

# 利用部分可信信号的导航终端欺骗干扰检测方法

王环宇 林红磊\* 欧钢 唐小妹

(国防科技大学电子科学学院卫星导航技术重点实验室 长沙 410073)

**摘要:** 导航信号认证服务处于初步部署阶段, 认证信号对地覆盖重数无法满足独立定位授时需求, 现有研究对这一阶段利用部分通过认证的信号, 即可信信号, 实现欺骗检测的方法关注度较低。针对这一现状, 该文根据欺骗攻击原理, 提出以可信信号为基准, 基于可信信号伪距残差的欺骗检测方法, 建立该场景下的欺骗检测模型, 并分析影响所提方法检测性能的因素。经过仿真, 在可信卫星数目为3颗、用户定位精度约10 m条件下, 当欺骗导致的定位偏差为100 m时, 该方法的平均欺骗检测概率可达0.96。此外, 该文对算法欺骗检测盲区进行了分析, 证明所提算法对于绝大部分欺骗导致的定位结果均有效。

**关键词:** 抗欺骗; 导航认证信号; 接收机自主完好性监测; 伪距残差

中图分类号: TN967.1

文献标识码: A

文章编号: 1009-5896(2024)10-4053-09

DOI: 10.11999/JEIT240067

## The Spoofing Detection Method of Navigation Terminal Using Partial Authenticated Signals

WANG Huanyu LIN Honglei OU Gang TANG Xiaomei

(Key Laboratory of Satellite Navigation Technology, College of Electronic Science and Technology,  
National University of Defense Technology, Changsha 410073, China)

**Abstract:** The navigation signal authentication service is in the initial stage. The coverage multiple numbers of the authentication signal to ground can not meet the requirement of independent positioning and timing. The existing research has paid little attention to the deception detection method based on partially trusted signals at this stage. Aiming at the status quo, according to the principle of spoofing attack, a spoofing detection method is proposed based on the pseudo-distance residual of the authentication signal, and the spoofing detection model is established in this scenario, and the factors that affect the detection performance of the proposed method are analyzed. After simulation, the average deception detection probability of the algorithm can reach 0.96 when the positioning deviation is 100 m, the positioning accuracy is about 10 m, and the number of trusted satellites is 3. In addition, the blind area of the algorithm is analyzed, and it is proved that the algorithm is effective for most of the deception positions.

**Key words:** Anti-spoofing; Navigation authentication signal; Receiver Autonomous Integrity Monitoring (RAIM); Pseudo-range residuals

### 1 引言

由于卫星导航系统采用单向广播体制, 民用导航信号格式公开, 恶意攻击方极易伪造民用卫星导航信号, 为用户获得真实可信的定位授时结果带来了挑战<sup>[1]</sup>。当前卫星导航用户应对欺骗攻击, 获得可信位置时间信息的方法包括两类: 导航设备层面<sup>[2]</sup>和卫星导航系统层面。本文关注系统层面的解决办法。系统层面的方法基于密码学原理, 在卫星导航信号中增加难以伪造的认证信息, 使用户设备具备区分真实信号和欺骗信号的能力<sup>[3]</sup>。国内外对导航

信号认证方法的研究主要集中在认证方案的设计上, 已投入试验阶段的主流认证方案是欧盟伽利略系统的公开服务导航消息认证(Open Service Navigation Message Authentication, OSNMA)<sup>[4,5]</sup>、美国GPS(Global Positioning System)的码片电文鲁棒性认证(Chips-Message Robust Authentication, Chimera)<sup>[6,7]</sup>、日本准天顶系统采用的导航电文摘要认证<sup>[8,9]</sup>等。这些方案主要面向的场景是接收机同时接收并通过认证的信号多于4颗星, 将通过认证的信号称为可信信号, 利用可信信号进行定位解算。考虑到当前导航信号认证服务仍处于实验或试运行阶段, 系统状态的优化升级需要逐步开展。在这一过程中, 无论认证信号部署在现有中高轨导航

收稿日期: 2024-01-29; 改回日期: 2024-09-05; 网络出版: 2024-09-09

\*通信作者: 林红磊 [linhonglei@nudt.edu.cn](mailto:linhonglei@nudt.edu.cn)

卫星系统还是正在发展中的低轨卫星系统<sup>[10]</sup>, 都可能由于认证信号播发策略或低轨卫星数目不足等原因而导致认证信号覆盖重数低于4重<sup>[11]</sup>, 使得接收机无法利用可信信号实现独立定位授时, 而业内对利用部分可信信号进行欺骗检测的方法研究较少。此外, 接收机已知自身位置的授时场景对利用少量可信信号实现欺骗检测也有较大需求。本文针对上述问题与需求开展研究。

欺骗信号通过改变导航终端的星地测量结果或电文信息, 实现对定位授时结果的控制。由于可信信号搭载了不可预测的认证信息, 可被视为抗欺骗信号, 本文将可信信号作为基准, 通过对比可信信号与常规导航信号参数的一致性实现欺骗信号检测。这一思路与传统的接收机自主完好性监测(Receiver Autonomous Integrity Monitoring, RAIM)算法有一定相似之处, 然而传统的RAIM算法在本文的应用背景下无法高效发挥可信信号的基准作用。同时, 现有的基于认证信号的欺骗检测方法中, 文献<sup>[12]</sup>利用3个及以上可信信号和一个无认证信号, 通过PVT(Position, Velocity, Time)计算和残差分析, 根据解算结果和参数结果间的一致性, 识别无认证信号是否受到欺骗。该方法不适用于本文的应用背景。因此本文重点研究存在可信信号时, 导航终端的欺骗存在性检测方法, 当可信信号数量小于4时, 利用可信伪距观测量、可信卫星位置以及终端采用常规导航信号得到的PVT结果3组参数, 根据伪距残差判断估算结果与实际测量结果的一致性, 实现对PVT结果的异常检测。

本文的其他部分按照以下结构展开: 第2节对欺骗信号模型与传统RAIM算法进行描述, 然后介绍本文提出的基于可信信号的欺骗检测算法模型, 并对影响该算法性能的因素进行分析; 第3节通过仿真两种应用场景, 分析不同因素对欺骗信号检测概率的影响; 第4节总结全文。

## 2 数学模型与问题描述

### 2.1 欺骗信号模型

生成式欺骗是民用场景的主要欺骗类型。文献<sup>[13]</sup>分析了生成式欺骗对接收机定位的影响, 对于利用伪距进行单点定位的接收机, 实现欺骗的主要方法是通过控制欺骗信号到接收机的时延, 从而改变码相位的测量结果, 进而实现伪距的欺骗。欺骗信号的码相位时延计算公式为

$$\Delta\tau = \Delta t_a - (\Delta t_s + t_p + \rho_s/c) \quad (1)$$

其中,  $\Delta\tau$ 表示欺骗信号和真实信号的码相位时延偏移量,  $\Delta t_a$ 为卫星信号到欺骗目标的传播时延,

$\Delta t_s$ 为卫星信号到欺骗器的传播时延,  $t_p$ 表示欺骗器内部的处理时延,  $\rho_s$ 表示欺骗器到欺骗目标之间的距离,  $c$ 表示光在真空中的传播速度, 取值为299792458 m/s。

