中国科学院大学
University of Chinese Academy of Sciences

研究生学位论文开题报告

报告题目 基于多天线的 GNSS 反欺骗技术研究

学生姓名 陈佳佳 学号 201918017227001

指导教师 袁洪 职称 研究员

学位类别 工学博士

学科专业 信号与信息处理

研究方向 卫星导航增强技术

研究所（院系） 空天信息创新研究院

填表日期 2020 年 11 月 16 日

中国科学院大学制

填 表 说 明

1. 本表内容须真实、完整、准确。
2. “学位类别”名称：学术型学位填写哲学博士、教育学博士、理学博士、工学博士、农学博士、医学博士、管理学博士，哲学硕士、经济学硕士、法学硕士、教育学硕士、文学硕士、理学硕士、工学硕士、农学硕士、医学硕士、管理学硕士等；专业学位填写工程博士、工程硕士、工商管理硕士（MBA）、应用统计硕士、翻译硕士、应用心理硕士、农业推广硕士、工程管理硕士、药学硕士等。
3. “学科专业”名称：学术型学位填写“二级学科”全称；专业学位填写“培养领域”全称。

目　录

目　录 1
1. 选题的背景及意义 1
2. 国内外本学科领域的发展现状与趋势 2
2.1 欺骗式干扰识别 2
2.2 欺骗式干扰抑制 3
3. 课题主要研究内容和预期目标 4
3.1 主要研究内容 4
3.2 预期目标 5
4. 拟采用的研究方法、技术路线、实验方案及其可行性分析 6
4.1 研究方法与技术路线 6
4.1.1 使用双天线的欺骗检测算法 6
4.1.2 基线向量估计算法 11
4.1.3 使用三天线的欺骗检测算法 13
4.2 实验方案 15
4.2.1 虚警率测试实验方案 15
4.2.2 静态性能实验方案 17
4.2.3 动态性能实验方案 19
4.3 可行性分析 22
5. 已有科研基础与所需的科研条件 22
5.1 已有的科研基础 22
5.2 所需科研条件 23
6. 研究工作计划与进度安排 23
7. 参考文献 23

1. 选题的背景及意义

全球导航卫星系统（Global Navigation Satellite System, GNSS）能够为全球用户提供不间断的高精准导航定位服务，已成为直接关系到国计民生的关键性技术支撑系统和基础设施[1,2]。GNSS 技术已经广泛应用于位置服务、气象预报、交通运输、系统授时、应急救援和军事等众多领域[3,4]。由于 GNSS 的极端重要性，世界范围内的众多国家均在积极组建自己的卫星导航系统。当前已经在商用的全球导航系统包括：GPS（美国）、GLONASS（俄罗斯）、Galileo（欧盟）和北斗卫星导航系统（中国）[5-7]。卫星导航系统由于其自身的脆弱性，非常容易受到干扰和攻击。针对卫星导航系统的可靠性问题，已经得到国内外机构的广泛关注[8,9]。

当前针对卫星导航系统的攻击方式主要分为压制式干扰和欺骗式干扰两类。压制式干扰是利用大功率压制干扰机发射单频、扫频、伪码等压制信号使得目标接收机无法正常工作。GNSS 卫星通常位于两万公里的高空，其导航信号到达地表附近时已经非常微弱（比接收机热噪声电平低 20dB 左右）。当接收机接收到干扰信号时，干扰信号的电平极易超过接收机处理增益所允许的信号电平，从而使卫星信号不能从噪声中提取出来，最终导致定位精度下降或者跟踪环路失锁，甚至不能正常捕获到卫星。距研究表明，只要使用功率为 1W 的发射机，就能对 100KM 范围的 GNSS 接收机造成干扰[10,11]。

欺骗式干扰通过转发或产生的形式伪造与真实卫星信号结构相同的信号作为干扰信号，利用其良好的隐蔽性特点诱导接收机接收欺骗信号，使接收机误认为这些信号是由卫星发射而来，对其进行捕获与跟踪，并可获得与卫星信号相似的增益[12]。其首要目标是在隐蔽的条件下使得 GNSS 终端得到虚假的时间、位置、速度等信息，达到欺骗目的。相比之下，压制干扰将导致无法定位，而欺骗干扰将导致用户接收到虚假的时间、位置信息，带来不可信时空信息服务。

从某种程度上来讲，欺骗干扰带来的危害比压制干扰更为严重，因而对欺骗攻击的可靠检测显得至关重要。2011 年 12 月，伊朗声称利用 GPS 欺骗干扰技术捕获了一架高度机密的美国无人机。在随后陆续开展的验证性试验中，攻击者成功使用低成本的 GNSS 欺骗设备，引导处于悬停状态的无人机俯冲向地面[13]。另外在 2013 年，美国德克萨斯大学 Humphreys 教授所进行的一个试验中，在游

艇不发出任何警报的前提下，成功诱导满载着乘客的游艇偏离了航线[14]。因此，针对 GNSS 反欺骗的研究显得迫在眉睫。

多天线（也称天线阵）是由多个天线阵元按一定规则排列组成的天线系统，可以实现对信号的空间采样，在通信、广播、雷达、声呐等无线电系统中被广泛应用。阵列信号处理技术作为一种通用技术，在导航对抗领域也发挥着重要作用。近年来一些基于空域特征的欺骗检测和抑制技术被相继提出，多天线技术在 GNSS 反欺骗领域也显示出巨大潜力[15,16]。

综上所述，本课题针对日益复杂的应用环境，开展基于多天线的 GNSS 反欺骗技术研究，可以保障卫星导航系统在各种复杂电磁环境下的安全应用，具有广阔的应用前景和重要的战略意义。

2. 国内外本学科领域的发展现状与趋势

目前，关于反欺骗式干扰的研究可以分为欺骗式干扰的识别和欺骗式干扰的抑制。其中，欺骗式干扰识别的研究占大多数。

2.1 欺骗式干扰识别

欺骗式干扰的识别主要是通过监视接收信号的某些信号特征有无异常变化来判断是否受到欺骗式干扰攻击。美国国家运输系统中心的 Volp 在 2001 年提交给国家运输部的技术报告文件中讨论了基于信号特征识别的欺骗式干扰识别技术，认为可以通过接收信号的信号功率，信号到达时及信号极化方式等信号特征识别欺骗式干扰。但该方法仅仅在报告中被提及，并没有做更深入的研究和界定。Shepard 等人通过大量的实验观察发现，欺骗式干扰为了能够确保有效地误导卫星导航接收机，其功率通常大于真实信号，于是提出了对信号的绝对功率进行监视以判断接收信号是否为欺骗式干扰，但该方法在欺骗信号功率和真实信号功率较为接近时性能会明显下降。加拿大 Calgary 大学的 Jafarnia-Jahromi 等人提出可以通过持续监视信号的载噪比来判断接收机是否受到欺骗式干扰[17]，该方法需要进行长时间的持续观测。Wen 等人提出利用 L1/L2 频率信号之间相对延时来识别欺骗式干扰[18]，但该方法不能应用于低成本的单频接收机。通过检测 GPS 的相关器输出峰值是否存在不正常的不对称来判断接收机是否受到欺骗式干扰是另一种利用接收信号特征的欺骗式干扰识别方法[19-21]。Akos 提出利用接收机跟

踪环路中 AGC（Automatic Gain Control）参数的异常来识别欺骗式干扰[22]，清华大学王强等人通过剩余矢量分析方法对欺骗干扰的识别进行了评估[23]，但这些方法通常只能在欺骗攻击的开始阶段有效，若接收机已经成功被欺骗信号牵引，则该方法可能失效。

除此之外，利用多个天线或者不同位置天线接收信号间的差异是另一类欺骗式干扰的识别方法。Psiaki 等人提出利用移动天线在不同位置接收信号参数的差别来识别欺骗式干扰[24-28]。Swaszek 等人提出利用两个以上接收机的定位结果差异来进行转发式欺骗式干扰的识别[29]。Montgomer，Humphreys 等人提出根据两根固定天线之间的接收信号相位差来识别欺骗式干扰[30]。O'Hanlon 等人提出用未受欺骗式干扰的接收机和可能受欺骗式干扰接收机接收信号中的 P 码信号的相关结果来识别欺骗式干扰[31]。Nielsen 等人提出利用不同天线间的信号相关值异常来识别欺骗式干扰[32]，但这些方法通常基于欺骗信号来自于同一方向的假设，当存在多个欺骗信号源时，这些方法可能会失效。此外，Jafarnia-Jahromi,Lin 论证了组合导航抗欺骗式干扰的可行性[33]，该方法需要惯性导航等辅助单元，硬件成本相对较高。Humphreys 等人对加密认证技术在民用接收机的应用进行了讨论[34-36]，该方法需要对现有的导航信号体制和接收机软硬件进行更改，其实施难度非常巨大。所有上述这些算法研究了欺骗式干扰的识别，并未研究识别出欺骗式干扰后如何保证接收机恢复正常的 PVT（Position Velocity and Time）功能。此外，上述算法都是针对 GPS 进行研究的，并未考虑其它卫星导航系统。

2.2 欺骗式干扰抑制

相对于欺骗式干扰的识别，欺骗式干扰的同时识别与抑制研究相对较少。Moon 等人提出利用更多的跟踪环路跟踪所有可能的欺骗式卫星信号和真实卫星信号，然后根据跟踪参数来区分欺骗式卫星信号和真实卫星信号[37]。Calgary 大学 PLAN 实验室提出了一种基于导向矢量估计的欺骗式干扰抑制方法。该方法将参考天线的接收信号与其余天线的接收信号进行互相关运算，以分别估计出欺骗式干扰导向矢量中每个元素的幅度和相角，利用估计的欺骗式干扰导向矢量构造干扰正交投影矩阵，对欺骗式干扰进行抑制。Konovaltsev 等人对利用天线阵来抑制欺骗式干扰进行了研究，通过利用类波束形成技术和正交投影技术来抑制

