一种面向商用接收机的 GNSS 欺骗干扰源测向方法

王仲潇^{1,2}, 李洪^{1,2*}, 周子恒^{1,2}, 陆明泉^{1,2}

1. 清华大学电子工程系, 北京 100084

2. 北京信息科学与技术国家研究中心, 北京 100084

* 通信作者. E-mail: lihongee@tsinghua.edu.cn

收稿日期: 2021-11-30; 修回日期: 2021-12-30; 接受日期: 2022-02-21; 网络出版日期: 2022-03-29

国家自然科学基金 (批准号: 61973181) 和清华大学自主科研项目 (批准号: 2018Z05JZY004) 资助

摘要 随着全球导航卫星系统 (global navigation satellite system, GNSS) 应用的日益广泛和欺骗攻击威胁的日益加剧, 针对商用接收机开展反欺骗研究是十分必要和迫切的. 本文提出了一种面向商用接收机的 GNSS 欺骗干扰源测向方法. 该方法利用水平面内运动接收机提供的多普勒 (Doppler) 观测量和钟漂解算信息构造双差观测量, 计算提取了由接收机运动产生的多普勒信息, 并利用该信息实现欺骗干扰源测向. 本文给出了欺骗源方位角和仰角测量的最大似然估计 (maximum likelihood estimation, MLE) 方法, 推导了克拉美罗下界 (Cramer-Rao lower bound, CRLB), 分析了影响角度估计性能的因素, 并通过外场试验验证了所提方法的有效性.

关键词 全球导航卫星系统, 欺骗攻击, 波达方向, 多普勒, 最大似然估计

1 引言

全球导航卫星系统 (global navigation satellite system, GNSS) 作为信息社会重要的基础设施, 为用户提供全天候、全天时的定位、测速和授时 (position, velocity and time, PVT) 服务, 在交通、通信、电子、金融和国防等诸多领域都有着广泛的应用. 但是近年来, GNSS 的安全性问题越发引起人们的关注和重视. 由于 GNSS 信号到达地面时的功率很低以及民用信号结构公开等原因, GNSS 容易遭受压制干扰 (jamming) 和欺骗攻击 (spoofing) 威胁, 因此存在巨大安全隐患^[1]. 不同于压制干扰使得 GNSS 丧失 PVT 功能, 欺骗干扰通过自主生成或者转发等手段播发与真实 GNSS 信号相似的欺骗信号, 可以在难以察觉的情况下让用户输出错误的 PVT 结果, 其危害性不言而喻. 事实上, 早在 2011 年

引用格式: 王仲潇, 李洪, 周子恒, 等. 一种面向商用接收机的 GNSS 欺骗干扰源测向方法. 中国科学: 信息科学, 2022, 52: 658–674, doi: 10.1360/SSI-2021-0399
Wang Z X, Li H, Zhou Z H, et al. A direction finding method of the GNSS spoofer for commercial receivers (in Chinese). Sci Sin Inform, 2022, 52: 658–674, doi: 10.1360/SSI-2021-0399

图1 (网络版彩图) GNSS 反欺骗处理流程图

Figure 1 (Color online) Scheme of GNSS anti-spoofing process

伊朗就宣称通过欺骗攻击手段俘获了美军的无人侦察机¹⁾; 德克萨斯大学 (University of Texas System) 的 Humphreys 团队^[2] 在 2014 年开展了欺骗攻击试验, 成功使游艇偏离了预定航线; 而近年来针对船舶、车辆和小型无人机等民用设备的欺骗攻击事件也越来越多地映入我们的眼帘^[3]。

面对日益严重的欺骗攻击威胁, 反欺骗技术研究应运而生。如图 1 所示, GNSS 反欺骗处理流程可以概括为欺骗检测、欺骗识别、欺骗抑制和欺骗源定位 4 个层次^[4]。其中, 欺骗检测和识别技术主要通过信号加密认证^[5,6]、惯性器件和高精度时钟等外部设备辅助^[7,8]、接收机终端信号信息处理^[9~11]等方式, 检测当前电磁环境是否存在欺骗信号, 并对真实信号和欺骗信号加以区分。欺骗抑制技术是在识别欺骗信号的基础上, 通过多天线波束调零或接收机多峰捕获跟踪等方式抑制欺骗信号的影响, 只接收处理真实信号从而为用户恢复正常的 PVT 功能^[12]。而欺骗源定位技术则是在以上 3 个层次基础之上, 通过挖掘欺骗信号的信号层、信息层特征, 反向测量欺骗源方位或位置^[13,14], 为从源头上消除欺骗干扰威胁提供了可能。

针对不同的用户接收机和应用场景, 反欺骗的技术路径各不相同。对于市面上应用广泛的智能手机、车载 GNSS 终端等商用接收机, 由于其硬件结构难以更改, 反欺骗处理只能从接收机提供的 GNSS 原始观测量入手, 这些观测量主要包括接收信号的伪距、多普勒 (Doppler)、载波相位和载噪比等。相比高速率的原始采样信号, 接收机输出观测量的数据率要低很多 (通常不高于 10 Hz), 能够利用的信息量较少, 开展反欺骗研究的难度较大。目前, 文献 [15] 提出的方法可以处理两个独立接收机 (如智能手机) 的伪距观测量, 实现欺骗信号的检测和识别; 文献 [16] 利用了运动接收机的多普勒观测量也实现了上述功能, 同时降低了接收机之间的时间同步要求。目前利用 GNSS 观测量的反欺骗研究还没有在测向和定位问题上更进一步。现有的欺骗源测向技术仍然停留在传统阵列信号处理的框架内, 需要利用多天线阵元或运动天线合成孔径的方式进行波达方向 (direction of arrival, DOA) 估计^[17~20], 通过欺骗信号到达不同天线阵元的载波相位差计算欺骗源的方位。但是, 对于一般只配备单一接收天线的商用接收机来说, 上述欺骗源测向技术将不再适用。

针对以上挑战, 本文提出了一种面向商用接收机的 GNSS 欺骗干扰源测向方法。本文考虑目前最为常见的静止欺骗源单一天线播发欺骗信号的场景, 在欺骗检测和识别的基础上, 利用商用接收机在

1) Peterson S, Faramarzi P. Exclusive: Iran hijacked US drone, says Iranian engineer. 2011. <http://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer>.

