of spoofing in mobile terminal based on power variation

FAN Guangteng, RAN Dechao, ZHANG Fei, TUO Zhouhui

(*National Innovation Institute of Defense Technology, Academy of Military Sciences, Beijing* 100071, *China*)

Abstract: Power detection of spoofing signal is one of the most commonly used spoofing detection methods. However, the spoofing source can still achieve spoofing attack on the terminal in the ring by adjusting the power of the transmitted spoofing signal. In order to solve this problem, this paper proposes a spoofing detection method for mobile terminals based on signal power Variation. This method utilizes the essential attributes of distance difference between real satellite and deception source and terminal, it can detect spoofing jamming sources in close range effectively. In this paper, the power ratio model of mobile terminal signal is established, and on this basis, the binary hypothesis test for deception signal is given. Through theoretical analysis and simulation experiments, the validity of the proposed spoofing detection technology for mobile terminals based on signal power variation is verified. When the distance between the jammer and the terminal is less than 2000 meters, and the distance between the terminal and the terminal is more than 200 meters, the effective detection of spoofing attack can be realized under 1% false alarm probability.

Keywords: satellite navigation; spoofing attack; spoofing detection; mobile terminal; power variation