单个转发式欺骗干扰[38]，美国 Rockwell Collins 公司的 McDowell 对多天线波束形成和调零技术的理论和性能进行了分析，利用 GPS 相关器参数及跟踪环路参数形成多波束来识别和抑制欺骗式干扰[39]，这些方法需要使用四个以上的天线构成天线阵列，其硬件成本相对较高。Daneshmand 提出了一种低复杂度的基于双天线的欺骗式干扰消除技术，将两根天线的接收信号进行互相关运算得到欺骗式干扰的来向角，进而对欺骗式干扰进行抑制[40]，该方法同样基于欺骗信号来自同一方向的假设。Ledvina 等人提出了一种扩展的 RAIM（Receiver Autonomous Integrity Monitoring）技术，该技术能够检测和排除欺骗式干扰所造成的异常测量值。然而，一方面这些算法仅有初步的结果，系统的分析方面还有待完善；另一方面所有这些算法均是针对 GPS 系统研究的，而对其它卫星导航抗欺骗式干扰的系统研究并未见到。

因此，亟需针对 GNSS 的欺骗式干扰抑制问题做更深入的研究。这不仅在理论研究方面有重要的意义，对于推进全球导航卫星系统在军事应用，民用基础设施建设等领域的应用具有重要的意义。

3. 课题主要研究内容和预期目标

3.1 主要研究内容

（1）使用双天线的 GNSS 欺骗检测方法

传统的双天线欺骗检测方法，通常基于所有欺骗的信号来自于同一方向的假设。由于真实信号来自于不同的方向，当单个天线播发多路欺骗信号时，能够有效检测出欺骗信号。但当只存在单个欺骗信号或是存在来自多个方向的欺骗信号时，该方法不能有效区分欺骗信号和真实信号。

因此本课题的研究内容之一是提出一种新型的使用双天线的 GNSS 欺骗检测方法，拟解决传统双天线欺骗检测方法不能检测来自多个方向欺骗信号问题。该方法拟使用两个低成本商用 GNSS 接收天线构成基线向量，采用载波相位双差法并联合星历数据进行基线向量解算，并使用已知的基线长度对解算出的基线向量进行修正，将修正后的值作为基线向量真实值的近似。对基线向量进行标准化后，使用用误差平方和（*SSE*）检验统计量来评估是否存在欺骗信号。

（2）使用三天线的 GNSS 欺骗检测方法

在阵列天线姿态已知的前提下，可以通过星历信息中的卫星位置和天线的几何结构确定真实信号在天线坐标系中的理论入射方向。若某一导航信号的到达角估计结果和这一理论值不符，则说明存在欺骗干扰信号。此种方法只需要欺骗信号与真实信号来向不同即可成立，适用范围最广。但是，该方法往往需要引入高复杂度的阵列校准技术来保证到达角的估计精度，而且需要惯导等辅助设备测量阵列姿态，具有非常高的硬件成本和实现难度。

本课题的研究内容之一是提出一种使用三天线的 GNSS 欺骗检测方法，该方法不需要惯导等辅助设备来确定天线的姿态，因此其成本和硬件复杂度相对降低。该方法通过计算三个天线构成的基线向量来确定天线的姿态信息，进而通过卫星信号入射方向与星历信息是否一致来判断是否存在欺骗信号。

（3）GNSS 多天线接收机软件化实验平台的设计与实现

干扰检测和抑制方法在应用到实际系统前，还需在真实数据中进行验证。因此，本课题的研究内容之一是基于实验室现有硬件设施和软件设施，设计并实现一套多功能 GNSS 多天线接收机实验平台，该平台由 GNSS 信号模拟器、GNSS 信号转发器、软件无线电设备、GNSS 信号处理软件等部分构建而成，为所提出算法的实际验证提供条件。

3.2 预期目标

针对以上研究内容，本研究课题的预期目标具体如下：

(1) 根据载波相位双差观测方程和基线长度，提出基线向量的估算方法；

(2) 提出双天线欺骗检测算法的理论分布模型；

(3) 搭建双天线欺骗检测系统测试环境和平台；

(4) 验证静态和动态环境下，双天线欺骗检测系统的检测性能；

(5) 依据双矢量定姿法，提出三天线的姿态估计方法；

(6) 提出三天线欺骗检测系统的卫星信号来向估计方法；

(7) 提出三天线欺骗检测系统的理论分布模型；

(8) 搭建三天线欺骗检测系统测试环境和平台；

(9) 验证静态和动态环境下三天线欺骗检测系统的检测性能。

4. 拟采用的研究方法、技术路线、实验方案及其可行性分析

4.1 研究方法与技术路线

4.1.1 使用双天线的欺骗检测算法

图 4.1 显示了由两个 GNSS 天线，两个 GNSS 接收器和一个信号处理单元组成的双天线欺骗检测系统示意图。基线矢量 b_{BA} 由连接到公共振荡器的两个 GNSS 天线构成。我们使用相同型号和批次的天线，以尽可能消除天线相位中心不一致引起的误差。基线向量的长度很容易获得，在本课题中认为是已知的。信号处理单元的输入是两个天线接收到的所有跟踪信号的载波相位和星历等观测数据。信号处理单元的输出是实时欺骗检测结果。

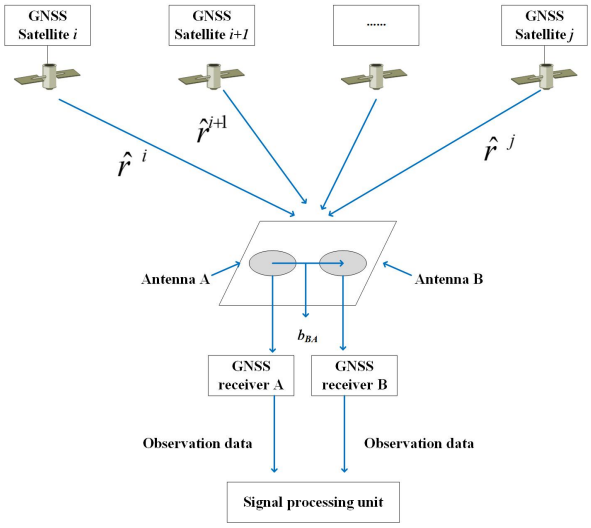


图 4.1 双天线欺骗检测系统结构示意图

对于该系统而言，由于基线长度很短（通常小于 10λ），因此其电离层和对流层误差可以认为完全相等，载波相位单差观测方程可以描述为：

$$\begin{aligned}\Delta\tilde{\varphi}^{i}_{BA}\lambda &= \varphi^{i}_{B}\lambda - \varphi^{i}_{A}\lambda \\ &= \Delta\rho^{i}_{BA} + c\cdot V_{ij} + \Delta N^{i}_{BA}\lambda + n^{i}_{rBA}\lambda \\ &= (\hat{r}^{\,i})^{T}\Delta X_{BA} + c\cdot V_{ij} + \Delta N^{i}_{BA}\lambda + n^{i}_{rBA}\lambda\end{aligned} \tag{1}$$

其中，φ^{i}_{B} 和 φ^{i}_{A} 分别是天线 B 和天线 A 所接收到的 GNSS 卫星 i 的载波相位观测值，λ是 GNSS 信号对应的波长。$\Delta\rho^{i}_{BA}$ 是两个天线对卫星 i 的伪距差，c 为光速，V_{ij} 是接收机钟差，ΔN^{i}_{BA} 为整周模糊度，n^{i}_{rBA} 为载波相位单差观测噪声，

为零均值的高斯白噪声。$\hat{r}^i$ 为 GNSS 卫星 i 到天线的方向余弦向量，为[3×1]的矩阵，可以由卫星的广播星历计算得知。ΔX_{BA} 为 ECEF 坐标系下的天线向量坐标，为[3×1]的矩阵，即 $\Delta X_{BA}=[\Delta x_{BA},\Delta y_{BA},\Delta z_{BA}]^T$。由于基线长度较短，整周模糊度非常容易确定，因此公式（1）可以写成：

$$\begin{aligned}\Delta\varphi_{BA}^{i}\lambda &= (\Delta\tilde{\varphi}_{BA}^{i}-\Delta N_{BA}^{i})\lambda \\ &= (\hat{r}^{i})^{T}\Delta X_{BA}+c\cdot V_{ij}+n_{rBA}^{i}\lambda\end{aligned} \tag{2}$$

对应的载波相位双差观测方程为：

$$\Delta\varphi_{BA}^{ij}\lambda=(\hat{r}^{ij})^{T}\Delta X_{BA}+n_{rBA}^{ij}\lambda \tag{3}$$

$\Delta\varphi_{BA}^{ij}$ 为载波相位双差值，$\hat{r}^{ij}$ 为卫星 i,j 到天线的方向余弦的向量差，n_{rBA}^{ij} 为观测噪声，$n_{rBA}^{ij}\sim N(0,\sigma_0^2)$。

当观测卫星数为 N 时，构成载波相位双差观测方程组为：

$$\Delta\varphi_{BA}\lambda=H\Delta X_{BA}+n_{rBA}\lambda \tag{4}$$

其中，$\Delta\varphi_{BA}$ 为[(N-1)×1]的矩阵，分别对应 N-1 颗卫星和基准星 i 之间的载波相位双差值。H 为[(N-1)×3]的矩阵，为 N-1 颗卫星和基准星 i 之间的方向余弦向量差，n_{rBA} 为观测噪声矩阵，同样为[(N-1)×1]的矩阵，为互相独立的正太分布。

