电网技术

北斗欺骗干扰对电力授时的影响与对策分析

陈建平[1]，王旭旭[2]，罗欣宇[2]，章坚武[2]，周剑峰[1]，谢咏海[1]

（1. 浙江双成电气有限公司，浙江 绍兴 312071；
2. 杭州电子科技大学 通信工程学院，杭州 310018）

摘 要：电力系统中对时间同步精度要求较高，多采用北斗时间与晶振时间相结合的方式为电力设备提供时间基准。但由于民用北斗信号的公开性及低功率特点，使得电力授时单元所依靠的北斗信号易受欺骗干扰的威胁。对此，首先分析了电力授时模块的工作原理；接着介绍了北斗欺骗干扰模型和欺骗干扰的验证实验；最后提出了抗卫星欺骗干扰的对策。经验证，上述对策已应用于实际电力授时系统中，并取得良好效果。

关键词：电力系统；时间同步；北斗欺骗干扰；抗欺骗干扰方法

文章编号：1007-1881(2020)11-0034-06 **DOI**: 10.19585/j.zjdl.202011006

中图分类号：TN967.1 **文献标志码**：B **开放科学(资源服务)标识码(OSID)**：

Study on the Influence of Beidou Deception Jamming on Power Time Service and the Countermeasures

CHEN Jianping[1], *WANG Xuxu*[2], *LUO Xinyu*[2], *ZHANG Jianwu*[2], *ZHOU Jianfeng*[1], *XIE Yonghai*[1]

(1. Zhejiang Shuangcheng Electric Co., Ltd., Shaoxing Zhejiang 312071, China;
2. School of Communication Engineering, Hangzhou Dianzi University, Hangzhou Zhejiang 310018, China)

Abstract: High accuracy of time synchronization is required in the power system, thus the combination of Beidou time and crystal oscillation time is often used to provide a time reference for power equipment. However, due to the accessibility and low power of the civil Beidou signal, the Beidou signal relied on by the power timing unit is vulnerable to the threat of deception jamming. In this paper, the working principle of the power timing module is analyzed firstly; then, the model of Beidou deception jamming is introduced, and the verification experiment of deception jamming is given. Finally, countermeasures of deception jamming in the power system are concluded. It is proved that the countermeasures used in the time services system have achieved favorable results.

Keywords: power system; time synchronization; Beidou deception jamming; Beidou countermeasures against deception jamming

0 引言

在电力系统中，对同步时间的精度要求较高。同步向量测量装置、雷电定位系统、行波故障测量装置等电力设备要求时间同步精度达到 1 μs[1]。在我国 2017 年制定的国家电力标准中，要求授时系统的内部时间精度应在 1 μs 之内，并优先采用北斗卫星信号作为主要授时手段[2-3]。目前正在运行的北斗二代系统，其授时精度可以达到 50 ns，可满足电力授时精度的要求。

由于民用北斗卫星信号的公开性以及低功率特点，使得电力授时单元所依靠的北斗授时信号易受欺骗干扰的威胁[4]。对北斗接收模块的北斗欺骗干扰是指利用伪北斗卫星信号生成器发射伪北斗信号，使北斗接收机计算到伪当地时间和伪

基金项目：国家自然科学智能电网联合基金(NSF U1866209)

当地位置的一种干扰[5]。目前电力信息化系统中的时间服务器依靠 GNSS(全球导航卫星系统)来校对时间，如果在北斗接收天线附近架设伪 GNSS 卫星生成器发射伪 GNSS 信号，会导致信息系统由于时间错乱而不能正常工作，造成的损失难以估计[6-7]。

关于卫星欺骗干扰的研究主要集中在 GPS(全球定位系统)位置欺骗干扰上，对北斗接收机时间欺骗干扰的研究相对较少。林肯实验室 Gilmore 和 Delaney 的实验表明，功率为 1W 的干扰机可以使 85 km 以内的 C/A 码接收机无法工作[8]。国网公司 2013 年第 2 期《信息安全通报》中介绍的灾备中心事故证明了时间出错对电网安全的重大影响。本文通过实验验证了北斗接收模块受到欺骗干扰后输出了伪位置和伪时间[9]，从而可能影响电网的正常运行。

本文首先分析了电力授时单元的工作原理，北斗可通过校正晶振时间，从而降低授时时间的随机误差和漂移误差。之后介绍了北斗欺骗干扰模型和欺骗干扰的验证实验。最后提出了抗卫星欺骗干扰的对策。