式(1)转换为伪距的表达式, 等号两边同时乘光速可得位置欺骗模型为

$$\tilde{\rho} = \rho_a + c(-\Delta\tau_s) \quad (2)$$

$\tilde{\rho}$ 表示欺骗信号的伪距,  $\rho_a$ 表示卫星信号的真实伪距,  $\Delta\tau_s$ 表示欺骗信号的码相位时延。本文关注单点定位情况下的生成式欺骗场景, 在仿真中通过设定欺骗存在时的定位坐标或钟差来计算欺骗信号的伪距。

### 2.2 传统RAIM检测算法

接收机采用伪距定位算法进行定位, 将定位方程组线性化并采用牛顿迭代法进行求解, 当有 $N(N>5)$ 个测量值时, 测量方程可以表示为<sup>[14]</sup>

$$\mathbf{y} = \mathbf{H}\Delta\mathbf{x} + \boldsymbol{\varepsilon} \quad (3)$$

其中,  $\Delta\mathbf{x} = [\Delta x, \Delta y, \Delta z, c\Delta\delta t_u]^T$ 表示位置偏差与时钟偏差的向量;  $\mathbf{H}$ 为 $N \times 4$ 的雅可比矩阵;  $\boldsymbol{\varepsilon}$ 表示各个卫星的等效测距误差, 不同卫星的测距误差相互独立且服从均值为0, 方差为 $\sigma_{\text{URE}}^2$ 的高斯分布, 该方差表示各部分测量误差方差的总和, 由于在实际中, 接收机通过估算获得 $\sigma_{\text{URE}}^2$ 的值<sup>[14]</sup>, 所以在本文的分析中, 为简化公式的表达, 统一使用 $\sigma_{\text{URE}}^2$ 表示测距误差方差;  $\mathbf{y}$ 是一个 $N$ 维向量, 表示伪距残差。使用最小二乘法进行定位解算求得

$$\Delta\mathbf{x} = (\mathbf{H}^T\mathbf{H})^{-1}\mathbf{H}^T\mathbf{y} \quad (4)$$

牛顿迭代法实现收敛后, 残差的表达式为<sup>[15]</sup>

$$\mathbf{v} = \mathbf{y} - \hat{\mathbf{y}} = \mathbf{y} - \mathbf{H}\Delta\mathbf{x} = \mathbf{Q}\boldsymbol{\varepsilon} \quad (5)$$

其中 $\mathbf{Q} = \mathbf{I} - \mathbf{H}(\mathbf{H}^T\mathbf{H})^{-1}\mathbf{H}^T$ 表示秩为 $(N-4)$ 的幂等矩阵, 检测统计量表达式为

$$\text{SSE} = \mathbf{v}^T\mathbf{v} \quad (6)$$

可作如下假设检验

$$\text{不存在欺骗信号 } \mathcal{H}_0: E(\boldsymbol{\varepsilon}) = \mathbf{0}, \text{SSE}/\sigma_{\text{URE}}^2 \sim \chi^2(N-4) \quad (7)$$

$$\text{存在欺骗信号 } \mathcal{H}_1: E(\boldsymbol{\varepsilon}) \neq \mathbf{0}, \text{SSE}/\sigma_{\text{URE}}^2 \sim \chi^2(N-4, \lambda) \quad (8)$$

通过设定虚警概率求得检测门限, 检测统计量高于检测门限即说明欺骗存在。

### 2.3 基于可信信号的欺骗检测算法

#### 2.3.1 欺骗检测模型

欺骗或故障信号会导致接收机估计的伪距与实

际伪距相比出现大偏差，而可信信号的伪距测量值不会被欺骗，因此本文以可信信号的伪距测量值为基准，建立欺骗检测模型。

接收机在同一历元接收两类导航信号，一类是卫星 $S_A$ 播发的认证信号，一类是卫星 $S_B$ 播发的常规导航信号。在现阶段，地面接收机存在可见 $S_A$ 不足4颗、 $S_B$ 颗数大于等于4颗的情况，此时，接收机采用常规导航信号进行定位解算，得到解算结果为 $[\hat{x}, \hat{y}, \hat{z}, c\hat{\delta}t_u]^T$ ，其中定位结果为 $\hat{\mathbf{x}} = [\hat{x}, \hat{y}, \hat{z}]^T$ ，设可信卫星 $\mathbf{x}^{(m)} = [x^{(m)}, y^{(m)}, z^{(m)}]^T$ 到接收机的几何距离为 $r^{(m)}(\hat{\mathbf{x}}) = \|\mathbf{x}^{(m)} - \hat{\mathbf{x}}\|_2, (m = 1, 2, \dots, M)$ ， $\|\cdot\|_2$ 表示2-范数运算符，以 $M(M < 4)$ 颗 $S_A$ 的伪距测量值为基准，检测量表示为

$$\mathbf{v}_A = \begin{bmatrix} \rho'_c{}^{(1)} - r^{(1)}(\hat{\mathbf{x}}) - c\hat{\delta}t_u \\ \rho'_c{}^{(2)} - r^{(2)}(\hat{\mathbf{x}}) - c\hat{\delta}t_u \\ \dots \\ \rho'_c{}^{(M)} - r^{(M)}(\hat{\mathbf{x}}) - c\hat{\delta}t_u \end{bmatrix} \quad (9)$$

$$\text{SSE}' = \mathbf{v}_A^T \mathbf{v}_A \quad (10)$$

$\rho'_c{}^{(m)} = r^{(m)}(\mathbf{x}_0) + c\delta t_u + \varepsilon_p^{(m)}$ 表示可信卫星 $m$ 校正后的伪距测量值， $\mathbf{x}_0 = [x_0, y_0, z_0]^T$ 表示接收机真实位置， $\delta t_u$ 表示实际的接收机钟差， $\varepsilon_p^{(m)}$ 表示可信卫星测距误差，与上文的 $\varepsilon$ 物理意义相同，服从均值为0、方差为 $\sigma_{\text{URE}}^2$ 的高斯分布。由于采用卫星 $S_B$ 的参数进行定位，则定位结果与 $S_A$ 无关，说明 $\mathbf{v}_A$ 中各元素相互独立、服从高斯分布，且方差与测距误差一致，为 $\sigma_{\text{URE}}^2$ 。需要注意的是，由于在定位时采用最小二乘法进行解算，解算结果是使卫星 $S_B$ 伪距残差平方和最小的值，因此定位解算结果并非精确解，虽然 $\mathbf{v}_A$ 中各元素均值的理论值为0，实际上可能存在小偏差，这里设为 $\lambda_1$ 。可作如下假设检验：

$$\text{不存在欺骗信号 } \mathcal{H}_0 : \text{SSE}' / \sigma_{\text{URE}}^2 \sim \chi^2(M, \lambda_1) \quad (11)$$

$$\text{存在欺骗信号 } \mathcal{H}_1 : \text{SSE}' / \sigma_{\text{URE}}^2 \sim \chi^2(M, \lambda_2) \quad (12)$$