对式（4）进行最小二乘解算，则

$$\Delta X_{BA}=A\Delta\varphi_{BA}\lambda \tag{5}$$

其中 $A=(H^TH)^{-1}H^T$，ΔX_{BA} 满足正太分布，我们对矩阵 H 进行奇异值分解（SVD）：

$$H=UDV^{T}=\sum_{i=1}^{3}\sigma_i\mu_i v_i^{T} \tag{6}$$

式中 $\sigma_i=\sqrt{\lambda_i}$ 为矩阵 H 的正奇异值，λ_i 为 H 的特征值，$D=diag(\sigma_1,\sigma_2,\sigma_3)$为对角矩阵，且$\sigma_1\geq\sigma_2\geq\sigma_3>0$。$\mu_i, v_i$ 分别为正交矩阵 U 和 V 的列向量，则ΔX_{BA} 的方差可以分别记为：

$$\sigma_x^2 = \sigma_0^2 \sum_{i=1}^{k} (\frac{v_{1,i}}{\sigma_i})^2$$
$$\sigma_y^2 = \sigma_0^2 \sum_{i=1}^{k} (\frac{v_{2,i}}{\sigma_i})^2 \quad (7)$$
$$\sigma_z^2 = \sigma_0^2 \sum_{i=1}^{k} (\frac{v_{3,i}}{\sigma_i})^2$$

因此我们可以将ΔX_{BA}记为$\Delta X_{BA} \sim N(b_{BA}, \sigma_X^2)$，$b_{BA} = [b_x, b_y, b_z]^T$为基线向量的真值，$\sigma_X = [\sigma_x, \sigma_y, \sigma_z]^T$。

先假设基线向量真值 b_{BA} 已知，我们将满足正太分布的ΔX_{BA}进行标准化，即：

$$\Delta X'_{BA} = (\Delta X_{BA} - b_{BA}) / \sigma_X \quad (8)$$

其中$\Delta X'_{BA} = [\Delta x'_{BA}, \Delta y'_{BA}, \Delta z'_{BA}]^T$，$\sigma_X = [\sigma_x, \sigma_y, \sigma_z]^T$。我们使用 *SSE* 来对$\Delta X_{BA}$进行测试统计，*SSE* 指标依照如下公式定义：

$$SSE = \Delta x'^2_{BA} + \Delta y'^2_{BA} + \Delta z'^2_{BA} \quad (9)$$

当没有欺骗信号时，载波相位观测值和信号来向相匹配，$\Delta X'_{BA} \sim N(0,1)$，则公式（9）所定义的 *SSE* 统计指标符合自由度为 3 的卡方分布。当存在欺骗信号时，载波相位观测方程组可表示为：

$$\Delta \varphi_{spBA} = \Delta \varphi_{BA} + \Delta \varphi_{spau} \quad (10)$$

其中$\Delta \varphi_{spau}$是[(N-1)×1)]的矩阵，表示欺骗信号和真实信号之间的载波相位差，则公式 5 可以表示为：

$$\Delta X_{spBA} = A\Delta \varphi_{spBA}\lambda = A(\Delta \varphi_{BA} + \Delta \varphi_{spau})\lambda = \Delta X_{BA} + A\Delta \varphi_{spau}\lambda \quad (11)$$

那么$\Delta X_{SPBA} \sim N(b_{BA} + A\Delta \varphi_{spau}\lambda, \sigma_X^2)$，公式 8 可以表示为：

$$\Delta X'_{SPBA} = (\Delta X_{SPBA} - b_{BA}) / \sigma_X, \quad (12)$$

其中$\Delta X'_{MBA} = [\Delta x'_{MBA}, \Delta y'_{MBA}, \Delta z'_{MBA}]^T$，$\Delta X'_{MBA} \sim N(A\Delta \varphi \lambda ./ \sigma_X, 1)$，对应的 *SSE* 为：

$$SSE = \Delta x'^2_{spBA} + \Delta y'^2_{spBA} + \Delta z'^2_{spBA} \quad (13)$$

此时 *SSE* 应当满足自由度为 3 的非中心卡方分布，记为$\chi^2(3,\gamma)$，γ表示偏心参量：

$$\begin{aligned} H_0(no\ \text{spoofing}) &: SSE \sim \chi^2(3) \\ H_1(\text{spoofing}) &: \quad SSE \sim \chi'^2(3,\gamma) \end{aligned} \tag{14}$$

其中 $\gamma = (b_{BA} + A\Delta\varphi_{spau}\lambda)^T (b_{BA} + A\Delta\varphi_{spau}\lambda)$，对于 H_1 假设，SSE 很明显与 $\Delta\varphi_{spau}$ 成正比。根据纽曼皮尔逊准则，我们可以通过设置合适的门限值，在一定的虚警率下确定对应的检测率。

$$\begin{cases} P_{fa} = P\{Q > Q_{th} \mid H_0\} = 1 - \int_0^{Qth} p_{\chi^2(3)}(Q)dQ \\ P_D = P\{Q > Q_{th} \mid H_1\} = 1 - \int_{Qth}^{\infty} p_{\chi^2(3,\gamma)}(Q)dQ \end{cases} \tag{15}$$

其中 $p_{\chi^2(3)}$ and $p_{\chi^2(3)}$ 是$\chi^2(3)$和$\chi^2(3,\gamma)$的概率密度函数。

我们假设卫星信号 j 为欺骗信号，则载波相位双差的相应方程如下：

$$\Delta\varphi_{spBA}^{ij} = \Delta\varphi_{BA}^{ij} + \Delta\varphi_{spau}^{ij} \tag{16}$$

其中 $\Delta\varphi_{spBA}^{ij}$ 为欺骗信号所对应的载波相位双差值，$\Delta\varphi_{BA}^{ij}$ 为真实信号的载波相位双差值，$\Delta\varphi_{spau}^{ij}$ 为欺骗信号 j 和真实信号载波相位双差值的偏差。我们将公式（2）重新写成式（17），二者是完全等价的：

$$\begin{aligned} \Delta\varphi_{BA}^{i}\lambda &= (\hat{r}^i)^T \Delta X_{BA} + c\cdot V_{ij} + \Delta N_{BA}^{i}\lambda + n_{rBA}^{i}\lambda \\ &= \mid d \mid \cos\theta_i + c\cdot V_{ij} + \Delta N_{BA}^{i}\lambda + n_{rBA}^{i}\lambda \end{aligned} \tag{17}$$

其中，d 为基线向量长度，θ_i 为信号的到达角，那么式（3）也可以写成：

$$\Delta\varphi_{BA}^{ij}\lambda = \mid d \mid (\cos\theta_i - \cos\theta_j) + n_{rBA}^{ij}\lambda \tag{18}$$

联立式（16）和（18）可得：

$$\begin{aligned} \Delta\varphi_{spau}^{ij}\lambda &= \Delta\varphi_{spBA}^{ij}\lambda - \Delta\varphi_{BA}^{ij}\lambda \\ &= \mid d \mid \cdot(\cos\theta_{spj} - \cos\theta_j) + n_{spau}^{ij}\lambda \\ &= \mid d \mid \cdot\Delta\cos\theta_{spau} + n_{spau}^{ij}\lambda \end{aligned} \tag{19}$$

其中，θ_{spj} 为欺骗信号的到达角，θ_j 为真实信号的到达角，$\Delta\cos\theta_{spau}$ 是欺骗信号和真实信号到达角的余弦差。从式（19）我们可以看出，$\Delta\varphi_{spau}^{ij}$ 与基线长度 d 以及欺骗信号和真实信号到达角的余弦差$\Delta\cos\theta_{spau}$ 正相关。在上文提到，SSE 指标与 $\Delta\varphi$ 正相关，因此当存在欺骗信号时，SSE 指标与 d 以及$\Delta\cos\theta_{spau}$ 正相关。

我们通过蒙特卡罗方法模拟了不同基线长度 d 以及$\Delta\cos\theta_{spau}$下，H_0和 H_1 假设所对应 *SSE* 指标概率密度分布，如图 4.2 所示。

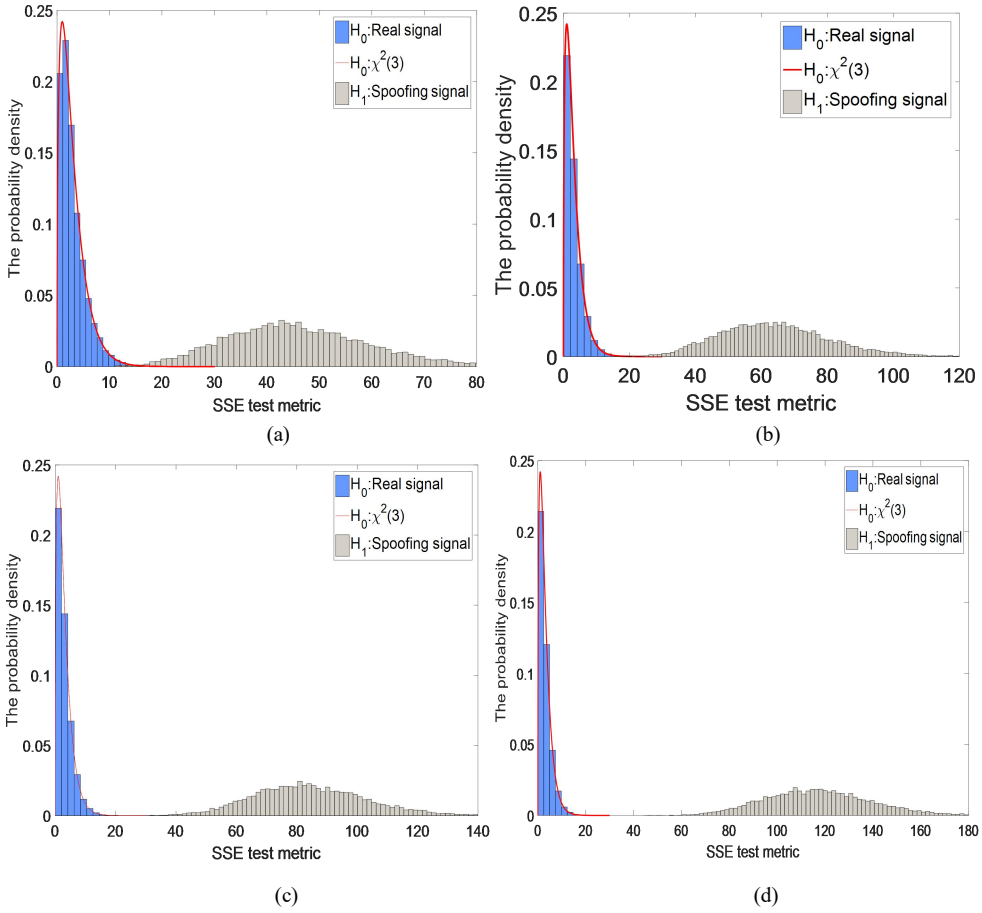


图 4.2　H_0 和 H_1 假设所对应的 *SSE* 概率密度分布 (a) d=4λ,$\Delta\cos\theta_{spau}$=0.06. (b) d=4λ,$\Delta\cos\theta_{spau}$=0.10. (c) d=5λ,$\Delta\cos\theta_{spau}$=0.06. (d) d=5λ,$\Delta\cos\theta_{spau}$=0.10.