1　电力授时单元

为了保证电力授时系统百纳秒级的时间精度，电力授时单元结合北斗卫星时间和晶振时间进行授时[10]。

北斗卫星时间的授时精度可达到 50 ns，长期稳定性较好。但是考虑到卫星信号传播路径的复杂性和不确定性，接收模块所处环境的差异性，以及接收模块解析信号时间的随机性，北斗时间的短期稳定性较差。而晶体振荡器的振荡频率主要受所施加电压和所处环境温度、气压的影响，具有较高的短期稳定性，但晶体振荡器所产生的时间误差会逐渐积累，最终造成时间漂移，所以晶体振荡器的长期稳定性较差[11]。

北斗授时时间与晶振授时时间的特点对比见表 1。

鉴于北斗授时和晶振授时之间存在长期稳定性和短期稳定性不均衡的问题，大多数设备采用北斗时间纠正晶振时间的方式为电力设备提供授时信号[12]。电力授时单元如图 1 所示。

电力授时单元中授时时间的信号来源包括北斗时间和晶振时间。其中，北斗时间由北斗芯片解析北斗导航数据产生，晶振时间由晶振及其控制电路产生。

表 1　北斗授时与晶振授时特点对比

授时方式	北斗授时	晶振授时
精度	50 ns	视具体晶振而定
干扰因素	卫星运动轨迹、信号传播路径、接收机环境、信号处理噪声	环境温度、气压
长期稳定性	优	差
短期稳定性	差	优

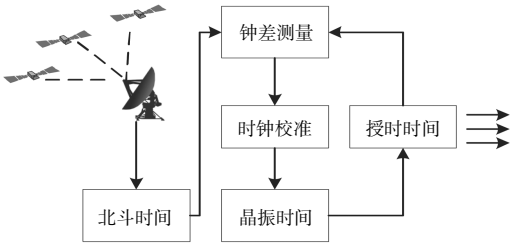

图 1　电力授时单元

由于长期使用晶振时间会出现时间漂移的现象，所以当时间漂移较大时，必须利用北斗时间对晶振时间进行矫正，这一功能主要由钟差测量和时钟校准完成。钟差测量单元可以一直测量授时时间和北斗时间的偏差值，当时间偏差值超过阈值时，时钟校准功能可以根据时间偏差量调整晶振的控制电路，使得晶振时间的漂移在误差允许范围之内。

由以上分析可知，电力授时单元依赖北斗时间进行时间校正。但北斗时间容易受到欺骗干扰，在受欺骗干扰的情况下，电力授时单元授时时间将由伪北斗信号决定，此时电力授时时间精度将无法得到保障。

2　欺骗干扰

2.1　北斗欺骗干扰与 GPS 欺骗干扰

GPS 导航卫星系统同时在 2 个频点上产生信号，其中 L1 频点信号为民用部分，载波频率为 1575.42 MHz，且其导航电文格式对外公开。而 L2 频点信号为军用部分，同时用到了 2 个频点的信号，且导航点位格式保密。L2 频点上调制的BPSK

(二元相移键控)信号源包括 3 个来源：P(Y)码、P(Y) 码和导航电文模二加、C/A 码和导航电文模二加，选用哪种信号进行 BPSK 信号调制由选择器选择，目前L2 信号一般选择 P(Y)码和导航电文模二加作为 BPSK 调制信号源。

北斗卫星发射卫星信号包括 B1，B2 和 B3 共 3 个频段。但是，北斗民用部分只使用了其中的 B1 和 B2 频段，B3 频段主要为军用部分。B1 和 B2 频段上的信号由卫星原子钟产生，载波频率分别为 1 561.098 MHz 和 1 207.140 MHz。B1 和 B2 频点上的信号采用 QPSK(四相移相键控)调制方式，由于正交相位上的信号处于测试阶段，北斗导航信号也可以视为 BPSK 调制信号。

已知卫星信号的导航电文、载波频率、调制方式等信息，伪卫星信号源可以模拟发射卫星信号。适当增加伪卫星信号的功率，调整发送信号的时间戳信息就可以实现对卫星接收机的欺骗干扰，使得卫星接收机解析出错误的时间信息和位置信息[13]。由于北斗信号和 GPS 信号民用部分导航电文、载波频率、调制方式信息都是公开的，所以 GPS 信号和北斗信号都会受到欺骗干扰的威胁[14-15]。