$\lambda_i (i = 1, 2)$ 的表达式为

$$\begin{aligned} \lambda_i &= \sum_{m=1}^M (\mu_m^2 / \sigma_{\text{URE}}^2) \\ &= \sum_{m=1}^M \left( E \left( \rho'_c{}^{(m)} - r^{(m)}(\hat{\mathbf{x}}) - c\hat{\delta}t_u \right)^2 / \sigma_{\text{URE}}^2 \right) \\ &= \sum_{m=1}^M (\Delta d'_m + c\Delta\delta t'_u)^2 / \sigma_{\text{URE}}^2 \end{aligned} \quad (13)$$

其中 $E(\cdot)$ 表示均值函数，对于 $\lambda_2$ ，测距误差的均值

$\mu_m$ 的物理意义为几何距离之差 $\Delta d'_m = \|\mathbf{x}^{(m)} - \mathbf{x}_0\|_2 - \|\mathbf{x}^{(m)} - \hat{\mathbf{x}}\|_2$ 与接收机钟差项被欺骗拉偏的距离 $c\Delta\delta t'_u = c(\delta t_u - \hat{\delta}t_u)$ 之和，几何距离是指可信卫星 $m$ 到接收机实际位置 $\mathbf{x}_0$ 的几何距离与可信卫星 $m$ 到被欺骗定位结果 $\hat{\mathbf{x}}$ 的几何距离。对于 $\lambda_1$ ， $\hat{\mathbf{x}}$ 表示无欺骗存在时接收机定位解算结果， $\Delta\delta t'_u$ 表示接收机钟差误差。

根据统计学理论，假设随机变量 $X_i (i=1, 2, \dots, k)$ ，服从均值为 $\mu_i$ ，方差为 $\sigma^2$ 的高斯分布，且相互独立，则 $\sum_{i=1}^k X_i^2 / \sigma^2$ 服从非中心 $\chi^2(k, \lambda)$ 分布， $\lambda = \sum_{i=1}^k (\mu_i / \sigma)^2$ ， $I_\nu(y)$ 是第1类 $\nu$ 阶贝塞尔函数。非中心卡方分布的概率密度函数表示为

$$f(x; k, \lambda) = \frac{1}{2} e^{-(x+\lambda)/2} \left( \frac{x}{\lambda} \right)^{k/4-1/2} I_{k/2-1}(\sqrt{\lambda x}) \quad (14)$$

则不存在欺骗与存在欺骗的概率密度函数分别表示为 $f(x; M, \lambda_1)$ 和 $f(x; M, \lambda_2)$ ，设虚警概率为 $P_{fa}$ ，得到检测门限 $\text{SSE}'_{\text{th}}$ ，表达式为

$$P_{fa} = \int_{\text{SSE}'_{\text{th}}}^{\infty} f(x; M, \lambda_1) dx \quad (15)$$

当检测统计量大于检测门限时，欺骗存在。综上，基于可信信号的导航终端欺骗干扰检测算法流程如下：

(1)根据接收机以往无欺骗状况下的定位情况，统计 $\text{SSE}'$ 的值，并估计当前可信卫星的等效测距误差方差，拟合得到 $\lambda_1$ 的值；

(2)根据用户需求设定虚警概率 $P_{fa}$ ，并通过式(15)计算检测门限 $\text{SSE}'_{\text{th}}$ ；

(3)根据式(9)和式(10)计算当前历元的检测统计量，与 $\text{SSE}'_{\text{th}}$ 进行对比，大于该值则输出欺骗存在，反之输出无欺骗存在。

本文将欺骗信号检测概率 $P_d$ 作为衡量算法欺骗检测性能的指标。表示为

$$P_d = \int_{\text{SSE}'_{\text{th}}}^{\infty} f(x; M, \lambda_2) dx \quad (16)$$

由表达式可知，影响本算法性能的因素主要为 $P_{fa}$ ， $\sigma_{\text{URE}}^2$ ， $M$ ，欺骗存在时可信卫星到接收机实际位置的几何距离与卫星到被欺骗定位结果的几何距离之差的平方和(下文简称差的平方和)，即 $\Delta d'^2 = \sum_{m=1}^M \Delta d'_m{}^2$ ，以及接收机钟差欺骗导致的偏差 $\Delta\delta t'_u$ 。欺骗检测概率的函数可以表示为

$$P_d = f_{P_d}(P_{fa}, \sigma_{\text{URE}}^2, M, \Delta d'^2, \Delta\delta t'_u) \quad (17)$$

### 2.3.2 欺骗检测性能分析

本节分别对算法的5个影响因素进行分析。

(1)虚警概率与欺骗检测概率的关系:由式(15)可知,当其他影响因素保持不变时,无欺骗和有欺骗存在的概率密度保持不变,随着虚警概率的提高,欺骗检测门限降低,欺骗信号检测概率提高。

(2)用户等效测距误差与欺骗信号检测概率的关系:第2节采用 $\sigma_{\text{URE}}^2$ 表示用户等效测距误差的方差,包含地面监控部分产生的卫星星历和卫星钟差模型、大气延时以及接收机和多路径等对测距的影响,该值由接收机根据电文、接收机环路等信息估算得到,具体的估算过程本文不作讨论,主要关注测距误差方差(标准差)的大小对信号检测概率的影响。

根据理论分析可知,在无欺骗存在和有欺骗存在时,检测统计量均对其方差作归一化处理,区别在于卡方分布的参数 $\lambda$ 的理论值不同,无欺骗存在时, $\lambda_1$ 的理论值为0,不受 $\sigma_{\text{URE}}^2$ 的影响,因此当设定其他影响因素不变时,无欺骗情况对应的概率密度函数保持不变;而存在欺骗信号时, $\lambda_2$ 与 $\sigma_{\text{URE}}^2$ 有关,随着 $\sigma_{\text{URE}}^2$ 的增大, $\lambda_2$ 的值逐渐减小,从而导致欺骗检测概率降低。