从图 4.2 中我们可以很清楚地看出，H_0 假设的 *SSE* 指标完美地符合χ^2(3；H_1 假设的的 *SSE* 指标与χ^2(3 产生了明显的偏差。*SSE* 指标与 d 和$\Delta\cos\theta_{spau}$成正比，与理论计算的结果完全一致。

图 4.3 显示了不同参数下的接受者操作特征曲线（ROC）曲线。可以看出，随着 d 和$\Delta\cos\theta_{spau}$的增加，欺骗检测的性能会随之提高。当 d=5λ，$\Delta\cos\theta_{spau}$=0.10 时，ROC 曲线非常接近理论性能边界。

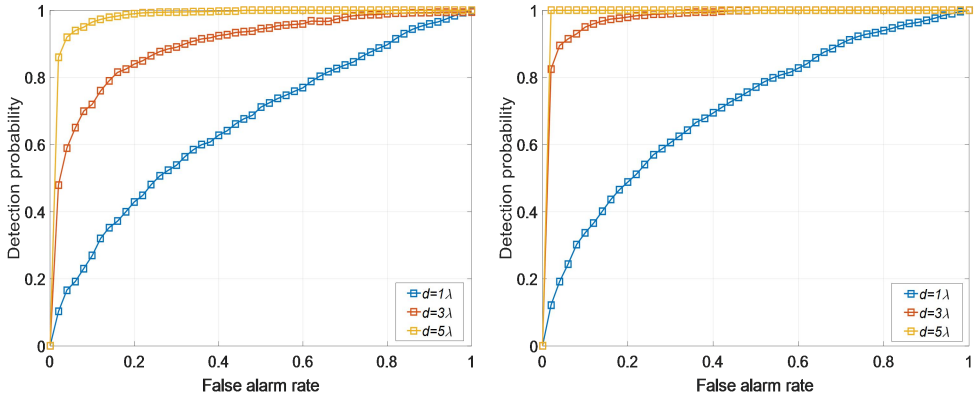


图 4.3 不同参数下的 ROC 曲线。(a) $\Delta\cos\theta_{spau}$=0.06. (b) $\Delta\cos\theta_{spau}$=0.10.

4.1.2 基线向量估计算法

在上诉的讨论中，我们假设基线向量b_{BA}是已知的。但由于该方法并未使用惯性辅助单元来提前获取天线的姿态信息，因此b_{BA}事实上并不可知，因此我们需要提出基线向量的估计方法。该方法本质上是用已知的基线长度对基线向量的观测值进行约束，并进行迭代计算，将若干次迭代之后的稳定值视为基线向量真值的有效近似。

记$b_{BA}^{'}$为b_{BA}的估计值，可以从如下形式的迭代方程式进行计算：

$$b_{n+1}^{'}=b_{n}^{'}+\delta_{Xn} \tag{20}$$

其中$b_{n+1}^{'}=[\Delta x_{n+1},\Delta y_{n+1},\Delta z_{n+1}]^T$，$b_{n}^{'}=[\Delta x_{n},\Delta y_{n},\Delta z_{n}]^T$分别为第 n+1 次和第 n 次迭代的结果，$\delta_{Xn}=[\delta_{xn},\delta_{yn},\delta_{zn}]^T$为第 n 次迭代的残差，$d$能够表示为：

$$\begin{aligned} d&=\sqrt{\Delta x_{n+1}^2+\Delta y_{n+1}^2+\Delta z_{n+1}^2} \\ &=\sqrt{(\Delta x_n+\delta_x)^2+(\Delta y_n+\delta_y)^2+(\Delta z_n+\delta_z)^2} \end{aligned} \tag{21}$$

我们用一阶泰勒展开对上式进行线性化可以得到：

$$d=\sqrt{\Delta x_n^2+\Delta y_n^2+\Delta z_n^2}+l_{Xn}\delta_{Xn} \tag{22}$$

式中，

$$l_{Xn}=\begin{bmatrix}l_{xn}\\l_{yn}\\l_{zn}\end{bmatrix}=\begin{bmatrix}\Delta x_n/\sqrt{\Delta x_n^2+\Delta y_n^2+\Delta z_n^2}\\\Delta y_n/\sqrt{\Delta x_n^2+\Delta y_n^2+\Delta z_n^2}\\\Delta z_n/\sqrt{\Delta x_n^2+\Delta y_n^2+\Delta z_n^2}\end{bmatrix},\ \delta_{\mathrm{Xn}}=\begin{bmatrix}\delta_{xn}\\\delta_{yn}\\\delta_{zn}\end{bmatrix} \tag{23}$$

将式（20）代入式（5），并和式（22）进行联立，

$$\begin{cases}d=\sqrt{\Delta x_n^2+\Delta y_n^2+\Delta z_n^2}+l_{Xn}\delta_{Xn}\\\Delta\varphi_{BA}\lambda=H\cdot(b_n^{'}+\delta_{Xn})+n_{rBA}\end{cases} \tag{24}$$

δ_{Xn} 可以通过最小二乘法得到。由（5）计算出的结果作为（20）迭代的初始值。多次迭代后的稳定值为 $b_{BA}^{'}$，它是 b_{BA} 的近似值。使用 $b_{BA}^{'}$ 重新计算 *SSE* 指标，所对应的概率密度分布如图 4.4 所示。

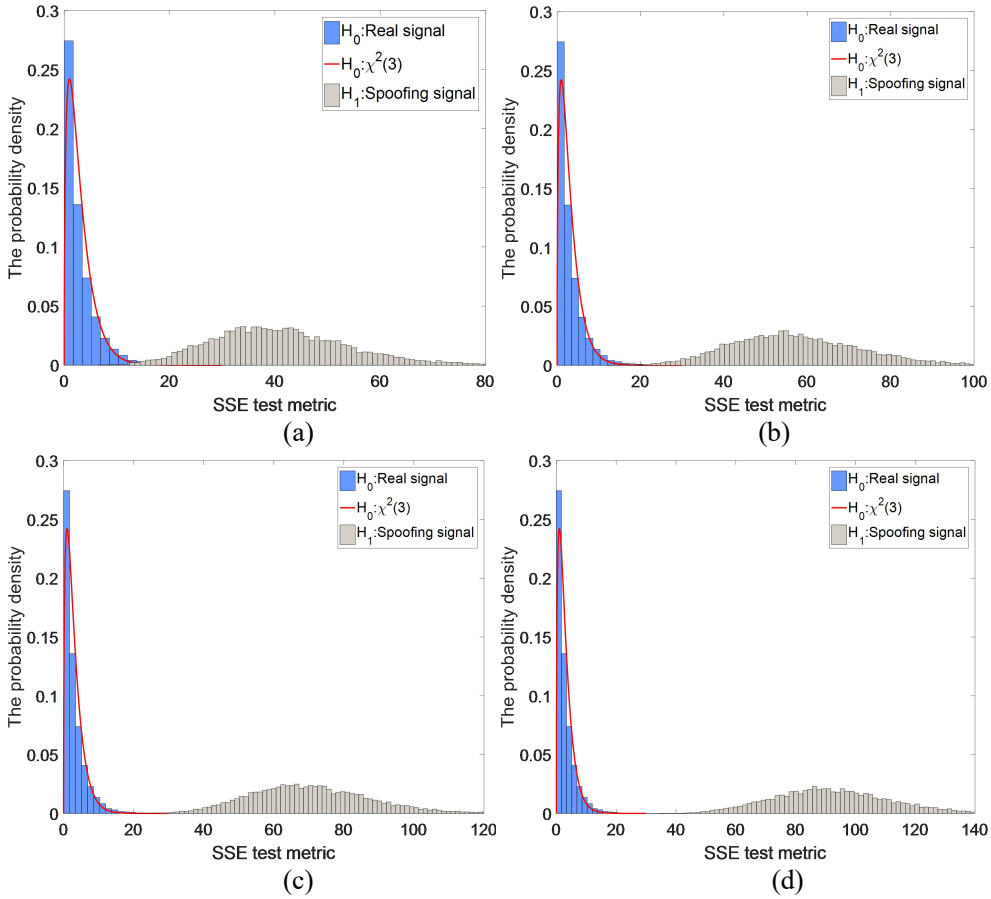


图 4.4 重新计算的 H_0 和 H_1 假设所对应的 *SSE* 概率密度分布 (a) d=4λ,$\Delta\cos\theta_{spau}$=0.06. (b) d=4λ,$\Delta\cos\theta_{spau}$=0.10. (c) d=5λ,$\Delta\cos\theta_{spau}$=0.06. (d) d=5λ,$\Delta\cos\theta_{spau}$=0.10.