图 2 为自主式欺骗干扰的示意图，在卫星信号接收机正常接收真实卫星信号的同时，欺骗信号产生模块产生功率较高的伪卫星信号，通过发射天线发射卫星信号，使得卫星信号接收机定位到错误的位置。欺骗产生模块可以是编程设计的软件定义无线电模块，也可以是现有的卫星信号模拟器。

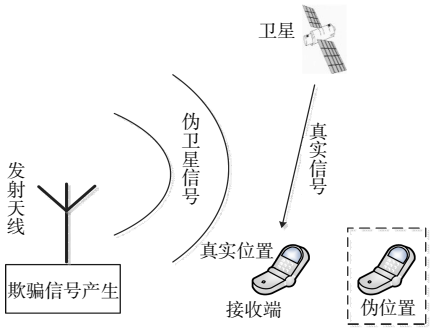

图 2　自主式欺骗干扰示意图

文献[16]指出，随着软件无线电技术的发展，伪导航卫星信号源的制作成本已大幅降低。无论从技术上，还是从成本上，通过制作伪卫星信号源实施欺骗干扰的可行性都很高。

文献[17]从理论和实验上研究了实施北斗/GPS 欺骗干扰的伪卫星信号功率要求，仿真结果表明，欺骗信号功率在高于真实卫星功率 4 dB 的情况下，即可实现对卫星接收机长达 50 min 的欺骗干扰。

文献[18]根据 GPS 卫星接收机位置与伪卫星信号源之间的距离，调节伪卫星信号源发射信号时延，可实现对卫星接收机的无缝欺骗干扰[17]。

2.2　欺骗干扰伪卫星信号个数分析

图 3 为卫星定位示意图。可以根据伪距公式计算出当地位置与当地时间。由于未知量包括当地位置三维坐标和当地时间，所以理论上列出 4 个伪距方程就可以解析出接收机的位置和时间变量[24]。

$$\rho_1(x_u)=\sqrt{(x_u-x_{s_1})^2+(y_u-y_{s_1})^2+(z_u-z_{s_1})^2}+cb+n_{\rho_1}，(1)$$

$$\rho_2(x_u)=\sqrt{(x_u-x_{s_2})^2+(y_u-y_{s_2})^2+(z_u-z_{s_2})^2}+cb+n_{\rho_2}，(2)$$

$$\rho_3(x_u)=\sqrt{(x_u-x_{s_3})^2+(y_u-y_{s_3})^2+(z_u-z_{s_3})^2}+cb+n_{\rho_3}，(3)$$

$$\rho_4(x_u)=\sqrt{(x_u-x_{s_4})^2+(y_u-y_{s_4})^2+(z_u-z_{s_4})^2}+cb+n_{\rho_4}，(4)$$

式中：下标 1，2，3，4 表示接收到的卫星信号序号；ρ_i 代表发射信号的卫星到接收模块的距离，其值等于发射时间戳 t_i、接收时间 t 之差与光速 c 的乘积；(x_u, y_u, z_u)代表当地位置；$(x_{s_i}, y_{s_i}, z_{s_i})$代表发射卫星的位置；$b$ 代表当地时间与标准卫星时间的偏差。在忽略伪距误差 n_{ρ_1}，n_{ρ_2}，n_{ρ_3}，n_{ρ_4}的情况下，根据式(1)—式(4)可以求出 x_u 和 b，进而求出(x_u, y_u, z_u)当地位置及当地时间$(t-b)$。

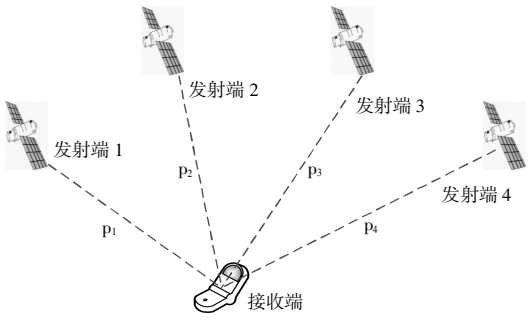

图 3　导航卫星定位原理

由于自发式欺骗干扰是一种卫星信号发生器模拟发射伪卫星信号、掩盖真实卫星信号的欺骗干扰，所以接收机接收伪卫星信号进行定位授时也至少接收 4 颗伪卫星的信号。

2.3　北斗欺骗干扰验证实验

为保证北斗接收模块既可以收到空中北斗信号，还可以收到伪北斗信号，将接收模块放置在室外空旷的草坪上，并设置伪北斗信号发生器与北斗接收模块的距离为 100 m 左右，通过计算机记录接收模块的实验数据进行验证实验。