(3)可信卫星数目与欺骗信号检测概率的关系:可信卫星数目和相对位置不是相互独立的两个因素,无法单独进行分析,后文将通过仿真来研究。

(4)相对位置、接收机钟差欺骗与欺骗信号检测概率的关系:根据上文的分析,物理量 $\Delta d^2$ 反映了接收机真实位置、可信卫星以及被欺骗的定位结果之间的相对位置关系,体现在参数 $\lambda_2$ 的取值上, $\lambda_2$ 与 $\Delta d^2$ 成正比,而本算法的欺骗检测概率与 $\lambda_2$ 成正比,因此欺骗检测概率与 $\Delta d^2$ 成正比。

值得注意的是,当定位结果精确 $\lambda_2 = \lambda_1 = 0$ 时,式(11)和式(12)概率分布函数相同,本算法将无法进行欺骗检测。此时,式(13)为四元二次方程组,由于可信卫星数不足4颗,该方程组不满秩,存在多解,除了接收机真实位置与钟差外,若欺骗方将定位解算结果设置在其余解的位置,本算法无法进行欺骗检测,定义这些区域为算法的检测盲区。

为减小检测盲区带来的影响,并进一步研究相对位置与钟差欺骗分别对欺骗检测概率的影响,本文主要讨论两种应用场景。

场景1:对于位置已知、进行钟差解算的授时型接收机,式(13)简化为

$$\lambda_2 = \left( \sum_{m=1}^M (c\Delta\delta t'_u)^2 \right) / \sigma_{\text{URE}}^2 = Mc^2\Delta\delta t'_u{}^2 / \sigma_{\text{URE}}^2 \quad (18)$$

此时,仅需要1颗可信卫星即可实现欺骗检测,本算法在此应用场景下不存在检测盲区。 $\lambda_2$ 与 $|\Delta\delta t'_u|$ 成正比。假设无欺骗存在时,定位授时结果精确,则 $\lambda_1 = 0$ ,设定欺骗检测概率低于0.9为本算法无法实现欺骗检测的性能指标,则不同可信卫星数目下,可检测出的接收机钟差欺骗距离的理论值如表1所示,理想情况下本算法可实现检测精度为 $10^{-7}$  s量级以上的时间欺骗。

场景2:当接收机采用频率稳定度较高的晶振,其钟差稳定在一定范围内,此时可以基于晶振的钟差外推结果进行辅助,此时式(13)简化为

$$\lambda_2 = \left( \sum_{m=1}^M (\Delta d'_m + c\Delta\delta t_u)^2 \right) / \sigma_{\text{URE}}^2 = 0 \quad (19)$$

$\Delta\delta t_u$ 表示接收机钟差外推导致的误差。此时该方程组为三元二次方程组,当可信卫星数 $M=1$ ,方程组不满秩,检测盲区为以可信卫星为球心、接收机到可信卫星的距离为半径的球面; $M=2$ 时,方程组不满秩,检测盲区为两个球面的交集,为整个圆周,当接收机真实位置与两颗可信卫星共线时,两球面相切,此时不存在算法检测盲区,切点为接收机真实位置; $M=3$ 时,当3颗可信卫星共线,算法检测盲区与两颗可信卫星存在时的盲区相同,增加的第3颗可信卫星不提供增益,当3颗可信卫星不共线,则可能存在一处检测盲区或不存在,说明卫星构型会影响本算法的检测性能,后文将进一步对本场景下的检测盲区进行验证。

### 3 仿真实验

本节以低轨卫星与北斗中高轨混合星座为应用背景,使用STK软件进行星座仿真。具体参数如表2所示,在观测时段内,接收机在5个位置的低轨卫星可见数目均小于4颗。

为了使仿真结果更具普遍性,本文引入平均欺骗检测概率 $\bar{P}_d$ 这一物理量,定义为

$$\bar{P}_d = \frac{1}{K} \sum_{i=1}^K P_d^{(i)} \quad (20)$$

$P_d^{(i)}$ 表示相同可信卫星数目下第 $i$ 组仿真得到的欺骗信号检测概率, $K$ 表示该场景下总的仿真组数。

表1 只存在时间欺骗时,不同可信卫星数目下,算法可检测出的接收机钟差欺骗距离的理论值(s)

可信卫星数目 $M$	1	2	3
算法可检测出的接收机钟差欺骗	$\geq 7.7 \times 10^{-8}$	$\geq 5.9 \times 10^{-8}$	$\geq 5.0 \times 10^{-8}$

后文将分别针对两种欺骗场景进行仿真。由于在实际中，接收机定位偏差和攻击方设计的欺骗位置是未知的， $\lambda_1$ 和 $\lambda_2$ 的值无法确定。因此，本节通过蒙特卡罗仿真统计得到检测量在存在欺骗和不存在欺骗时的概率密度曲线，设定虚警概率，计算检测门限和欺骗信号检测概率，为保证欺骗存在时的定位结果为设定的位置，假设欺骗存在时每颗可见的北斗中高轨卫星均为欺骗源。

同时，为得到较为普遍的结论，本文通过以下方法近似实现对相对位置的遍历：选取5个不同位置的接收机进行观测；针对每一个位置的接收机，在观测时段内，以10 min为观测间隔，对可信低轨卫星和北斗卫星的可见性进行记录并分析；对于位置欺骗场景，针对每一个接收机，假设被欺骗的定位结果与接收机真实位置的距离为 $r$  m，以接收机真实位置为圆心， $r$ 为半径，取圆周上均匀分布的8个点为存在欺骗时的定位结果。

### 3.1 时间欺骗场景

#### (1) 场景设置

接收机已知自身坐标，只进行钟差解算。

#### (2) 欺骗信号检测概率分析

欺骗方实施时间欺骗，使用表2的仿真参数，研究接收机在此场景下采用本算法进行欺骗检测的性能。本节分别对5个位置的接收机在144个历元实施时间欺骗进行仿真，每个历元的蒙特卡罗仿真次数为1000次，设定 $P_{fa} = 0.01$ ，根据文献[14]，用户测距误差标准差大致等于 $\sigma_{URE} = 5.9$  m，对于每个 $\Delta\delta t_n$ 的取值均得到562个欺骗检测概率仿真结果，其中可信卫星数为1颗、2颗或3颗的仿真结果分别为144, 377, 41个，即根据式(20)对于不同数量可信卫星，仿真组数 $K$ 的取值为144, 377和41，将相应可信卫星数目的仿真结果和 $K$ 值代入式(20)求得平均欺骗检测概率。如图1所示，对接收机的钟差拉偏100 ns以上时，可实现检测概率高于0.9的欺骗检测，且本算法在不同可信卫星数条件下的检