将图 4.4 和图 4.2 对比我们可以看出，由于 $b_{BA}^{'}$ 是 b_{BA} 的近似，存在一定的误差，因此图 3 中 H_0 假设的 *SSE* 指标与$\chi^2(3)$的概率密度分布存在些许的偏差。为了表征我们提出的基线向量估计方法的性能，我们使用 R-squared 和 F-test 对 H_0

的 *SSE* 概率密度分布和$\chi^2(3)$概率密度分布进行了统计，表 4.1 显示了 H_0 假设与$\chi^2(3)$之间的 R-squared 和 F-test 统计值。

表 4.1　R-squared 和 F-test 统计值

d	R-squared	F-test
2λ	0.887	1.041
4λ	0.886	1.065
6λ	0.875	1.060
8λ	0.879	1.062
10λ	0.881	1.056

我们通常使用 R-squared 统计量来评估拟合程度。R-squared 越接近 1，则统计模型与数据的拟合效果越好，并且模型解释的能力越强。在任何基线向量长度下，表 4.1 中的 R-squared 都非常接近 1。另一方面，F 检验的作用是评估两个样本的方差是否一致。通过查表法可以得知，在任何基线向量长度下，H_0 假设和$\chi^2(3)$之间均存在高度的相关性。因此，$\chi^2(3)$是 H_0 假设的有效近似值。通过设置合理的阈值，我们仍然可以有效地检测到欺骗信号。

4.1.3 使用三天线的欺骗检测算法

在多天线姿态已知的前提下，我们可以通过星历信息中的卫星位置和阵列的几何结构确定信号在天线坐标系中的理论入射方向，另一方面可以通过载波相位数据确定卫星信号实际的入射方向，当二者不一致时，则认为存在欺骗信号。我们采用三个天线时，就能够确定天线的姿态，因此我们需要构建基于三天线的姿态确定方法。

我们采用双天线欺骗检测方法中的基线向量估计方法，用基线向量长度去约束载波相位观测方程，能够得到较为精确的两组独立基线。此时，可以采用双矢量定姿法确定天线的姿态矩阵。

假设基线向量在载体坐标系和导航坐标系的坐标分别为V_1^b、V_2^b、V_1^n、V_2^n，我们用 C_n^b 用来表示载体坐标系和导航坐标系之间的旋转关系，即：

$$\begin{aligned} V_1^b &= C_n^b V_1^n \\ V_2^b &= C_n^b V_2^n \end{aligned} \tag{25}$$

将公式（25）的两边依次做叉乘得到：

$$V_1^b \times V_2^b = (C_n^b V_1^n) \times (C_n^b V_2^n) = C_n^b (V_1^n \times V_2^n) \tag{26}$$

写成矩阵形式并最终得到：

$$C_n^b = [V_1^b \; V_2^b \; V_1^b \times V_2^b][V_1^n \; V_2^n \; V_1^n \times V_2^n]^{-1} \tag{27}$$

其中 C_n^T 在理想状态应是单位正交矩阵，则有：

$$C_n^b = [(C_n^b)^T]^{-1} \tag{28}$$

对公式 27 等号两边同时先求转置再求逆可以得到两个坐标系的姿态阵为：

$$C_n^b = \begin{bmatrix} (V_1^b)^T \\ (V_2^b)^T \\ (V_1^b \times V_2^b)^T \end{bmatrix}^{-1} \begin{bmatrix} (V_1^n)^T \\ (V_2^n)^T \\ (V_1^n \times V_2^n)^T \end{bmatrix} \tag{29}$$

但是这个矩阵也存在问题，V_1^b 、V_2^b 、V_1^n 、V_2^n 是由测量得到的，存在的测量误差会导致由公式（29）计算出的姿态阵不满足单位正交的条件。

为了解决上述问题，我们在导航坐标系中由测量矢量 V_1^n 和 V_2^n 来构造下列三个正交的单位矢量：

$$\frac{V_1^n}{|V_1^n|}、\frac{V_1^n \times V_2^n}{|V_1^n \times V_2^n|}、\frac{V_1^n \times V_2^n \times V_1^n}{|V_1^n \times V_2^n \times V_1^n|} \tag{30}$$

类似的在载体坐标系中由 V_1^b 和 V_2^b 来构造下列三个正交的单位矢量：

$$\frac{V_1^b}{|V_1^b|}、\frac{V_1^b \times V_2^b}{|V_1^b \times V_2^b|}、\frac{V_1^b \times V_2^b \times V_1^b}{|V_1^b \times V_2^b \times V_1^b|} \tag{31}$$

将上述矢量代入公式（29）可以得到：

$$C_n^b = \begin{bmatrix} (\frac{V_1^b}{|V_1^b|})^T \\ (\frac{V_1^b \times V_2^b}{|V_1^b \times V_2^b|})^T \\ (\frac{V_1^b \times V_2^b \times V_1^b}{|V_1^b \times V_2^b \times V_1^b|})^T \end{bmatrix}^{-1} \begin{bmatrix} (\frac{V_1^n}{|V_1^n|})^T \\ (\frac{V_1^n \times V_2^n}{|V_1^n \times V_2^n|})^T \\ (\frac{V_1^n \times V_2^n \times V_1^n}{|V_1^n \times V_2^n \times V_1^n|})^T \end{bmatrix} = \begin{bmatrix} \frac{V_1^b}{|V_1^b|} \frac{V_1^b \times V_2^b}{|V_1^b \times V_2^b|} \frac{V_1^b \times V_2^b \times V_1^b}{|V_1^b \times V_2^b \times V_1^b|} \end{bmatrix} \begin{bmatrix} (\frac{V_1^n}{|V_1^n|})^T \\ (\frac{V_1^n \times V_2^n}{|V_1^n \times V_2^n|})^T \\ (\frac{V_1^n \times V_2^n \times V_1^n}{|V_1^n \times V_2^n \times V_1^n|})^T \end{bmatrix} \tag{32}$$

根据坐标系的旋转关系可以得到：

$$C_n^b = \begin{bmatrix} (\cos\gamma\cos\psi - \sin\gamma\sin\theta\sin\psi) & (\cos\gamma\sin\psi + \sin\gamma\sin\theta\cos\psi) & -\sin\gamma\cos\theta \\ -\cos\theta\sin\psi & \cos\theta\cos\psi & \sin\theta \\ (\sin\gamma\cos\psi + \cos\gamma\sin\theta\sin\psi) & (\sin\gamma\sin\psi - \cos\gamma\sin\theta\cos\psi) & \cos\gamma\cos\theta \end{bmatrix} \tag{33}$$

其中γ为横滚角，θ为俯仰角，ψ为航向角。我们记

$$C_n^b = \begin{bmatrix} C_{11} & C_{12} & C_{13} \\ C_{21} & C_{22} & C_{23} \\ C_{31} & C_{32} & C_{33} \end{bmatrix} \tag{34}$$

则三个姿态角计算公式为：

$$\begin{aligned} \gamma &= -a\tan 2(C_{13}, C_{33}) \\ \theta &= -a\tan 2(C_{23}, \sqrt{C_{21}^2 + C_{22}^2}) \\ \psi &= -a\tan 2(C_{21}, C_{22}) \end{aligned} \tag{35}$$

GNSS 信号在载体坐标系的方向矢量可以记为：

$$g(\alpha,\beta) = -[\cos\alpha\cos\beta, \cos\alpha\sin\beta, \sin\alpha]^T \tag{36}$$

其中α和β是信号在载体坐标系的仰角和方位角。另一方面，根据卫星的星历信息，可以得到信号在 ENU 坐标系下的方向矢量：

$$g_{ENU}(El, Az) = -[\cos El\cos Az, \cos El\sin Az, \sin El]^T \tag{37}$$

根据坐标系变换矩阵，则方向矢量应当满足如下关系：

$$g(\alpha,\beta) = C_n^b g_{ENU}(El, Az) \tag{38}$$

当不存在欺骗信号时，根据天线的几何关系可以得到：

$$\Delta\varphi^i\lambda = b^T g(\alpha,\beta) + N \tag{39}$$

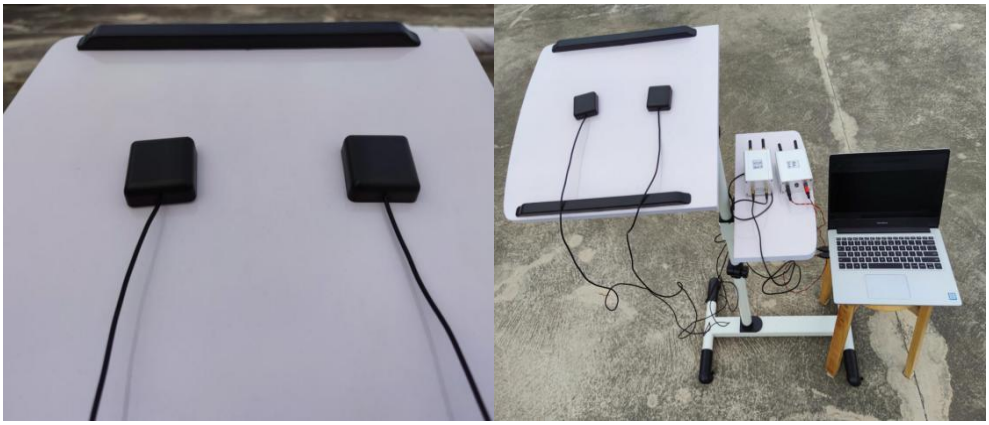
其中 N 为观测噪声，$\Delta\varphi^i$ 载波相位单差矩阵，b^T 为载体坐标系下的基线向量矩阵。而当存在欺骗信号时，公式(39)不再成立，等号两边存在显著的不一致性，因此能够检测出欺骗信号的存在。

4.2 实验方案

4.2.1 虚警率测试实验方案

为了验证本课题所提出的欺骗检测方法的虚警率，于中国科学院空天信息创新研究院的楼顶架设系统接收真实的无欺骗信号。系统的结构和布局如图 4.5 所

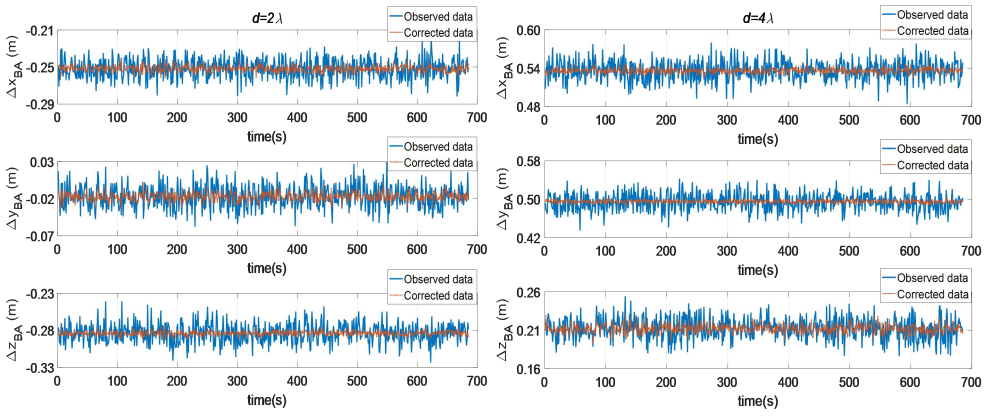
示。本实验中使用的接收器是封装的 Ublox Neo-M8n 模块。运行欺骗检测软件的笔记本电脑充当系统的信号处理单元。接收器接受非欺骗性的 GNSS 信号，并将其发送到笔记本电脑以估计基线向量和相应的 *SSE* 测试指标。笔记本电脑实时给出欺骗检测和定位的结果。