伪北斗信号发生器最多可以模拟 12 颗北斗卫星信号，由于接收模块解算位置信息至少需要 4 颗卫星的信号，因此分别让信号模拟器产生 4，5，6，7，8 颗伪卫星信号进行实验验证。

当计算机记录接收模块收到的位置和时间数据发生跳变时，并在 2 min 内保持稳定状态，可认为北斗接收模块解析出了伪卫星信号，欺骗干扰获得成功。改变伪北斗信号发生器的功率，记录发射伪北斗信号时间和欺骗干扰成功时间，两者之差即为北斗接收模块同步到伪北斗信号发生器的时间。所得实验结果如图 4 所示。

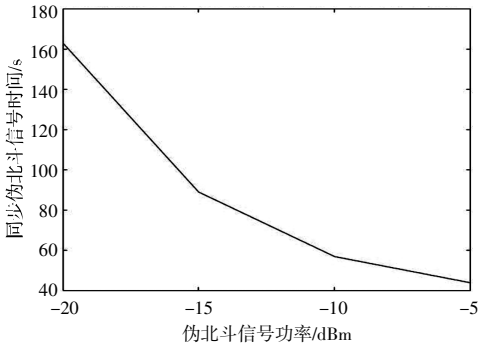

图 4　同步伪信号所需时间与伪信号功率关系

从图 4 可以看出，随着伪北斗信号功率的增大，北斗接收模块同步到伪北斗信号的时间越快。当伪北斗信号的功率为−5 dBm 时，同步伪北斗信号的时间仅为 44 s 左右。

由前文分析可知，一旦北斗接收模块同步到伪北斗信号，事实上已失去与真实北斗信号的同步。同时，当精度较低的伪北斗时间信号纠正电力授时单元中的时间信号时，会造成授时单元输出信号精度的降低。根据 2.2 节的分析，虽然实现欺骗干扰需要 4 颗卫星信号，但实验发现要完成干扰欺骗至少需要 6 颗伪北斗卫星信号[9]。

3　抗北斗欺骗干扰对策

在电力系统中需要有效抑制欺骗干扰以保护电力授时单元正常工作。利用欺骗干扰检测技术检测出存在的欺骗干扰之后，需要在授时单元关闭对伪卫星信号的接收。授时单元失去卫星时间的校正作用之后，依靠晶振可以保证输出时间的短期稳定性。欺骗干扰抑制技术使接收机只解析真实卫星信号，同时保证授时单元输出时间的短期稳定性和长期稳定性。

3.1　欺骗干扰检测

目前，卫星欺骗干扰检测的方法主要包括信号幅度检测方法、信号波达角检测方法和分布式接收机检测方法。

文献[19−20]利用卫星接收芯片的信号功率估计功能检测导航卫星信号的绝对功率，从而判断接收机是否受到欺骗干扰攻击。这种办法在欺骗干扰信号的功率较大时，检测效果较好。目前，随着欺骗干扰技术的发展，欺骗干扰的功率不必远大于真实卫星信号的功率，此时采用绝对功率检测的方法很难检测出卫星欺骗干扰。

文献[21]提出一种在天线端依据信号波达角完成欺骗干扰检测的办法。目前，大多数卫星导航欺骗干扰源大都采用单一天线发射欺骗信号[22]。在这种欺骗干扰模型下，不同路欺骗干扰信号到达接收机天线的方向角相同；在不受欺骗干扰的情况下，不同真实导航卫星信号到达接收机天线的方向角不会完全相同。利用欺骗干扰信号与真实导航卫星信号的这一空间特性，可根据信号波达角完成欺骗干扰检测。但在空域进行波达角检测，需要阵列天线来完成，增加了进行欺骗干扰检测的成本。

文献[6，18]提出了 2 种分布式检测欺骗干扰的办法。其中，文献[6]通过 2 个天线获取 2 组卫星信号的信噪比，通过信噪比差值的离散程度来判断接收机是否受到了欺骗干扰。但该方法要求2个接收天线的辐射方向角满足互补关系，且实验环境过于理想，在室外真实环境中利用该方法检测欺骗干扰的效果有待进一步验证。文献[18]从理论上提出了分布式接收机间相对距离为 0，可以根据分布式接收机间的相对距离检测欺骗干