测性能相近，此时使用一颗可信卫星即可实现欺骗检测。

### 3.2 位置欺骗场景

#### (1) 场景设置

接收机采用频率稳定度较高的晶振，在计算检测统计量时将标称钟差值作为 $\delta t_n$ 代入公式，此时，接收机只关注位置欺骗。

#### (2) 欺骗信号检测概率分析

##### (a) 钟差外推精度对欺骗信号检测概率的影响

本节选择位于北京的接收机进行仿真，并选择观测时段内可信卫星数为2颗的历元，共74个，则对于每个 $\Delta\delta t_n$ 取值的仿真组数 $K=74$ 。设 $P_{fa} = 0.01$ ，用户测距误差标准差为 $\sigma_{URE} = 5.9$  m，欺骗拉偏的距离为50 m，对每一历元的每个 $\Delta\delta t_n$ 均进行 $10^3$ 次蒙特卡罗仿真，统计并计算得到观测时段内接收机平均欺骗检测概率与钟差外推精度 $\Delta\delta t_n$ 的关系曲线图。如图2所示，当钟差外推精度优于10 ns时，钟差外推精度基本不影响本算法的欺骗信号检测概率。根据文献[16]，采用恒温晶振的接收机在2 h内钟差变化的量级低于 $10^{-9}$  s，采用温补晶振的接收机在50 s内钟差变化量级低于 $10^{-8}$  s。此类接收机采用钟差外推的方式，可认为在短小时内不影响算法的欺骗检测性能。

##### (b) 虚警概率与欺骗信号检测概率的关系

图3为观测时段内5个观测站统计得到的不同数目安全认证信号的检测性能曲线，设欺骗信号存在时定位结果为以接收机实际位置为圆心，半径为 $r=50$  m的圆周上均匀分布的8个点，统计得到可信卫星为1颗、2颗和3颗的仿真组数 $K$ 分别为1152, 3016和328，每组仿真均进行 $10^4$ 次，得到无欺骗和有欺骗存在的检测统计量分布曲线，根据不同虚警概率计算欺骗检测概率，并根据式(20)得到平均欺骗检测概率，仿真结果与理论分析保持一致。

##### (c) 用户测距误差与欺骗信号检测概率的关系

本节首先验证在无欺骗存在时， $\sigma_{URE}^2$ 对检测统

表2 仿真场景参数

参数	描述
仿真时段	2023年9月2日16:00-2023年9月3日16:00，观测时间间隔为10 min，观测历元共144个
北斗星座	本文采用北斗三号卫星星座，包括：24颗MEO卫星，Walker24/3/1星座，卫星轨道高度为21 528 km，轨道倾角为55°；3颗GEO卫星，轨道高度为35 786 km，分别定位于东经80°、110.5°、140°；3颗IGSO卫星，轨道高度35 786 km，轨道倾角55°，相位间隔120°
低轨星座	卫星播发认证信号，为近极地星座，为Walker类型，共有60颗卫星，6个轨道面，相位因子为1，轨道高度为1 175 km，轨道倾角为86.5°
接收机位置	随机选择国内5个城市作为接收机所在位置(地心地固坐标)，包括：哈尔滨(-2661.32,3576.94,4546.01) km、北京(-2176.85,4387.47,4071.96) km、兰州(-1231.5014.65,3736.14) km、成都(-1334.67,5326.66,3234.39) km、海口(-2083.66,5620.29,2172.46) km
接收机天线	最低仰角为15°

计量分布的影响是否与理论分析一致，之后结合存在欺骗的场景，分析欺骗信号检测概率的变化情况。

选定2023年9月2日18:30, 16:20和16:30为观测时刻，位于北京的接收机可见低轨卫星数分别为1颗、2颗和3颗，北斗可见卫星数分别为9颗、10颗和10颗，设定虚警概率为0.01，接收机采用单点定位算法进行定位，在仿真中分别设定 $\sigma_{URE} = 1\text{ m}$ ,  $\sigma_{URE} = 5.9\text{ m}$ ,  $\sigma_{URE} = 10\text{ m}$ 对应用户测距误差方差偏小、正常和偏大的情况，蒙特卡罗仿真次数为 $10^4$ 次，得到3个观测时刻定位精度统计结果，这里的定位精度是指定位结果与接收机真实位置的几何

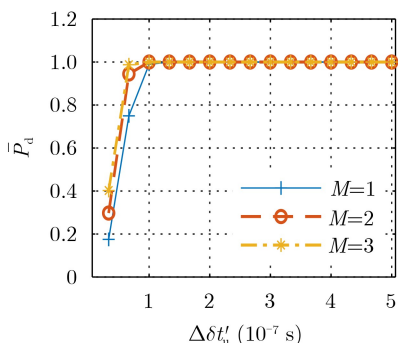


图1 不同可信卫星数目下时间欺骗导致的伪距拉偏距离与平均欺骗检测概率的关系曲线

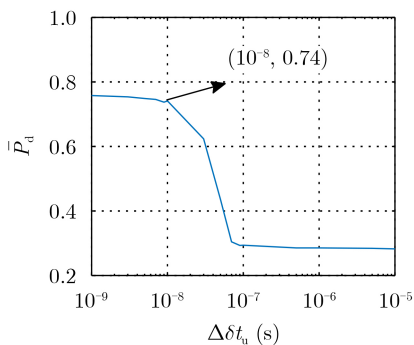


图2 M=2时接收机钟差变化量对算法检测性能的影响曲线

距离，如图4和图5所示，仿真中用于定位的常规导航信号数目对定位精度的影响很小，随着用户测距误差方差的增大，接收机定位精度降低，在3种用户测距误差方差的取值下，仿真得到的平均定位误差分别约为1.4 m, 8.3 m, 14.1 m，但检测统计量的分布基本保持不变，说明在无欺骗信号存在的场景下，用户测距误差造成的定位偏差不会影响检测统计量的分布。

当存在欺骗时，设置虚警概率为0.01，对不同位置接收机以及不同欺骗位置进行仿真，欺骗导致的定位偏差为50 m，每组蒙特卡罗仿真次数为 $10^3$ 次，平均欺骗检测概率计算方法与3.2节(b)相同，得到图6所示的不同可信信号数目下伪距测量误差标准差与平均检测概率的关系图，可知随着伪距测量误差标准差的增大，平均欺骗检测概率逐渐降低。

(d)可信卫星数目与欺骗信号检测概率的关系

本节在探讨不同数目可信卫星对欺骗信号检测概率的影响时，遍历可信卫星数目相同的历元，得到图7，该图表示欺骗导致的定位偏差为r m时平均欺骗检测概率的大小。仿真设定 $P_{fa} = 0.01$ 、每个历元的蒙特卡罗仿真次数为 $10^3$ 次、用户测距误差标准差为 $\sigma_{URE} = 5.9\text{ m}$ ，平均欺骗检测概率的计