运动过程中收集的多普勒观测量和 PVT 解算信息构造双差, 消除欺骗信号本身包含的多普勒分量, 获得了仅由接收机运动产生的多普勒分量, 并将其与欺骗源方位角和仰角建立联系, 以此实现欺骗信号的 DOA 估计. 与 MUSIC, ESPRIT 等使用载波相位的传统 DOA 估计方法^[21]不同, 本文提出的多普勒测向方法无需为每个用户配置多个天线阵元, 仅需两个单天线用户相互配合即可实现欺骗源测向, 因此更加适用于当前已得到广泛应用的单天线商用接收机. 本文利用两个商用 U-Blox 接收机开展了对静止欺骗源测向的试验测试, 实测结果表明在接收机速率大于 0.5 m/s、观测时长大于 10 s 的情况下, 欺骗源方位角和仰角的估计精度可以达到 4° 以内.

本文的后续章节安排如下: 第 2 节建立接收机终端的多普勒和 DOA 观测模型. 第 3 节介绍多普勒频偏的双差计算和 DOA 估计的最大似然估计 (maximum likelihood estimation, MLE) 算法. 第 4 节推导测向误差的克拉美罗下界 (Cramer-Rao lower bound, CRLB) 并结合数值仿真分析影响角度估计性能的因素. 第 5 节给出外场试验测试结果. 第 6 节讨论未来可以进一步开展的工作. 第 7 节对本文研究内容进行总结.

2 系统模型

2.1 DOA 观测模型

多普勒频偏 f_d 源自信号发射源和用户接收机的相对运动, 在数值上正比于相对运动速度在信号来波方向上的投影, 即

$$f_d = \frac{1}{\lambda} \mathbf{v}^T \mathbf{l}, \quad (1)$$

其中 λ 是与信号发射频率相对应的信号波长, $\mathbf{v} = [v_x, v_y, v_z]^T$ 是三维的相对速度, $\mathbf{l}$ 是单位方向矢量. 如图 2 所示, 以接收机为原点建立东北天 (east-north-up, ENU) 坐标系, 单位方向矢量可以表示为

$$\mathbf{l} = [\cos \theta \cos \phi, \sin \theta \cos \phi, \sin \phi]^T, \quad (2)$$

其中 θ 和 ϕ 分别是信号源相对接收机的方位角和仰角. 这样由式 (1) 可得以下 DOA 观测方程:

$$f_d = \frac{1}{\lambda} (v_x \cos \theta \cos \phi + v_y \sin \theta \cos \phi + v_z \sin \phi). \quad (3)$$

在图 1 给出的反欺骗架构中, 接收机在实现欺骗检测、识别和抑制后, 可以将真实信号和欺骗信号分组解算, 输出自身正确的定速结果, 从而建立起多普勒频偏 f_d 和 DOA 参数的定量关系.

2.2 多普勒观测模型

用 $\mathbf{v}^{(i)}$ 和 $\mathbf{v}_r$ 分别表示信号发射源和用户接收机的速度, 可以根据速度来源的不同将式 (1) 的多普勒频偏拆分为两部分:

$$f_d = \frac{1}{\lambda} (\mathbf{v}_r - \mathbf{v}^{(i)})^T \mathbf{l}_r^{(i)} = \frac{1}{\lambda} \mathbf{v}_r^T \mathbf{l}_r^{(i)} - \frac{1}{\lambda} \mathbf{v}^{(i)T} \mathbf{l}_r^{(i)}, \quad (4)$$

$$f^{(i)} = -\frac{1}{\lambda} \mathbf{v}^{(i)T} \mathbf{l}_r^{(i)}, \quad f_r = \frac{1}{\lambda} \mathbf{v}_r^T \mathbf{l}_r^{(i)}, \quad (5)$$

其中 $f^{(i)}$ 和 f_r 分别定义为源多普勒 (source Doppler) 和用户多普勒 (receiver Doppler).

GNSS 接收机的多普勒观测量除了以上两个主要来源, 还包含了时钟频漂等非理想因素, 其观测方程可以由伪距和伪距率观测方程推导得到^[16]. 无论欺骗信号还是真实信号, 第 n 时刻编号为 r 的

图2 (网络版彩图) DOA 观测模型

Figure 2 (Color online) Observation model of DOA

接收机对编号为 \$(i)\$ 的卫星信号的多普勒观测方程都可以统一表示为

$$f[n] = f^{(i)}[n] - \delta f^{(i)}[n] + f_r[n] + \delta f_r[n] + \delta f_{r_0} + \varepsilon_{f^{(i)}}[n], \quad (6)$$

其中,

- $f^{(i)}[n]$ 是源多普勒, 是由信号发射源运动产生的多普勒频偏. 对于真实信号而言, 其来源就是真实卫星的运动; 而对于欺骗信号而言, 其来源有两方面——欺骗信号模拟的卫星运动以及欺骗源自身的运动.

- $f_r[n]$ 是用户多普勒, 是由用户接收机运动产生的多普勒频偏.
- $\delta f^{(i)}[n]$ 表示卫星和欺骗源的时钟频漂.
- $\delta f_r[n]$ 表示接收机的时钟频漂.
- δf_{r_0} 表示接收机下变频器中心频点与信号源发射频点的固有偏差, 通常可以看作一个常数.
- $\varepsilon_{f^{(i)}}[n]$ 是多普勒观测噪声, 包含了对流层和电离层延时变化率等因素的影响. 为了后续推导方便, 不妨将其建模为均值为 0 方差为 $\sigma_{f^{(i)}}^2$ 的高斯 (Gauss) 白噪声.

对于静止的欺骗源, 2.1 小节用于 DOA 估计的多普勒频偏即为用户多普勒, 即 $f_d[n] = f_r[n]$. 从总的多普勒观测测量中提取用户多普勒需要首先排除时钟频漂等因素的影响.