扰。该方法受环境噪声影响较小，且对分布式接收机天线的要求不高。

以上方法均需对信号进行解析，而对于北斗接收模块很难从中提取出相关信号，故直接对解析后输出信号的位置和时间数据是否发生跳变进行检测，虽然有一定滞后，但可靠性高，非常实用。

3.2 欺骗干扰抑制

目前，欺骗式干扰抑制技术主要分为 2 类：RAIM(接收机完好性监视)[22]技术和阵列天线[23]技术。

文献[22]中所提出的 RAIM 方法通过冗余导航卫星伪距测量来检测故障，在欺骗干扰环境中，伪卫星信号的伪距与真实卫星信号的伪距不同。但该方法需要修正导航定位芯片的工作机制，可实现性较小。

文献[24]利用天线间互相关处理估计出较强的欺骗式干扰子空间，再构造正交投影矩阵抑制欺骗式干扰。但是这种方法只适用于单欺骗干扰源的情况，在多欺骗干扰源的情况下，该方法抑制欺骗干扰信号效果不佳。

文献[7]考虑了单欺骗干扰源和多欺骗干扰源情况，分别采用 MUSIC 算法估算单欺骗干扰源波达角，采用 RELAX 算法估算多欺骗干扰源波达角。检测出伪卫星信号源波达角之后，构造伪卫星信号干扰子空间，然后利用正交补空间投影抑制伪卫星信号。

实验已经验证要完成欺骗干扰至少需要 6 颗伪北斗卫星信号[9]，所以单欺骗源实际上只能干扰正常接收，但不能完成欺骗，也容易抑制(比如前端采用简单滤波)，所以主要要抑制多欺骗干扰源。通过实验发现，可采取以下 2 种手段：

(1)由于人为的欺骗干扰源架设相对都比较低，抬高接收天线仰角可有效减少伪卫星信号的接收个数，如 6 颗以下就可以不受欺骗干扰的影响。

(2)北斗接收机前端采用高性能滤波器可以有效抑制欺骗干扰。通过对市场上北斗接收模块进行对比，发现一些北斗接收模块由于前端滤波器成本低廉、结构简单而使其性能较差，易受欺骗干扰影响。

4 结语

当前，电力授时单元主要采用北斗时间与晶振时间相结合的方式为电力时间同步提供高精度时间基准。但由于民用北斗信号的公开性及低功率特点，使得北斗信号容易受到欺骗干扰的威胁，且随着干扰技术的发展，实施北斗欺骗干扰的成本逐渐降低。电力授时单元受到北斗欺骗干扰后，授时精度将主要由伪北斗时间决定，严重影响电力设备的正常运行。

当前抗北斗欺骗干扰的方法研究主要集中在北斗欺骗干扰检测和北斗欺骗干扰抑制上。其中，北斗欺骗干扰检测技术可以保证授时时间的短期稳定性，而北斗欺骗干扰抑制技术可以同时保证北斗欺骗干扰的短期稳定性和长期稳定性。目前欺骗干扰检测的技术较为成熟，从节约成本的角度来看，可在不改动导航授时芯片工作机制的条件下，直接对解析后输出信号的位置和时间数据是否发生跳变进行欺骗检测。同时，采用抬高接收天线仰角可以从空域有效抑制伪北斗信号，或选择前端滤波性能较好的北斗接收模块从频域有效抑制伪北斗信号。经实验验证，上述方法已推广到实际电力授时系统中，并取得了良好的效果。

2019 年 5 月 17 日，随着第 45 颗北斗导航卫星成功发射，我国“北斗二号”区域导航系统建设圆满收官；同年，北斗三号系统建设启动；2020 年6 月 23 日，北斗三号最后一颗全球组网卫星发射成功，完成 30 颗卫星发射组网，至此北斗三号全球卫星导航系统星座部署比原计划提前半年全面完成。这也意味着我国的北斗导航终于和美国的 GPS、俄罗斯的格洛纳斯“平起平坐”“三分天下得其一”。随着北斗卫星全球组网“修成正果”，产业链共振效应也将释放。北斗的服务由北斗二号系统和北斗三号系统共同提供，可以相信有了北斗三号系统的支持，我国的北斗应用将走向全球，其抗干扰能力也会得到极大的提高。

参考文献：

[1] 赵莎.基于卫星共视法的电网时频测量及同步技术[J].计算机测量与控制,2016,24(12):49-52.

[2] 国家电网公司.智能变电站合并单元技术规范:Q/GDW 426—2010.北京:中国电力出版社,2010.