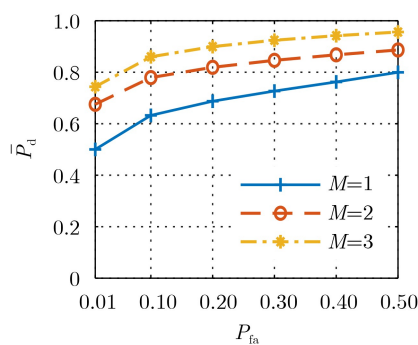
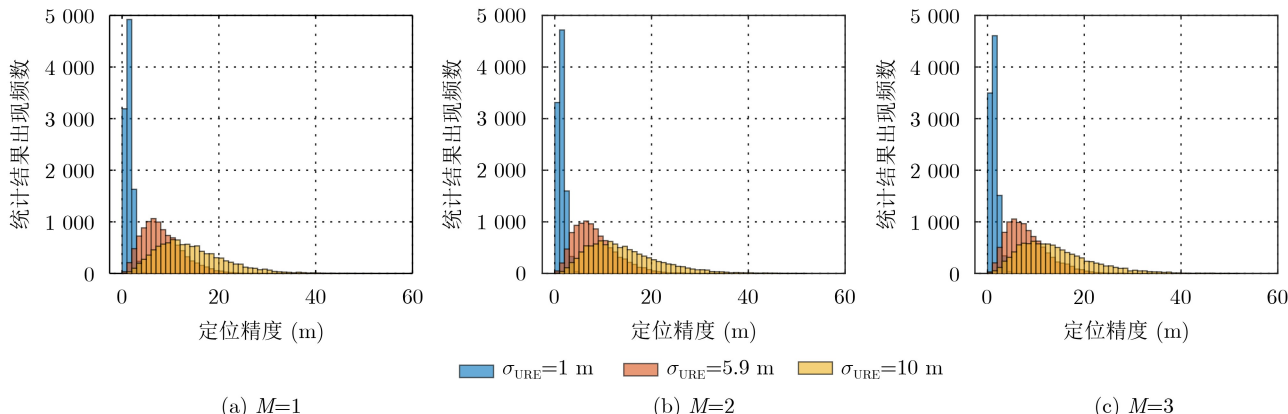


图3 不同安全认证信号数目的检测性能



(a) M=1 (b) M=2 (c) M=3

图4 观测时刻不同用户测距误差的标准差与不同可信卫星数目单点定位精度统计结果对比图

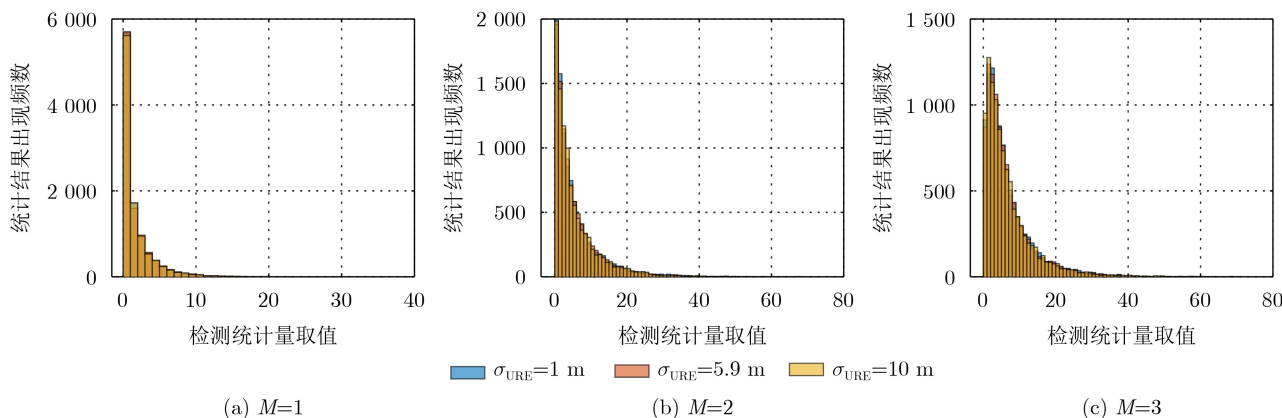


图5 不同卫星数目观测时刻检测统计量取值统计结果对比图

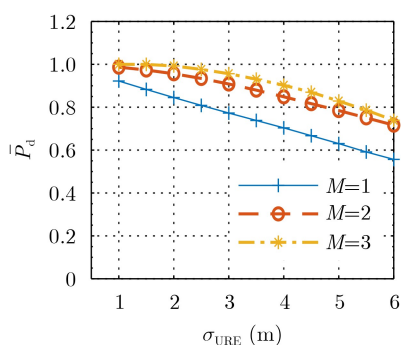


图6 伪距测量误差标准差与平均欺骗检测概率的关系

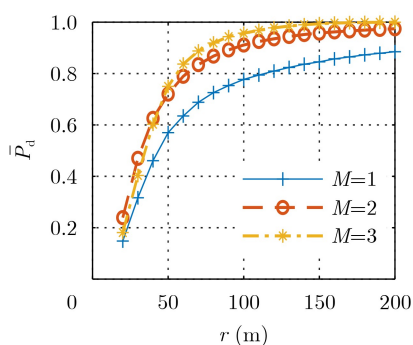


图7 欺骗导致的定位偏差r与平均欺骗检测概率之间的关系曲线

算参数与3.2节(b)相同，不再赘述。由统计结果可知，平均欺骗检测概率与可信卫星数目之间的关系可以分为两部分。 $r < 50 \text{ m}$ 时，欺骗拉偏距离较小，可信卫星数目的增加不会为算法的性能带来显著提升； $r \geq 50 \text{ m}$ 时，算法的欺骗检测性能随可信卫星数目增多而增大。当欺骗导致的定位偏差为100 m时，本算法在可见3颗可信卫星时的平均欺骗检测概率可达0.96。可见本算法在接收机定位精度约为10 m量级时，对低于50 m的小偏差位置欺骗检测能力较弱，对大偏差位置欺骗检测效果显著，随着可信卫星数目的增多而增大。

(e) 相对位置与欺骗信号检测概率的关系

本文采用 $\Delta d^2$ 表征可信卫星、接收机真实位置、被欺骗的定位结果之间的相对位置关系。本节以位于北京的接收机为例，设 $r=50 \text{ m}$ ，以接收机真实位置为圆心， $r$ 为半径，在与该接收机同一 $x-y$ 平面作圆(地心地固坐标系下)，以 $x$ 轴为参考逆时针旋转 $\theta^\circ$ ，每 $6^\circ$ 取一点作为被欺骗后的定位结果，共60个位置，设用户测距误差标准差为5.9 m，虚警概率设定为0.01，选择2023年9月2日16:00为观测时刻，接收机可见低轨卫星数为2颗。