2.3 时钟频漂观测模型

本小节对接收机的时钟频漂进行建模. 考虑接收机 PVT 输出的钟漂解算结果 t_i , 该物理量反映了所有参与定位解算的信号从发射到接收所经历的公共传输时延变化率. 由于不同卫星播发的真实信号到达用户接收机的路径不尽相同, 真实信号的公共传输时延变化率主要来自接收机时钟频漂. 所以真实信号 PVT 解算得到的钟漂结果可以表示为

$$\dot{t}_a[n] = \frac{\lambda}{c}(\delta f_r[n] + \varepsilon_t[n]). \quad (7)$$

其中 c 是信号传播速度. $\varepsilon_t[n]$ 是钟漂解算误差, 同样为了讨论方便将其建模为均值为 0、方差为 σ_t^2 的高斯白噪声. 对于本文考虑的静止欺骗源集中式欺骗攻击, 由于欺骗信号由同一个天线播发, 不同欺骗信号到达用户接收机的方向矢量是相同的, 接收机运动同样对公共传输时延变化率产生影响. 因此

图 3 (网络版彩图) 从用户接收机提取观测测量

Figure 3 (Color online) Extracting measurements from receivers

欺骗信号 PVT 解算得到的钟漂结果还包含了用户多普勒 $f_r[n]$, 即

$$\dot{t}_s[n] = \frac{\lambda}{c}(f_r[n] + \delta f_r[n] + \varepsilon_i[n]). \quad (8)$$

3 测向算法

3.1 多普勒频偏的双差计算

完整的欺骗源测向算法需要用到两个单天线接收机, 如图 3 所示. 接收机 R_1 和 R_2 同时接收来自同一个静止欺骗源 Spoofing 的欺骗信号. 其中 R_1 为参考接收机, 其作用是为用户提供差分观测测量, 可以位于能够接收到欺骗信号的任意位置, 静止或运动状态均可; R_2 为用户接收机, 需通过主动运动产生用户多普勒分量, 并以此测量欺骗源相对自身的方位. 下面利用两个接收机的多普勒观测测量和钟漂解算结果构造双差, 计算用于 DOA 估计的多普勒频偏. 计算双差需要用到的物理量如下:

- 接收机 R_1 和 R_2 各自对第 (i) 个欺骗信号的多普勒观测矢量 $\mathbf{f}_1^{(i)}$ 和 $\mathbf{f}_2^{(i)}$,
- 接收机 R_1 用欺骗信号解算得到的钟漂矢量 $\frac{c}{\lambda}\dot{\mathbf{t}}_1$,
- 接收机 R_2 用真实信号解算得到的钟漂矢量 $\frac{c}{\lambda}\dot{\mathbf{t}}_2$,

其中, $\mathbf{f}_r^{(i)} = [f_r^{(i)}[1], f_r^{(i)}[2], \dots, f_r^{(i)}[N]]^T$, $\frac{c}{\lambda}\dot{\mathbf{t}}_r = \frac{c}{\lambda}[\dot{t}_r[1], \dot{t}_r[2], \dots, \dot{t}_r[N]]^T$, $i = 1, 2, \dots, M$, $r = 1, 2$.

首先定义每个接收机输出的单差. 单差的目的是消除接收机时钟频漂, 本文将定义为多普勒观测测量和钟漂解算结果的差分. 接收机 R_1 的单差为

$$\Delta \mathbf{f}_1^{(i)} = \mathbf{f}_1^{(i)} - \frac{c}{\lambda}\dot{\mathbf{t}}_1. \quad (9)$$

根据式 (6) 和 (8) 可得

$$\Delta f_1^{(i)}[n] \sim \mathcal{N}(f^{(i)}[n] - \delta f^{(i)}[n] + \delta f_{10}, \sigma_{f_1^{(i)}}^2 + \sigma_{t_1}^2), \quad n = 1, 2, \dots, N. \quad (10)$$

接收机 R_1 输出的单差 $\Delta f_1^{(i)}$ 是对第 (i) 颗欺骗信号源多普勒和欺骗源钟漂的有效观测. 同理定义接收机 R_2 的单差

$$\Delta f_2^{(i)} = f_2^{(i)} - \frac{c}{\lambda} \dot{t}_2, \quad (11)$$

$$\Delta f_2^{(i)}[n] \sim \mathcal{N}(f^{(i)}[n] - \delta f^{(i)}[n] + f_2[n] + \delta f_{20}, \sigma_{f_2^{(i)}}^2 + \sigma_{t_2}^2), \quad n = 1, 2, \dots, N. \quad (12)$$

接收机 R_2 的单差 $\Delta f_2^{(i)}$ 不仅包含了对第 (i) 颗欺骗信号的源多普勒和欺骗源钟漂, 还包含了接收机 R_2 运动产生的用户多普勒.

用于 DOA 估计的多普勒频偏可由两个接收机的单差再次差分得到. 综合式 (10) 和 (12), Q 维多普勒频偏表示为以下双差形式:

$$\mathbf{f}_d = \mathbf{e} \otimes (\Delta \mathbf{f}_2^{(i)} - \Delta \mathbf{f}_1^{(i)}), \quad (13)$$

其中 $Q = M \times N$, $\otimes$ 表示 Kronecker 积, $\mathbf{e}$ 是 $M \times 1$ 的全 1 列向量. 且有

$$\mathbf{f}_d \sim \mathcal{N}(\mathbf{u}(\mathbf{f}_d), \mathbf{C}), \quad (14)$$

其中多普勒观测量的均值 $\mathbf{u}(\mathbf{f}_d) = \mathbf{e} \otimes (\mathbf{f}_r + \delta f_{20} - \delta f_{10})$, 协方差矩阵 $\mathbf{C} = \mathbf{I}_N \otimes \mathbf{\Lambda}_M$. $\mathbf{f}_r = [f_r[1], f_r[2], \dots, f_r[N]]^T$, $\mathbf{I}_N$ 表示 N 阶单位矩阵, $\mathbf{\Lambda}_M$ 是 M 阶对角矩阵, $\mathbf{\Lambda}_M = \text{diag}(\sigma_1^2, \sigma_2^2, \dots, \sigma_M^2)$, $\sigma_i^2 = \sigma_{f_1^{(i)}}^2 + \sigma_{t_1}^2 + \sigma_{f_2^{(i)}}^2 + \sigma_{t_2}^2, i = 1, 2, \dots, M$.