(a) (b)

图 4.5 欺骗检测系统(a)放置于同一平面的天线；(b)系统的布局。

天线基线向量的观测值和修正值如图 4.6 所示。每组的观察时间约为 11 分钟。两组的基线长度分别为 2λ和 4λ。由于受到高斯白噪声的影响，蓝色曲线所表示的基线矢量观测值ΔX_{BA}遵循正态分布。这与上文模拟的结论是一致的。与此同时，红色曲线表示的基线向量的修正值b'_{BA}显然比观测值更平滑，并且更接近真值。



(a) (b)

图 4.6 基线向量的观测值和修正值(a)d=2λ, b_{BA}= [-0.252m, -0.017m, -0.284m]^T. (b) d=4λ, b_{BA}= [0.536m, 0.495m, 0.212m]^T.

表 4.2 给出了基线向量观测值和修正值的平均值和标准差。可以很容易地看出，修正值的平均值非常接近真实值，并且修正值的标准偏差明显小于观测值。因此，采用修正值作为真实基线向量的近似是一种有效的统计估计方法。

表 4.2 基线向量观测值和修正值的平均值和标准差

d	Situation	Parameter	Δx_{BA}	Δy_{BA}	Δz_{BA}
2λ	observed	mean (m)	-0.250	-0.017	-0.283
		std (m)	0.011	0.015	0.013
	corrected	mean (m)	-0.252	-0.018	-0.284
		std (m)	0.004	0.006	0.003
4λ	observed	mean (m)	0.535	0.496	0.210
		std (m)	0.015	0.018	0.014
	corrected	mean (m)	0.536	0.496	0.212
		std (m)	0.004	0.003	0.006

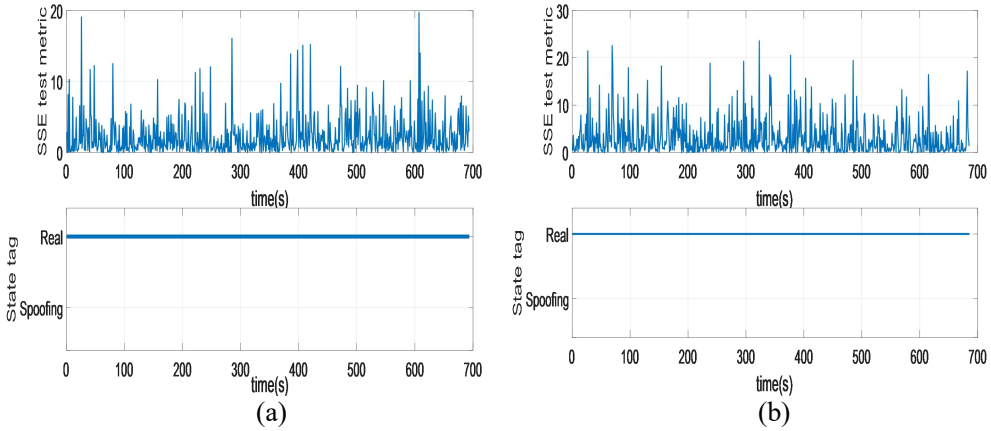


图 4.7 *SSE* 指标和状态标签 (a)d=2λ,(b) d=4λ。

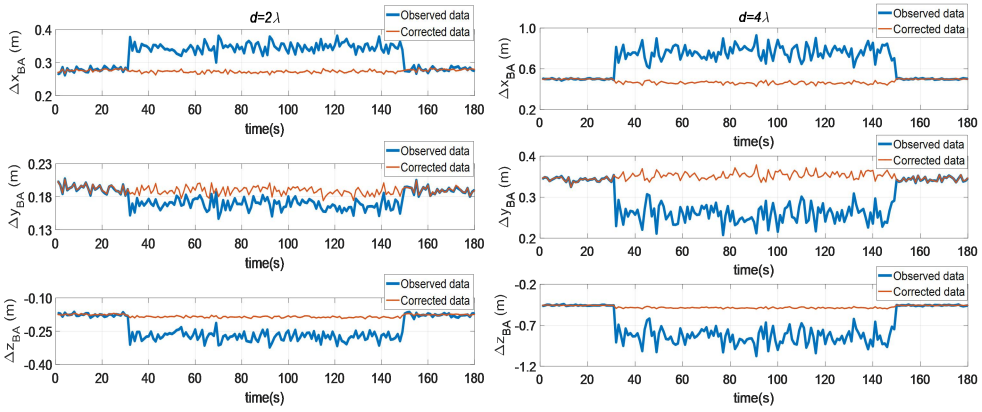
我们根据$\chi^2(3)$的累积分布函数（CDF）设置适当的阈值 $SSE_{th}=30$，对应的理论虚警率为 1.38×10^{-6}。我们定义了两个卫星信号状态标签。当 *SSE* 测试指标小于 SSE_{th}时，我们将其标记为“real”，这表示当前接收到的卫星信号全部都是非欺骗性的。否则，我们将其标记为“spoofing”，表示存在至少一个欺骗信号。*SSE* 测试指标如图 4.7 所示。因为系统在整个实验期间均接收真实信号，因此状态标签均为“real”，误报率为零。

4.2.2 静态性能实验方案

我们采用 GNSS 信号转发器作为欺骗攻击的信号源，以干扰一路 GNSS 信号。为了确保接收器可以成功跟踪欺骗信号，我们使用低噪声放大器适当地放大了信号。同时，放大器功率应尽可能低，以避免对其他实际 GNSS 信号的干扰。

测试的基线向量观测值和估计值如图 4.8 所示，每组的测试时间为 180s。我们在 30 秒时打开转发器，然后在 150 秒时关闭它。两组的基线长度分别为 2λ和 4λ。转发器在 0-29s 和 151s-180s 处于关闭状态时，蓝色曲线所示的基线向量观

测值遵循正态分布。当转发器在 30s 开启时，由于欺骗信号的功率大于真实信号，因此接收器会立即跟踪欺骗信号，蓝色曲线在 30-150s 发生了非常显著的偏移，红色曲线所示的基线向量修正值非常接近实际值，波动很小。



(a) (b)

图 4.8 基线向量的观测值和修正值 (a)d=2λ,(b) d=4λ。

SSE 测试指标和状态标签计算的结果如图 4.9 所示。当转发器在 30s 开始工作时，*SSE* 测试指标无任何延迟地急剧增加。在图 4.9(a)中，除了 69s 以外，*SSE* 测试指标在 30s 至 150s 之间均大于阈值，并且检测概率 P_{D1}=99.2%。在图 4.9(b)中，*SSE* 测试指标远大于阈值，状态标签均为“spoofing”，检测概率 P_{D1}=100%。这表明随着基线向量的长度增加，系统的检测概率也增加。

在这种情形下，基线长度为 2λ的 *SSE* 测试指标的最大值为 583，而基线长度为 4λ的 *SSE* 测试指标的最大值为 1274。这表明，随着基线长度的增加，*SSE* 测试指标也随之增加，*SSE* 测试指标与基线长度 d 呈正相关，与上文讨论的结果完全一致。

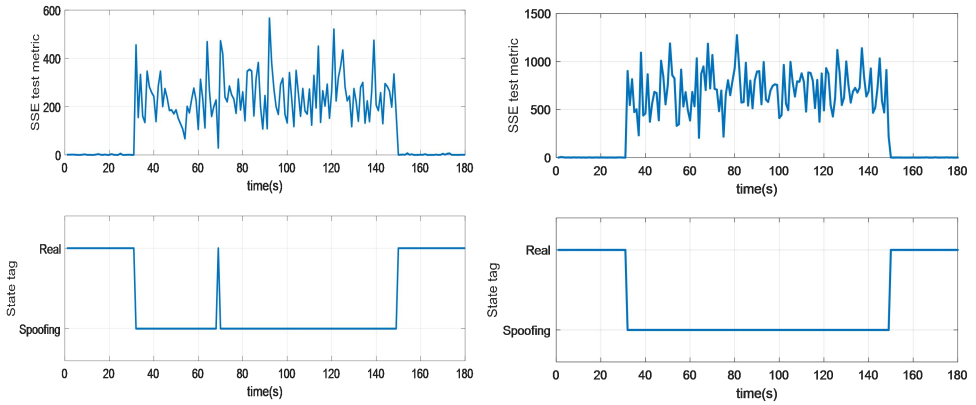


图 4.9 *SSE* 指标和状态标签 (a)d=2λ,(b) d=4λ。

图 4.10 显示了天线 A 的一组定位估计。接收机在这种静态情况下同时跟踪 7 个 GPS 卫星信号。当 30 秒钟开启时，转发器立即干扰一个 GPS 信号，并对接