如图8，虽然 $r$ 的量级远小于可信卫星到接收机距离的量级，但是 $\Delta d^2$ 的变化很明显。由于在仿真

中，接收机存在定位误差，欺骗位置未知， $\lambda_1$ 和 $\lambda_2$ 属于未知量。为验证理论的正确性，本节通过拟合得到仿真场景下 $\lambda_1 \approx 3$ ，通过设定被欺骗的定位结果计算 $\Delta d^2$ ，将计算结果代入公式计算 $\lambda_2$ 的值，设虚警概率为0.01，从而得到欺骗检测概率的理论结果，如图8(a)，仿真结果与理论值保持一致。欺骗信号检测概率与 $\Delta d^2$ 成正比。对于不同位置的接收机，该结论依然成立，本节不再展示其他位置接收机的仿真结果。

下面讨论算法的欺骗检测盲区。由于低轨卫星轨道高度为 $10^6 \text{ m}$ 量级，为找到检测盲区所在位置需要遍历大量3维位置坐标，若采用表2的仿真参数，计算复杂度过高，因此本节假设地心地固坐标系下的卫星位置与接收机位置，通过理论计算得到不同位置的欺骗检测概率，设检测概率低于0.1的位置位于检测盲区， $P_{fa} = 0.01$ ， $\sigma_{URE} = 5.9 \text{ m}$ ，得到图9所示的算法检测盲区分布图。

图中三角形表示可信卫星所在位置，“\*”表示接收机所在位置，“.”表示算法检测盲区，结果与上文的理论分析保持一致。对于接收方，可信卫星数目为3颗时，算法的检测结果可靠性最高，但仍然存在一定模糊度，可以通过判断定位结果的合理性，进一步判断欺骗信号的存在性。

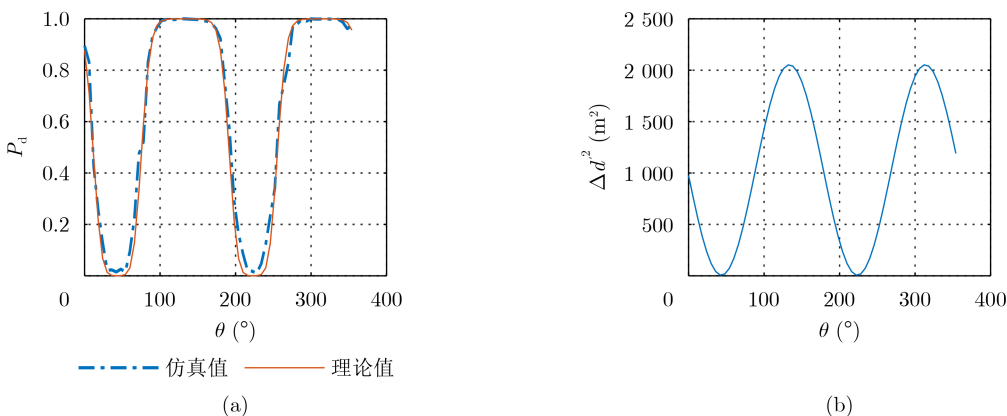


图8  $\Delta d^2$ 与欺骗信号检测概率之间的曲线对比图(接收机位于北京,  $r=50$  m,  $P_{fa}=0.01$ ,  $\sigma_{URE}=5.9$  m)

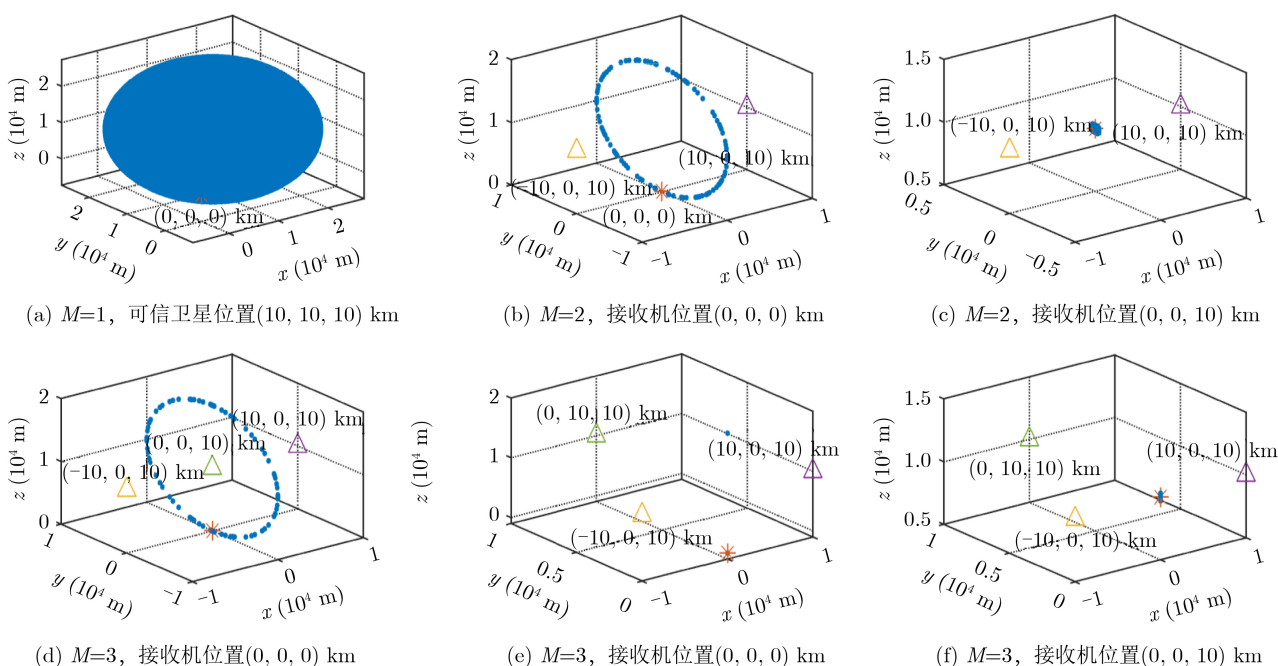


图9 算法检测盲区理论计算分布图

### 4 结束语

针对接收机同时接收常规导航信号和可信信号的场景, 其中常规导航信号覆盖重数高于4重, 可信信号覆盖重数低于4重, 本文提出终端利用部分可信信号实现欺骗检测的方法。该方法采用常规信号进行定位解算, 以可信信号为基准, 通过比较伪距残差平方和与阈值来判断是否存在欺骗信号。

经过理论与仿真分析可以得到如下结论:

(1) 导航终端接收不同数目的可信卫星信号均可实现欺骗检测, 随着可信卫星数目的提高, 平均欺骗检测概率提高, 检测性能趋于稳定, 本算法在欺骗导致的定位偏差为100 m、用户定位精度约10 m、接收机可见3颗可信卫星的条件下, 算法的平均欺骗检测概率为0.96, 且在相同条件下该算法对高于 $10^{-8}$  s量级的钟差外推精度不敏感;

(2) 本算法存在性能恶化的欺骗检测盲区, 盲区的面积大小随可信卫星的增多呈减小趋势, 但即使存在超过4颗可信卫星也不一定保证完全消除检测盲区, 这与卫星构型有关。

本文主要探讨接收机在单历元的欺骗信号检测方法, 后续还将继续研究如何利用可信信号实现多历元的欺骗检测, 并针对在未来可见多颗可信卫星场景下的卫星选取问题进一步开展研究。

### 参考文献

[1] CARROLL J V, VAN DYKE K, KRAEMER J H, *et al*. Vulnerability assessment of the U. S. transportation infrastructure that relies on GPS[C]. Proceedings of the 14th International Technical Meeting of the Satellite Division of the Institute of Navigation, Salt Lake City, USA, 2001: 975-981.

- [2] WU Zhijun, ZHANG Yun, YANG Yiming, *et al.* Spoofing and anti-spoofing technologies of global navigation satellite system: A survey[J]. *IEEE Access*, 2020, 8: 165444–165496. doi: [10.1109/ACCESS.2020.3022294](https://doi.org/10.1109/ACCESS.2020.3022294).
- [3] YUAN Muzi, TANG Xiaomei, and OU Gang. Authenticating GNSS civilian signals: A survey[J]. *Satellite Navigation*, 2023, 4(1): 6. doi: [10.1186/s43020-023-00094-6](https://doi.org/10.1186/s43020-023-00094-6).
- [4] NICOLA M, MOTELLA B, PINI M, *et al.* Galileo OSNMA public observation phase: Signal testing and validation[J]. *IEEE Access*, 2022, 10: 27960–27969. doi: [10.1109/ACCESS.2022.3157337](https://doi.org/10.1109/ACCESS.2022.3157337).
- [5] FERNÁNDEZ I, RIJMEN V, ASHUR T, *et al.* Galileo navigation message authentication specification for signal-in-space testing - v1.0[R]. European Commission, 2016.
- [6] ANDERSON J M, CARROLL K L, DEVILBISS N P, *et al.* Chips-message robust authentication (chimera) for GPS civilian signals[C]. Proceedings of the 30th International Technical Meeting of the Satellite Division of the Institute of Navigation, Portland, USA, 2017: 2388–2416. doi: [10.33012/2017.15206](https://doi.org/10.33012/2017.15206).
- [7] CHAPMAN D C. Chips message robust authentication (chimera) enhancement for the L1C signal: Space segment/user segment interface[R]. IS-AGT-100, 2019.
- [8] MANANDHAR D and SHIBASAKI R. Signal authentication for anti-spoofing based on L1S[C]. Proceedings of the ION 2017 Pacific PNT Meeting, Honolulu, USA, 2017: 938–947. doi: [10.33012/2017.15029](https://doi.org/10.33012/2017.15029).
- [9] MANANDHAR D and SHIBASAKI R. Authenticating GALILEO open signal using QZSS signal[C]. Proceedings of the 31st International Technical Meeting of the Satellite Division of the Institute of Navigation, Miami, USA, 2018: 3995–4003. doi: [10.33012/2018.15872](https://doi.org/10.33012/2018.15872).
- [10] 王磊, 李德仁, 陈锐志, 等. 低轨卫星导航增强技术——机遇与挑战[J]. *中国工程科学*, 2020, 22(2): 144–152. doi: [10.15302/J-SSCAE-2020.02.018](https://doi.org/10.15302/J-SSCAE-2020.02.018).  
WANG Lei, LI Deren, CHEN Ruizhi, *et al.* Low earth orbiter (LEO) navigation augmentation: Opportunities and challenges[J]. *Strategic Study of CAE*, 2020, 22(2): 144–152. doi: [10.15302/J-SSCAE-2020.02.018](https://doi.org/10.15302/J-SSCAE-2020.02.018).
- [11] SUN Tianyu, HU Min, and YUN Chaoming. Low-orbit large-scale communication satellite constellation configuration performance assessment[J]. *International Journal of Aerospace Engineering*, 2022, 2022: 4918912. doi: [10.1155/2022/4918912](https://doi.org/10.1155/2022/4918912).
- [12] S·柳辛. 使用PVT解估算来检测和消除GNSS欺骗信号[P]. 中国, 110114695A, 2019.  
S·LIUXIN. Detection and elimination of GNSS spoofing signals with PVT solution estimation[P]. CN, 110114695A, 2019.
- [13] 张超, 吕志伟, 张伦东, 等. 欺骗干扰对GNSS/INS系统定位性能的影响[J]. *导航定位学报*, 2022, 10(4): 20–28. doi: [10.3969/j.issn.2095-4999.2022.04.003](https://doi.org/10.3969/j.issn.2095-4999.2022.04.003).  
ZHANG Cao, LYU Zhiwei, ZHANG Lundong, *et al.* Influence analysis of spoofing interference on positioning performance of GNSS/INS system[J]. *Journal of Navigation and Positioning*, 2022, 10(4): 20–28. doi: [10.3969/j.issn.2095-4999.2022.04.003](https://doi.org/10.3969/j.issn.2095-4999.2022.04.003).
- [14] 谢钢. GPS原理与接收机设计[M]. 北京: 电子工业出版社, 2009.  
XIE G. Principles of GPS and Receiver Design[M]. Beijing: Publishing House of Electronics Industry, 2009.
- [15] PARKINSON B W and AXELRAD P. Autonomous GPS integrity monitoring using the pseudorange residual[J]. *Navigation*, 1988, 35(2): 255–274. doi: [10.1002/j.2161-4296.1988.tb00955.x](https://doi.org/10.1002/j.2161-4296.1988.tb00955.x).
- [16] FU Dong, PENG Jing, GONG Hang, *et al.* Impact analysis of meaconing attack on timing receiver[M]. YANG Changfeng and XIE Jun. China Satellite Navigation Conference (CSNC 2021) Proceedings. Singapore: Springer, 2021: 423–434. doi: [10.1007/978-981-16-3146-7\\_39](https://doi.org/10.1007/978-981-16-3146-7_39).
- 王环宇: 女, 博士生, 研究方向为卫星导航信号认证.  
林红磊: 男, 副研究员, 研究方向为卫星导航系统与信号处理.  
欧 钢: 男, 教授, 研究方向为卫星导航定位、综合导航定位授时.  
唐小妹: 女, 研究员, 研究方向为导航信号体制设计、导航安全对抗等.

责任编辑: 陈 倩