3.2 DOA 参数的 MLE

为了算法实现方便, 本文将接收机 R_2 的运动限制在水平方向上, 并令其在东向和北向对应的 Q 维速度矢量分别为 $\mathbf{v}_x$ 和 $\mathbf{v}_y$. 根据式 (3), 多普勒频偏与欺骗信号 DOA 具有如下关系:

$$\mathbf{u}(\mathbf{f}_d) = \frac{1}{\lambda} (\mathbf{v}_x \cos \theta \cos \phi + \mathbf{v}_y \sin \theta \cos \phi) + \delta f_{20} - \delta f_{10}, \quad (15)$$

其中接收机固有频差项 $\delta f_{20} - \delta f_{10}$ 是不随速度和时间变化的常数, 可在 $\mathbf{v}_x = \mathbf{v}_y = \mathbf{0}$ 即接收机 R_2 静止时对多普勒频偏长时间观测获得, 为了接下来讨论方便可将其视为已知量. 除去固有频差的影响, 多普勒频偏可以表示为

$$\tilde{\mathbf{u}}(\mathbf{f}_d) = \mathbf{u}(\mathbf{f}_d) - (\delta f_{20} - \delta f_{10}) = \frac{1}{\lambda} (\mathbf{v}_x \cos \theta \cos \phi + \mathbf{v}_y \sin \theta \cos \phi), \quad (16)$$

其中方位角 θ 和仰角 ϕ 是待估计参数, 其似然函数为

$$p(\mathbf{f}_d | \alpha, \beta) = \frac{1}{\sqrt{(2\pi)^Q |\mathbf{C}|}} \exp \left(-\frac{1}{2} (\mathbf{f}_d - \tilde{\mathbf{u}}(\mathbf{f}_d))^T \mathbf{C}^{-1} (\mathbf{f}_d - \tilde{\mathbf{u}}(\mathbf{f}_d)) \right), \quad (17)$$

对应的代价函数是

$$J(\theta, \phi) = (\mathbf{f}_d - \tilde{\mathbf{u}}(\mathbf{f}_d))^T \mathbf{C}^{-1} (\mathbf{f}_d - \tilde{\mathbf{u}}(\mathbf{f}_d)). \quad (18)$$

为了求解方便, 进行如下——变换:

$$\alpha = \frac{1}{\lambda} \cos \theta \cos \phi, \quad (19)$$

$$\beta = \frac{1}{\lambda} \sin \theta \cos \phi. \quad (20)$$

其逆变换为

$$\theta = \arctan \left(\frac{\beta}{\alpha} \right), \quad (21)$$

$$\phi = \arccos (\lambda \sqrt{\alpha^2 + \beta^2}). \quad (22)$$

于是, 式 (17) 的代价函数可以写为

$$\begin{aligned} J(\alpha, \beta) &= (\mathbf{f}_d - \alpha \mathbf{v}_x - \beta \mathbf{v}_y)^T \mathbf{C}^{-1} (\mathbf{f}_d - \alpha \mathbf{v}_x - \beta \mathbf{v}_y) \\ &= (\mathbf{f}_d - \mathbf{H}\Theta)^T \mathbf{C}^{-1} (\mathbf{f}_d - \mathbf{H}\Theta), \end{aligned} \quad (23)$$

其中 $\Theta = [\alpha, \beta]^T$, $\mathbf{H} = [\mathbf{v}_x, \mathbf{v}_y]$. 最小化该代价函数的解为

$$\hat{\Theta} = [\hat{\alpha}, \hat{\beta}]^T = (\mathbf{H}^T \mathbf{C}^{-1} \mathbf{H})^{-1} \mathbf{H}^T \mathbf{C}^{-1} \mathbf{f}_d. \quad (24)$$

根据 MLE 参数变换的不变性, 最终可得到 DOA 参数的 MLE:

$$\hat{\theta} = \arctan \left(\frac{\hat{\beta}}{\hat{\alpha}} \right), \quad (25)$$

$$\hat{\phi} = \arccos \left(\lambda \sqrt{\hat{\alpha}^2 + \hat{\beta}^2} \right). \quad (26)$$

4 性能评估

4.1 DOA 估计的 CRLB

根据 MLE 的渐近有效性, 可以利用 CRLB 评估 DOA 参数的估计性能. 为了求解需要, 首先考察中间参数 Θ 的 CRLB. 根据式 (23), 参数 Θ 和观测数据 $\mathbf{f}_d$ 之间构成线性模型, 因此在观测噪声符合独立高斯分布的情况下, $\hat{\Theta}$ 是最小方差无偏 (minimum variance unbiased, MVU) 估计量且能够达到 CRLB^[22], CRLB 由其 Fisher 信息矩阵 $\mathbf{I}(\Theta)$ 求逆后的对角线元素给出. 这里有

$$\mathbf{I}^{-1}(\Theta) = (\mathbf{H}^T \mathbf{C}^{-1} \mathbf{H})^{-1}. \quad (27)$$

为了能够更直观地分析影响 DOA 参数估计性能的因素, 这里对噪声方差模型进一步简化. 在 2.2 小节中曾假设接收机对第 (i) 颗卫星信号的多普勒观测量的噪声方差 $\sigma_{f^{(i)}}^2$ 不随时间变化, 现在我们进一步假设接收机对不同卫星信号的多普勒观测量具有相同的噪声方差, 即 $\sigma_{f^{(i)}}^2 = \sigma_{f^{(j)}}^2 \triangleq \sigma_f^2$, $i, j \in \{1, 2, \dots, M\}$. 这样多普勒频偏 $\mathbf{f}_d$ 的协方差矩阵 $\mathbf{C}$ 便可简化为数量矩阵 $\sigma^2 \mathbf{I}_Q$, 其中 $\sigma^2 = \sigma_{f_1}^2 + \sigma_{t_1}^2 + \sigma_{f_2}^2 + \sigma_{t_2}^2$. 故式 (27) 中 Fisher 信息矩阵的逆矩阵可以展开为

$$\begin{aligned} \mathbf{I}^{-1}(\Theta) &= \sigma^2 \begin{bmatrix} \mathbf{v}_x^T \mathbf{v}_x & \mathbf{v}_x^T \mathbf{v}_y \\ \mathbf{v}_y^T \mathbf{v}_x & \mathbf{v}_y^T \mathbf{v}_y \end{bmatrix}^{-1} \\ &= \frac{\sigma^2}{\sum v_{xi}^2 \sum v_{yi}^2 (1 - \rho)} \begin{bmatrix} \sum v_{yi}^2 & -\sum v_{xi} v_{yi} \\ -\sum v_{xi} v_{yi} & \sum v_{xi}^2 \end{bmatrix}, \end{aligned} \quad (28)$$