收器的定位结果产生一定的影响。最大定位误差在 93s 时达到 0.21 米。

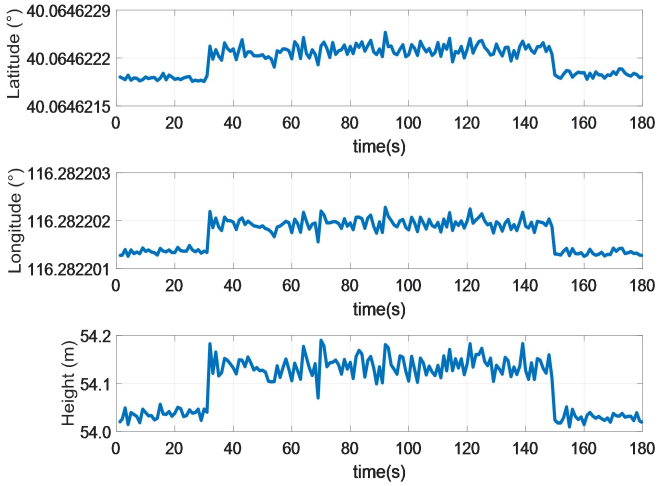
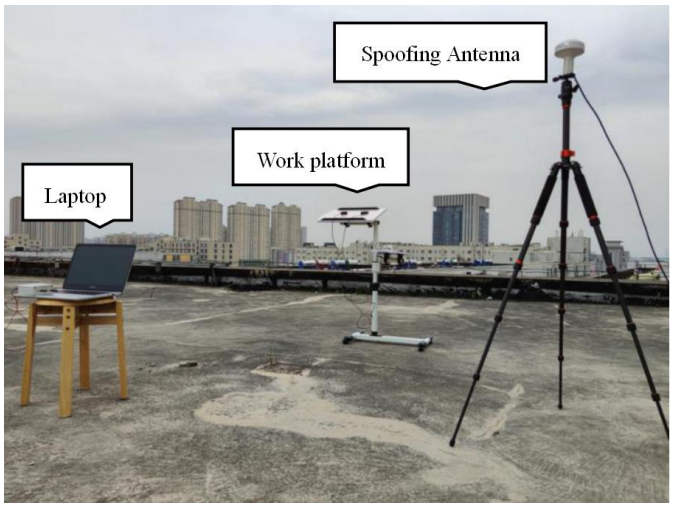


图 4.10 静态场景的定位结果

4.2.3 动态性能实验方案

在动态测试场景中，GNSS 转发器的天线固定在三脚架上，如图 4.11 所示。我们在可移动的工作平台上安装课题的欺骗检测系统。我们移动工作平台以模拟用户的低速运动。沿东西方向线性移动工作平台逐渐接近三脚架，然后移开。由于实验场的区域有限，如果转发器的功率电平足够高，则接收器将仅跟踪欺骗信号。因此，为了演示接收器捕获欺骗信号的整个过程，应尽可能降低转发器的功率电平，并使其略高于实际信号。

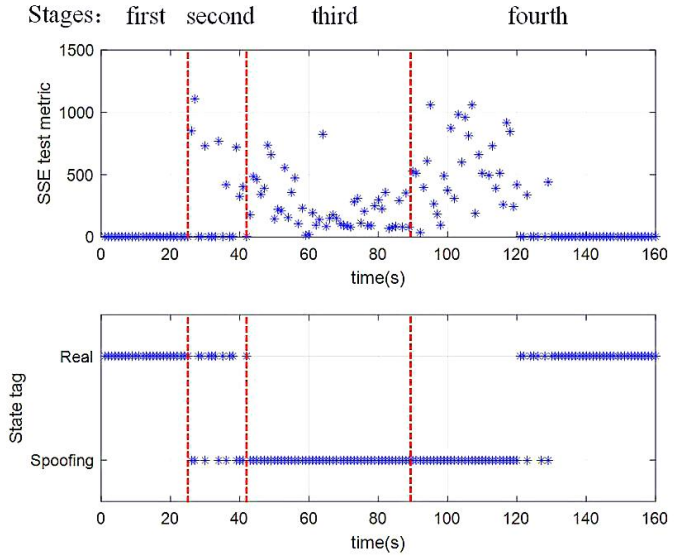


4.11 在建筑物屋顶的动态测试场景

动态测试场景的 *SSE* 指标和状态标签如图 4.12 所示，测试时间为 160s，可以分成四个阶段。在第一阶段 0~25s，工作平台从远处逐渐接近转发器，此时，

由于工作平台距离转发器天线较远，接收机接收的是真实信号，*SSE* 指标明显小于门限值，对应的状态标志均为“real”。

在第二阶段为 26s-42s，工作平台开始接近转发器天线。可以看出，由于欺骗信号和真实信号的功率逐渐接近，接收机的跟踪信号变得非常不稳定。换句话说，接收器的跟踪环路开始捕获欺骗信号，并在此阶段导致接收器频繁失锁。*SSE* 测试指标变化很大，最大值在 27s 达到 1109。*SSE* 测试指标的最大值与静态测试方案中的最大值相一致。信号状态标签在“real”和“spoofing”之间来回摆动。



4.12 动态场景中的 *SSE* 测试指标和状态标签

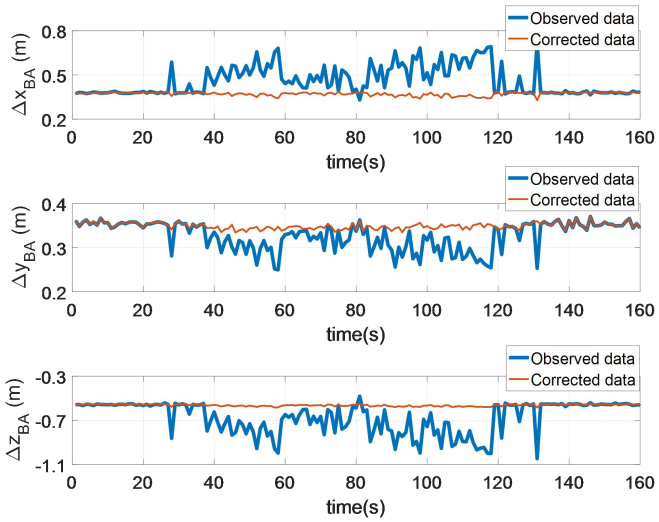
在第三阶段 43s-89s，真实信号完全被欺骗信号淹没。由于欺骗信号的功率明显大于真实信号，因此接收机跟踪了欺骗信号。在该阶段，*SSE* 测试指标超出阈值很多，并且信号状态标签都标记为“spoofing”。同时，可以明显看出，此阶段的 *SSE* 指标明显小于第二阶段的 *SSE* 指标。在此阶段，*SSE* 指标的最大值在 64 秒时为 820。由于工作平台靠近转发器天线，欺骗信号和真实信号的到达角在接近。因此，到达角的余弦差呈下降趋势，*SSE* 度量指标也呈下降趋势。这与模拟结论完全一致。

第四阶段为 90s 后，工作平台逐渐远离转发器天线，这与上述过程相反，在此不再赘述。

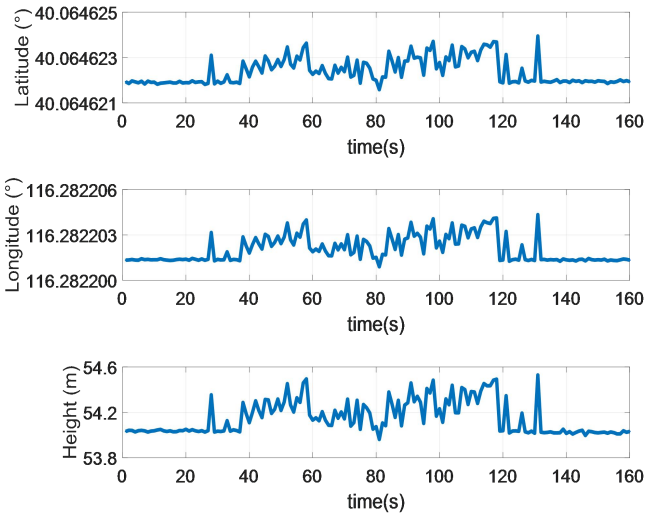
动态场景中基线向量计算结果如图 4.13 所示。蓝色曲线显示的基线向量观测值的变化规律与 *SSE* 指标一致。接收器在 0-25s 时跟踪真实信号，基线向量的观测值遵循正态分布。随着接收器在 26s-42s 逐步捕获欺骗信号，基线向量的观

测值开始发生明显的偏移和抖动。当接收器在 43s-89s 跟踪欺骗信号时，基线矢量的观测值与真值之间会出现明显的偏差。

基线矢量的修正值在图 4.13 中用红色曲线表示。与观察值相比，修正后的数据非常稳定，接近真实值。在整个观察期内，它几乎不会随着欺骗信号的产生而变化。



4.13 动态场景中的基线向量



4.14 动态场景中的定位结果

在此测试方案中，接收器同时跟踪 8 个 GPS 卫星信号。由于我们使用的转发器仅干扰一个 GPS 卫星信号，因此图 4.14 中所示的定位估计结果变化相对较小。在 133s 时，最大定位误差为 0.67 米。考虑到当前单点定位的精度（通常在 10 米左右），用户很难通过用户的定位结果偏差来判断是否存在欺骗信号。将图 4.12 与图 4.14 进行比较，*SSE* 测试指标明显更具有鲁棒性，对检测欺骗信号更加敏感。

4.3 可行性分析

本课题拟开展的研究内容和采用的研究方法均进行了充分的文献调查和仿真分析，基于多天线的欺骗检测理论基础已经非常成熟。传统的多天线欺骗检测方法通常基于所有欺骗信号来自同一方向的假设，或者需要惯性测量单元获取天线的姿态信息，前者不能检测来自不同方向的欺骗信号，后者硬件成本相对较高。课题对上述方法进行了进一步的改进，提出了使用双天线的新型欺骗检测算法，能够检测来自不同方向的欺骗信号。另一方面提出了一种使用三天线的欺骗检测方法，能够在不需要任何辅助硬件设备的条件下确定天线的姿态，进而检测出欺骗信号的到达角。本课题的方法均通过仿真和实验的初步认真，具备切实的可行性且性能符合预期。

同时，本人所在的实验室在 GNSS 导航定位领域承担了大量的实验和科研项目，能够为课题的开展提供软件和硬件的支持，保障了本课题的顺利推进和经费需求，确保课题能够按时高效地完成。