[3] 国家标准化管理委员会.智能变电站时间同步系统及设备技术规范:GB/T 33591—2017.北京:中国标准出版社,2017.

[4] 李昊洋.北斗导航信号欺骗干扰检测算法研究[J].电子

技术,2018,47(1):6-10.
[5] 张鑫.卫星导航欺骗干扰信号检测技术综述[J].全球定位系统,2018,43(6):1-7.
[6] ZHANG Z H,TRINKLE M,QIAN L J,et al.Quickest detection of GPS spoofing attack[C]//MILCOM 2012—2012 IEEE Military Communications Conference.Orlando:IEEE,2012:1-6.
[7] HAN S,YU Z,MENG W X,et al.GPS anti-spoofing technology based on RELAX algorithm in smart grid[C]//2015 10th International Conference on Communications and Networking in China (ChinaCom).Shanghai:IEEE,2015:637-642.
[8] 郇浩,牛景硕.GPS/BD 接收机抗干扰实验平台开发[J].实验技术与管理,2014,31(12):80-83.
[9] 车浩军,王旭旭,陈建平,等.针对 BD/GPS 接收模块欺骗干扰的实验研究[J].实验室研究与探索,2019,38(8):119-123.
[10] 谢荣平,孙凌枫,朱峰.时频中心时间同步方法[J].指挥信息系统与技术,2016,7(1):58-62.
[11] 姜雷,郑玉平,艾淑云,等.基于合并单元装置的高精度时间同步技术方案[J].电力系统自动化,2014,38(14):90-94.
[12] 叶增.卫星授时方法与星地同步数据处理技术研究[D].哈尔滨:哈尔滨工程大学,2010.
[13] ZHANG Y T,WANG L,WANG W Y,et al.Spoofing jamming suppression techniques for GPS based on DOA estimating[M]//Lecture Notes in Electrical Engineering.Berlin:Springer Berlin Heidelberg,2014:683-693.
[14] GUCMA M.New threat to global transport. GNSS Receiver Spoofing[J].Archives of Transport,2015,35(3):7-14.
[15] WANG F,LI H,LU M Q.GNSS spoofing countermeasure with a single rotating antenna[J].IEEE Access,2017,5:8039-8047.
[16] RANGANATHAN A,ÓLAFSDÓTTIR H,CAPKUN S.SPREE:a spoofing resistant GPS receiver[C]//Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking.New York City New York. New York:ACM,2016.
[17] 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.
[18] TIPPENHAUER N O,PÖPPER C,RASMUSSEN K B,et al.On the requirements for successful GPS spoofing attacks[C]//Proceedings of the 18th ACM conference on Computer and communications security.Chicago:ACM Press,2011.
[19] DEHGHANIAN V,NIELSEN J,LACHAPELLE G.GNSS spoofing detection based on receiver C/N_0 estimates[C]//Proceedings of International Technical Meeting of the Satellite Division of the Institute of Navigation.[S.l.:s.n.],2012:2878-2884.
[20] DEHGHANIAN V,NIELSEN J,LACHAPELLE G.GNSS spoofing detection based on signal power measurements:statistical analysis[J].International Journal of Navigation and Observation,2012:1-8.
[21] JAFARNIA JAHROMI A,BROUMANDAN A,NIELSEN J,et al.GPS spoofer countermeasure effectiveness based on signal strength,noise power,and C/N_0 measurements[J].International Journal of Satellite Communications and Networking,2012,30(4):181-191.
[22] LI J F,LI H,PENG C X,et al.Research on the random traversal RAIM method for anti-spoofing applications[C]//Lecture Notes in Electrical Engineering.Singapore: Springer Singapore,2019:593-605.
[23] 王璐,吴仁彪,王文益,等.基于多天线的 GNSS 压制式干扰与欺骗式干扰联合抑制方法[J].电子与信息学报,2016,38(9):2344-2350.
[24] 崔建华,程乃平,倪淑燕.阵列天线抑制欺骗式导航干扰信号方法研究[J].电子学报,2018,46(2):365-371.
[25] 鲁郁.北斗/GPS 双模软件接收机原理与实现技术[M].北京:电子工业出版社,2016.

收稿日期:2020-06-27

作者简介:陈建平(1969),男,高级工程师,长期从事电力工程技术研究。

章坚武(1961),男,教授,博士生导师,从事通信网络与信息安全研究。(通讯作者)

(本文编辑:方明霞)