表 1 蒙特卡洛仿真参数设置

Table 1 Parameter settings of Monte Carlo simulations

Case	Corresponding figure	Noise (Hz)	Data length	Velocity (m/s)	Direction of speed	Azimuth of spoofer (°)	Elevation of spoofer (°)
1	Figure 4	1	10, 20, 50, 100, 200, 500, 1000	2	0° and 90°	45	45
2	Figure 5	1	100	0.5, 1, 2, 5, 10, 15, 20	0° and 90°	45	45
3	Figure 6	1	200	2	6 sets of direction referring to Figure 7	45	45
4	Figure 8	1	50	2	0° and 90°	45	5, 15, 25, 35, 45, 55, 65, 75, 85

其中 $\rho = \frac{(\sum v_{xi}v_{yi})^2}{\sum v_{xi}^2 \sum v_{yi}^2}$, $\sum \triangleq \sum_{i=1}^Q$.

式 (18) 和 (19) 中参数变换的雅可比 (Jacobi) 矩阵为

$$\mathbf{J} = \begin{bmatrix} \frac{\partial \theta}{\partial \alpha} & \frac{\partial \theta}{\partial \beta} \\ \frac{\partial \phi}{\partial \alpha} & \frac{\partial \phi}{\partial \beta} \end{bmatrix} = \begin{bmatrix} \frac{-\lambda \sin \theta}{\cos \theta} & \frac{\lambda \cos \theta}{\cos \phi} \\ \frac{-\lambda \cos \theta}{\sin \phi} & \frac{-\lambda \sin \theta}{\sin \phi} \end{bmatrix}. \quad (29)$$

所以, 方位角和仰角估计量的 CRLB 可以由下式最终给出:

$$\begin{aligned} \mathbf{I}^{-1}(\theta, \phi) &= \mathbf{J} \mathbf{I}^{-1}(\Theta) \mathbf{J}^T \\ &= \frac{\sigma^2}{\sum v_{xi}^2 \sum v_{yi}^2 (1 - \rho)} \begin{bmatrix} \frac{\lambda^2}{\cos^2 \phi} \sum |\mathbf{v}_i \cdot \tilde{\mathbf{l}}|^2 & \dots \\ \dots & \frac{\lambda^2}{\sin^2 \phi} \sum |\mathbf{v}_i \times \tilde{\mathbf{l}}|^2 \end{bmatrix}, \end{aligned} \quad (30)$$

其中 $\tilde{\mathbf{l}} = [\cos \theta, \sin \theta]^T$ 为欺骗信号的方位矢量 (方向矢量 $\mathbf{l}$ 在水平面的投影), $\mathbf{v}_i = [v_{xi}, v_{yi}]^T$ 是第 i 个样本点的速度矢量.

4.2 性能影响因素分析

下面根据 4.1 小节的 CRLB 推导结果, 结合数值仿真分析影响欺骗信号 DOA 估计精度的因素.

观测噪声. 即式 (30) 中的 σ^2 , 由接收机的欺骗信号多普勒测量噪声和钟漂解算误差两部分构成. 观测噪声方差越小, DOA 估计精度越高. 主要由信号质量、传输路径和接收机跟踪环路性能等因素决定. 事实上, 接收机输出的多普勒观测量具有很高的精度, 往往比伪距观测量低一至两个数量级^[23], 对应的钟漂解算结果也比授时结果更精确. 在本文第 5 节的外场试验中, 测量噪声大约在 1 Hz 范围以内, 对 DOA 估计精度的影响很小.

数据长度. 由于式 (19) 和 (20) 的参数变换是非线性的, MLE 的最终结果 $\hat{\theta}$ 和 $\hat{\phi}$ 并不是有效估计量. 但是由于 MLE 具有渐近有效性, 随着数据长度增大, MLE 可以逐渐逼近 CRLB. 图 4 中的箱形图给出了不同数据长度下 1000 次蒙特卡洛 (Monte Carlo) 仿真方位角和仰角估计误差绝对值的统计分布情况 (其他仿真参数的设置详见表 1, 下同). 图 4 中橙色点划线是根据式 (30) 计算的 CRLB, 反映了 DOA 参数估计理论上能够达到的最好性能. 从仿真结果可以看到, 当数据量较少时, 由于 MLE 求解涉及了反三角函数等非线性运算, 估计误差距离理论最优下界存在较大差距. 但是当参与估计的数据长度逐渐增加后, 由于 MLE 的渐进有效性, 参数估计精度得到改善, 估计误差也逐渐逼近 CRLB.

接收机运动速率. 在式 (30) 中体现为求和项 $\sum v_{xi}^2 \sum v_{yi}^2$. 高度运动下的多普勒效应更加显著, 因此无论是东向速度还是北向速度, 接收机运动速率的增加都能显著提高估计性能. 图 5 给出了不同接

图 4 不同数据长度下蒙特卡洛仿真方位角 (a) 和仰角 (b) 估计误差的统计分布

Figure 4 Statistical distribution of estimation errors for both azimuth (a) and elevation (b) in 1000 times Monte Carlo simulation under different data lengths

图 5 不同接收机运动速率下蒙特卡洛仿真方位角 (a) 和仰角 (b) 估计误差的统计分布

Figure 5 Statistical distribution of estimation errors for both azimuth (a) and elevation (b) in 1000 times Monte Carlo simulation under different velocities

收机运动速率下 DOA 估计误差的仿真结果. 从仿真结果可以看到, 当接收机运动速率达到 1 m/s 及以上时, 方位角和仰角的估计误差能够控制在约 4° 范围内.