总而言之，本课题在现阶段是切实可行的。

5. 已有科研基础与所需的科研条件

5.1 已有的科研基础

（1） 经过本人前期的文献调研，对基于多天线的 GNSS 欺骗检测相关领域的研究状况和主要理论已有了充分的了解。

（2）本人从博士阶段一直开展导航增强技术领域的相关研究工作，对导航定位算法、GNSS 信号处理、多径信号抑制等方向进行了较为深入的研究，具备一定的研究基础。

（3）本人博士阶段已经发表 GNSS 欺骗检测相关 SCI 论文一篇，申请专利两项（实审中）。

（4）本人所在的实验室对 GNSS 导航系统有相当深入的理论研究及工程经验，为今后的研究提供了良好的基础。

5.2 所需科研条件

（1）笔记本计算机一台，用于理论仿真研究以及程序编写、数据的记录和处理；

（2）MATLAB 软件工具包，用于场景仿真和数据处理；

（3）U-blox 接收机和对应的天线三套，用于数据采集；

（4）GNSS 信号模拟器和转发器一套，用于欺骗信号的生成以及实验测试平台的搭建。

6. 研究工作计划与进度安排

根据本课题的研究内容，沿循课题技术路线，拟将本课题的研究分为以下几个阶段：

2020 年 9 月—2020 年 11 月：完成博士期间研究方向的选题，完成开题报告的撰写，完成前期的调研，做好准备工作。

2020 年 12 月—2021 年 02 月：进一步完善双天线欺骗检测算法的理论模型，利用软件对性能进行仿真。

2021 年 2 月—2021 年 5 月：构建使用三天线欺骗检测算法的理论模型，完成三天线定姿算法的性能分析。

2021 年 6 月—2021 年 9 月：搭建欺骗检测测试验证平台，分别验证静态和动态情境下欺骗检测算法的检测性能。

2021 年 10 月—2021 年 12 月：完成小论文并投稿，撰写中期中期报告并准备中期答辩。

2022 年 1 月—2022 年 4 月：整理博士期间的研究成果，撰写毕业论文，准备毕业答辩。

7. 参考文献

[1] Misra P, Enge P. Global Positioning System: Signals, measurements, and performance[M]. Massachusetts, USA: Ganga-Jamuna Press, 2011.

[2] 谢钢. 全球导航卫星系统原理：GPS、格洛纳斯和伽利略系统[M]. 北京: 电子工业出版社, 2013.

[3] Yang Y, Li J, Xu J, et al. Contribution of the Compass satellite navigation system to global PNT users[J]. Chinese Science Bulletin, 2011, 56(26): 2813.

[4] Nosenko Y. GLONASS in a Multi-GNSS World[C]// Proceedings of ION GNSS 2008, Savannah, GA, USA, 2008: 7-19.

[5] Hegarty C J, Chatre E. Evolution of the Global Navigation Satellite System (GNSS)[J]. Proceedings of the IEEE, 2008, 96(12): 1902-1917.

[6] 谭述森. 北斗卫星导航系统的发展与思考[J]. 宇航学报, 2008, (2): 391-396.

[7] 谭述森, 周兵, 郭盛桃, 等. 我国全球卫星导航信号设计研究[J]. 中国科学:物理学 力学天文学, 2010, (5): 514-519.

[8] 邓中卫. GPS 与未来战争中的导航战[J]. 国际航空, 2000(5):52-53.

[9] 谭显裕. GPS 在导航战中的作用及其干扰对抗研究[J]. 现代防御技术, 2001(03):42-47.

[10] Ioannides T, Pany T, Gibbons G. Known vulnerabilities of global navigation satellite systems, status, and potential mitigation techniques[J]. Proceedings of the IEEE, 2016, 104(6): 1174-1194.

[11] Warner J, Johnston R. A Simple Demonstration that the Global Positioning System (GPS) is Vulnerable to Spoofing. Journal of Security Administration, 2003.

[12] 闻新, 刘彦军. GPS 干扰与反干扰技术在伊拉克战争中应用[J]. 全球定位系统, 2003(03):20-23.

[13] Kerns A J , Shepard D P , Bhatti J A , et al. Unmanned Aircraft Capture and Control Via GPS Spoofing[J]. Journal of Field Robotics, 2014, 31(4):617-636.

[14] Bhatti J , Humphreys T E . Hostile Control of Ships via False GPS Signals: Demonstration and Detection[J]. Navigation, 2017, 64(1):51-66.

[15] Broumandan A, Jafarnia-Jahromi A, Daneshmand S, et al. Overview of Spatial Processing Approaches for GNSS Structural Interference Detection and Mitigation[J]. Proceedings of the IEEE, 2016, 104(6):1246-1257.

[16] Guo Yi. Spoofing interference suppression using space-time process for GPS receiver[J]. Signal Processing, 2007:1537-1541.

[17] Jafarnia-Jahromi 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, 3(4):181-191.

[18] Wen H, Huang P, Dyer J, et al. Countermeasures for GPS Signal Spoofing[C]. Proceedings of the 18th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2005), Long Beach, CA, USA, 2005:1285-1290.

[19] Pini M, Fantino M, Cavaleri A, 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 (ION GNSS 2011), Portland, OR, USA, 2011:1888-1896.

[20] Dovis F, Chen X, Cavaleri A, et al. Detection of Spoofing Threats by Means of Signal Parameters Estimation[C]. Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011), Portland, OR, USA, 2011:416-421.

[21] Wesson K, Shepard D, Bhatti J. An Evaluation of the Vestigial Signal Defense for Civil GPS Anti-Spoofing[C]. Proceedings of the 24th International Technical0 Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011), Portland, OR, USA, 2011:2646-2656.

[22] Akos D. Who’s Afraid of the Spoofer? GPS/GNSS Spoofing Detection via Automatic Gain Control[J]. Navigation, 2012, 59(4):281-290.

[23] Wang Q, Li H, Lu M Q. Residual Vector Analysis Method (RVAM) for Evaluating the Performance of GNSS Part of Channels’ Replay Attacks[C]. IEEE China Summit & International Conference on Signal and Information Processing, Beijing, CHN, 2013:561-565.

[24] Psiaki M, Powell S, O'Hanlon B. GNSS Spoofing Detection Using High-Frequency Antenna Motion and Carrier-Phase Data[C]. Proceedings of the 26th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2013), Nashville, TN, USA, 2013:2949-2991.

[25] Psiaki M, Powell S, B. O'Hanlon. GNSS Spoofing Detection, Correlating

Carrier Phase with Rapid Antenna Motion[J]. GPS World, 2013, 24(6):53-58.

[26] Nielsen J, Broumandan A, Lachapelle G. GNSS Spoofing Detection for Single Antenna Handheld Receivers[J]. Navigation, 2012, 58(4):335-344.

[27] 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 (ION GNSS 2012), Nashville, TN, USA, 2012:1233-1243.

[28] Konovaltsev A, Cuntz M, Haettich C, et al. Performance Analysis of Joint Multi-Antenna Spoofing Detection and Attitude Estimation[C]. Proceedings of the 2013 International Technical Meeting of The Institute of Navigation, Nashville, TN, USA, 2013:864-872.

[29] Swaszek P, Hartnett R. Spoof Detection Using Multiple COTS Receivers in Safety Critical Applications[C]. Proceedings of the 26th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2013), Nashville, TN, USA, 2013:2921-2930.

[30] Montgomery P, Humphreys T. Receiver-autonomous Spoofing Detection: Experimental Results of a Multi-antenna Receiver Defense Against a Portable Civil GPS Spoofer[C]. Proceedings of the Institute of Navigation International Technical Meeting (ITM' 09), Anaheim, CA, USA, 2009:124-130.

[31] Psiaki M, O'Hanlon B, Bhatti J, et al. GPS Spoofing Detection via Dual-Receiver Correlation of Military Signals[J]. IEEE Transactions on Aerospace and Electronic Systems, 2013, 49(4):2250-2267.

[32] Nielsen J. Method and System for Detecting GNSS Spoofing Signals[P]. 2011, US patent, No. 7952519.

[33] Jafarnia-Jahromi A, Lin T, Broumandan A, et al. Detection and Mitigation of Spoofing Attack on a Vector Based Tracking GPS Receiver[C]. Proceedings of the International Technical Meeting of The Institute of Navigation, Newport Beach, CA, USA, 2012:790-800.

[34] Cheng X, Xu J, Cao K, et al. An Authenticity Verification Scheme Based on Hidden Messages for Current Civilian GPS Signals[C]. Proceedings of the 4th

International Conference on Computer Sciences and Convergence Information Technology (ICCIT' 09), Seoul, KOR, 2009:345-352.

[35] Humphreys T, Bhatti J, Shepard D, et al. The Texas Spoofing Test Battery: Toward a Standard for Evaluating GPS Signal Authentication Techniques[C]. Proceedings of the 25th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2012), Nashville, TN, USA, 2012:3569-3583.

[36] Wesson K, Rothlisberger M, Humphreys T. A Proposed Navigation Message Authentication Implementation for Civil GPS Anti-Spoofing[C]. Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011), Portland, OR, USA, 2011:3129-3140.

[37] Moon G, Im S H, Jee G I. A Civil GPS Anti-Spoofing and Recovering Method Using Multiple Tracking Loops and an Adaptive Filter Technique[C]. Proceedings of the 26th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2013), Nashville, TN, USA, 2013:2916-2920.

[38] Konovaltsev A, Cuntz M, Haettich C, et al. Autonomous Spoofing Detection and Mitigation in a GNSS Receiver with an Adaptive Antenna Array[C]. Proceedings of the 26th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2013), Nashville, TN, USA, 2013:2937-2948.

[39] McDowell C. GPS Spoofer and Repeater Mitigation System Using Digital Spatial Nulling[P]. 2007, US Patent, No.7250903.

[40] Daneshmand S, Jafarnia-Jahromi A, Broumandan A et al. Low-Complexity Spoofing Mitigation[J]. GPS World, 2011, 22(12):44-46.