接收机运动方向. 同时实现方位角和仰角的二维参数估计需要接收机提供至少不同运动方向的观测信息. 不妨将式 (28) 中的参数 ρ 定义为接收机速度方向的“相关系数”. $\rho = 1$ 意味着各个时刻的速度方向“完全相关”, 此时接收机只沿单一方向运动, CRLB 趋于无穷大. 正如图 6 第 3 组实验的仿真结果, 接收机运动方向集中在方位角 90° 附近 (接收机运动方向示意图如图 7 所示), 此时方位角和仰角估计都出现了较大的误差; 而在第 1 和 2 组实验中, 接收机分别沿方位角 0° 和 90° 以及 45° 和 135° 两个正交方向运动, 能够提供两个不同方向的观测量, 此时方位角和仰角估计误差控制在较低水平.

接收机运动方向对方位角和仰角的影响也存在差异性, 体现在式 (30) 的矩阵对角线元素上. 当接收机运动方向与欺骗信号方位矢量平行时, 多普勒频偏达到极值点, 多普勒对方位角的变化率为 0, 方位角估计误差达到极大值 (如图 6 第 5 组实验所示). 而仰角的估计与之相反, 当接收机运动方向与欺骗信号方位矢量垂直时, 任意仰角下的多普勒频偏都在 0 附近波动, 仰角估计误差达到极大值 (如图 6 第 4 组实验所示).

欺骗源仰角. 欺骗源本身仰角的高低对估计性能的影响, 同样体现在式 (30) 矩阵的对角线元素上. 如图 8 仿真结果所示, 欺骗源仰角较低时仰角的估计误差较大, 而欺骗源仰角较高时方位角的估

图 6 不同接收机运动方向下蒙特卡洛仿真方位角 (a) 和仰角 (b) 估计误差的统计分布

Figure 6 Statistical distribution of estimation errors for both azimuth (a) and elevation (b) in 1000 times Monte Carlo simulation under different speed directions

图 7 图 6 每组仿真的接收机运动方向示意图. 第 1 组, 方位角 0° 和 90° 附近的直线运动; 第 2 组, 方位角 45° 和 135° 附近的直线运动; 第 3 组, 方位角 90° 附近的直线运动; 第 4 组, 方位角 135° 附近的直线运动; 第 5 组, 方位角 45° 附近的直线运动; 第 6 组, 圆周运动

Figure 7 Directions of the velocity of each set in Figure 6. Set 1, linear motion azimuth near 0° and 90° ; set 2, linear motion azimuth near 45° and 135° ; set 3, linear motion azimuth near 90° ; set 4, linear motion azimuth near 135° ; set 5, linear motion azimuth near 45° ; set 6: circular motion

计误差较大, 其本质原因与接收机运动方向的影响分析相同, 这里不再赘述.

5 试验验证

5.1 场景设置

我们开展了外场试验对本文提出的欺骗源测向方法进行验证. 试验场景设置如图 9 所示.

图 8 不同欺骗源仰角下蒙特卡洛仿真方位角 (a) 和仰角 (b) 估计误差的统计分布

Figure 8 Statistical distribution of estimation errors for both azimuth (a) and elevation (b) in 1000 times Monte Carlo simulation under different spoofer elevations

图 9 外场试验场景设置

Figure 9 Experimental configuration

- 试验地点在清华大学伟清楼天台。
- 使用清华大学卫星导航实验室的 GNSS 欺骗源模拟器生成一段 GPS 欺骗信号, 并通过架设在天台高处的螺旋天线定向播发。欺骗信号的功率事先被调整到合适的范围内, 使其作用范围局限在天台上, 避免对其他用户造成干扰。
- 两个 U-Blox 商用接收机, 各自连接一个普通商用 GPS 天线接收欺骗信号, 同时将多普勒观测测量和 PVT 解算结果传输至 PC, 数据率为 10 Hz。两个接收机一个静止, 另一个则主动运动产生多普勒以实现对欺骗信号 DOA 的观测。试验过程中, 接收机多普勒观测噪声的标准差约为 0.5 Hz。

下面考虑试验中可行的接收机运动模式。4.2 小节曾得出结论: DOA 估计需要接收机在至少两个水平方向上运动; 且为了实现更好的估计精度, 运动方向应尽可能避免与接收机方位矢量平行或垂直。综上考虑, 旋转运动能够让接收机在多个不同的水平方向上提供观测测量, 是实现欺骗源测向的理想选择。在 4.2 小节图 6 的第 6 组实验中, 我们已经给出了接收机做旋转运动时 DOA 估计误差的仿真结

表 2 试验的方位参数

Table 2 Positions and azimuth parameters of the experiment

Item	Description
Transmitting antenna of the spoofer	[40.0015847 116.3301709 86.867]
Center of the rotating platform	[40.0015100 116.3302245 82.289]
Azimuth	118.89°
Elevation	25.79°

果, 结果表明旋转运动能够同时兼顾方位角和仰角的估计精度. 因此有如下设置:

- 试验中先后通过图 9 所示的半径为 1 m 的旋转平台和手持的方式让接收机进行旋转运动.
- 试验开始前事先标定了欺骗源发射天线位置、旋转中心位置, 其坐标及方位角、仰角如表 2 所示.

5.2 测试结果

首先是接收机多普勒的双差提取结果, 这是 DOA 估计算法的输入量. 正如前文提到的, 接收机多普勒仅由接收机运动产生, 其大小取决于运动速度在接收机到欺骗源方向矢量上的投影. 如图 10(c) 所示, 不同欺骗信号提取的接收机多普勒大致相等并且呈现出与接收机速度相同的变化趋势. 图 10(b) 是接收机输出的欺骗信号总多普勒观测量, 由于叠加了源多普勒的影响, 接收机自身的运动模式在总多普勒中并没有明显的体现. 在本次试验中, 欺骗源将用户欺骗到固定的位置, 所以源多普勒近似随时间缓慢线性变化. 但是在更复杂的欺骗攻击场景中 (如用户被欺骗做圆周运动), 欺骗信号的源多普勒变化将更加复杂, 接收机多普勒无法从单一的接收机观测量中提取. 而式 (15) 提出的差分方法可以无视欺骗攻击策略以及源多普勒的变化, 在各种欺骗攻击场景中都能精确地提取出接收机多普勒, 从而保证了欺骗信号 DOA 估计的顺利进行.

图 11 和 12 给出了不同测试场景下接收机三维速度和接收机多普勒的变化情况, 表 3 和 4 是对应的方位角和仰角的估计结果.

其中图 11 和表 3 的测试在旋转平台上进行, 第 1~3 组测试分别使用了第 400~600, 650~850 和 1075~1175 三个时段的观测数据. 可以看到在第 1 和 2 组测试数据长度相同 (数据长度为 200, 观测时长为 20 s) 的情况下, 具有较大接收机转速的第 2 组测试获得了更小的方位角和仰角估计误差; 而在第 2 和 3 组接收机转速相当的情况下, 第 3 组测试 (数据长度为 100, 观测时长为 10 s) 参与估计的数据长度较短而误差相对较大. 总体来看, 在转台速度大于 0.5 m/s、观测时长不低于 10 s 的情况下, 欺骗源仰角和方位角的估计误差都能被控制在 4° 范围内.

为了模拟商用接收机的真实使用场景, 图 9 中试验者手持接收机天线以自身为轴进行转动, 旋转一圈的时长约为 4.2~4.7 s. 如图 12(a) 所示, 手持旋转时半径较旋转平台更短, 所以产生的线速度较小; 另外由于手持的稳定性较差, 多普勒的观测噪声相对较大. 对于本次试验采用的 U-Blox 接收机, 其观测量输出的最快频率为 10 Hz; 但是对于安卓智能手机, Google GNSSLogger 支持其输出观测量的频率只有 1 Hz²⁾. 因此这里重点考察不同观测量的采样率对 DOA 估计精度的影响. 试验中使用第 350~550 时段的观测数据进行 DOA 估计, 并设置了 1~10 Hz 不等的采样率, 采样率越低对应参与 DOA 估计的数据点数就越少. 测试结果如表 4 所示. 随着采样率降低, 方位角的估计结果波动较小, 估计误差仍在 4° 范围以内; 但是仰角的估计结果出现了较大的波动, 甚至出现了 10° 以上的偏差. 这与图 8 的理论仿真结果是相符的, 本次试验欺骗源本身仰角较低, 需足够的数据点数才能保证足够好

2) <https://developer.android.com/guide/topics/sensors/gnss>.

图 10 接收机多普勒随运动速度变化情况. (a) 接收机三维运动速度; (b) 接收机的总多普勒; (c) 通过差分方法提取的用户多普勒

Figure 10 Variation of Doppler with the velocity of the receiver. (a) Velocity of the receiver; (b) total Doppler; (c) the extracted receiver Doppler by the difference method

图 11 旋转平台试验的 (a) 接收机三维运动速度和 (b) 用户多普勒

Figure 11 Velocity of the receiver (a) and the extracted receiver Doppler (b) in rotating platform test

的仰角估计精度; 而方位角估计性能在低仰角时表现较好, 试验中数据点数的减少对其估计精度影响不大.

6 讨论

本文通过外场实试验验证了所提方法的有效性. 与现有基于阵列信号处理的欺骗源测向方法相比 (如表 5 所示), 本文所提方法可以获得大致相当的 DOA 估计精度, 同时摆脱了矢量跟踪这一复杂接收机结构的束缚, 可以仅依靠 GNSS 观测量实现测向功能, 系统和计算复杂度更小, 可以广泛应用于智能手机等商用接收机. 此外值得注意的是, 本文方法与现有方法一样会受到欺骗源本身仰角的影响,

图 12 手持试验的 (a) 接收机三维运动速度和 (b) 用户多普勒
Figure 12 Velocity of the receiver (a) and the extracted receiver Doppler (b) in handheld test

表 3 旋转平台试验的测试结果
Table 3 Experiment results of rotating platform test

Test sets	Data length	Average speed (m/s)	Estimated azimuth (°)	Azimuth error (°)	Estimated elevation (°)	Elevation error (°)
Set 1	200	0.68	115.93	2.96	29.20	3.41
Set 2	200	1.03	118.99	0.10	24.69	1.10
Set 3	100	1.07	120.69	1.80	28.76	2.97

表 4 手持试验的测试结果
Table 4 Experiment results of handheld test

Test sets	Data rate (Hz)	Data length	Estimated azimuth (°)	Azimuth error (°)	Estimated elevation (°)	Elevation error (°)
Set 1	10	200	117.82	1.07	26.36	0.57
Set 2	5	100	115.06	3.83	19.88	5.91
Set 3	2.5	50	115.79	3.10	14.07	11.72
Set 4	2	40	121.16	2.27	25.89	0.10
Set 5	1	20	120.87	1.98	20.73	5.06

表 5 欺骗源测向方法对比
Table 5 Comparison of spoofer direction finding methods

Method	User/antenna complexity	Receiver hardware complexity	Typical error of DOA estimation (°)	Accuracy at low elevation	DOA purpose
Array antenna method by [17, 18]	Four elements planar antenna array	Vector tracking needed	3	Poor	Spoofing detection and discrimination
Aperture antenna method by [19, 20]	One single rotating antenna	Vector tracking needed	2	Poor	Spoofing detection and discrimination
Double difference MLE method in this paper	Two moving commercial receivers with single antenna	Only requiring GNSS measurements	4	Poor	Spoofing localization

DOA 估计在低仰角时误差较大. 这是因为本文的 DOA 估计模型只使用了接收机在水平方向的速度分量, 以便获得方位角和仰角 MLE 的显式解. 增加垂直方向速度分量可以有效地改善上述问题, 后续我们将进一步考察接收机垂直方向往复运动对测向精度的影响, 同时进行相关试验验证.

本文的估计模型将接收机速度视为确定且已知的参数, 而事实上接收机定速结果是有误差的. 通常情况下定速误差很小^[23], 但不排除个别情况下的接收机定速异常会对欺骗源测向精度产生较大影响. 在进一步的研究中, 可以将接收机速度建模为随机变量, 对估计算法和估计性能进行更严格的评估.

在整个测向过程中, 欺骗源方位角和仰角都被视作恒定不变的物理量, 因此接收机应该在小范围内运动 (如本文试验中手持接收机天线转动), 以确定欺骗源方位角和仰角在测向过程中的变化可以忽略不计. 对于接收机大范围运动的场景 (如车载导航), 如何快速准确地对欺骗源进行测向和实时跟踪是一个值得研究的问题.

欺骗源自身的运动也是需要考虑的问题. 当欺骗源运动后, DOA 估计算法必须在较短时间内完成, 无法通过长时间的数据观测累积提升估计精度. 更重要的是, 由于欺骗源运动引入了额外的源多普勒, 3.1 小节的多普勒频偏的双差计算方法将不再适用. 欺骗源的运动让欺骗源测向的难度陡增, 这是后续我们需要重点研究的问题.

7 总结

不同于传统的利用载波相位阵列信号处理的欺骗源测向方法, 本文面向商用接收机提出了一种基于多普勒的测向方法. 我们分析了导航信号各个多普勒分量的来源, 利用两个接收机的多普勒观测量和钟漂解算结果构建双差, 消除了欺骗信号中的源多普勒分量, 获得了仅由接收机运动产生的接收机多普勒分量, 并与欺骗源方位角和仰角建立联系, 以此实现欺骗源测向. 对于静止的集中式欺骗源, 仿真结果和实验结果均表明, 本文提出的方法可以仅利用两个单天线商用接收机的观测量, 得到较高精度的欺骗源测向结果. 该方法可以推广应用于当前广泛存在的智能终端中, 利用海量终端的 GNSS 观测量实现更高精度的欺骗源测向.

参考文献

- 1 John A. Volpe National Transportation Systems Center. Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System. Technical Report. U.S. Department of Transportation, 2001
- 2 Kerns A J, Shepard D P, Bhatti J A, et al. Unmanned aircraft capture and control via GPS spoofing. *J Field Robot*, 2014, 31: 617–636
- 3 Psiaki M L, Humphreys T E, Stauffer B. Attackers can spoof navigation signals without our knowledge. Here's how to fight back GPS lies. *IEEE Spectr*, 2016, 53: 26–53
- 4 Wang F. GNSS anti-spoofing techniques based on multi-signal processing. Dissertation for Ph.D. Degree. Beijing: Tsinghua University, 2018 [王斐. 基于多信号处理的 GNSS 反欺骗技术研究. 博士学位论文. 北京: 清华大学, 2018]
- 5 Wesson K, Rothlisberger M, Humphreys T. Practical cryptographic civil GPS signal authentication. *J Inst Navig*, 2012, 59: 177–193
- 6 Wu Z, Zhang Y, Liu R. BD-II NMASSI: an scheme of anti-spoofing and open BeiDou II D2 navigation message authentication. *IEEE Access*, 2020, 8: 23759–23775
- 7 Borio D, Gioia C. A sum-of-squares approach to GNSS spoofing detection. *IEEE Trans Aerosp Electron Syst*, 2016, 52: 1756–1768
- 8 Tanil C, Khanafseh S, Joerger M, et al. An INS monitor to detect GNSS spoofers capable of tracking vehicle position. *IEEE Trans Aerosp Electron Syst*, 2018, 54: 131–143
- 9 Manfredini E G, Motella B, Dovis F. Signal quality monitoring for discrimination between spoofing and environmental

- effects, based on multidimensional ratio metric tests. In: Proceedings of the 28th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2015), Tampa, 2015. 3100–3106
- 10 He L, Li H, Lu M Q. Global navigation satellite system spoofing-detection technique based on the Doppler ripple caused by vertical reciprocating motion. *IET Radar Sonar & Navigation*, 2019, 13: 1655–1664
 - 11 Chu F, Li H, Wen J, et al. Statistical model and performance evaluation of a GNSS spoofing detection method based on the consistency of Doppler and pseudorange positioning results. *J Navigation*, 2019, 72: 447–466
 - 12 Jahromi A J, Broumandan A, Lachapelle G. GNSS signal authenticity verification using carrier phase measurements with multiple receivers. In: Proceedings of the 8th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC), Noordwijk, 2016
 - 13 Shang S, Li H, Peng C, et al. A novel method for GNSS meaconer localization based on a space-time double-difference model. *IEEE Trans Aerosp Electron Syst*, 2020, 56: 3432–3449
 - 14 Dempster A G, Cetin E. Interference localization for satellite navigation systems. *Proc IEEE*, 2016, 104: 1318–1326
 - 15 Wen J, Li H, Wang Z X, et al. Spoofing discrimination using multiple independent receivers based on code-based pseudorange measurements In: Proceedings of the 32nd International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2019), Washington, 2019. 3892–3903
 - 16 Wang Z, Li H, Wen J, et al. GNSS spoofing discrimination method based on Doppler frequency double difference for multiple independent moving receivers. In: Proceedings of the International Technical Meeting of the Institute of Navigation (ION ITM 2021), 2021. 56–68
 - 17 Cuntz M, Konovaltsev A, Meurer M. Concepts, development, and validation of multiantenna GNSS receivers for resilient navigation. *Proc IEEE*, 2016, 104: 1288–1301
 - 18 Meurer M, Konovaltsev A, Cuntz M, et al. Robust joint multi-antenna spoofing detection and attitude estimation using direction assisted multiple hypotheses RAIM. In: Proceedings of the 26th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2013), Nashville, 2013. 3007–3016
 - 19 Pany T, Falk N, Riedl B, et al. GNSS synthetic aperture processing with artificial antenna motion. In: Proceedings of the 26th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2013), Nashville, 2013. 3163–3171
 - 20 Dampf J, Pany T, Bär W, et al. Real World Spoofing Trials and Mitigation via Direction of Arrival Discrimination. *Inside GNSS*, 2017, 12: 55–65
 - 21 Stoica P. Introduction to Spectral Analysis. New Jersey: Prentice Hall. Inc., 1997
 - 22 Kay S M. Fundamentals of Statistical Signal Processing, Volume I: Estimation Theory. Upper Saddle River: Prentice Hall, 1993
 - 23 Xie G. Principles of GPS and Receiver Design. Beijing: Publishing House of Electronics Industry, 2009

A direction finding method of the GNSS spoofer for commercial receivers

Zhongxiao WANG^{1,2}, Hong LI^{1,2*}, Ziheng ZHOU^{1,2} & Mingquan LU^{1,2}

1. *Department of Electronic Engineering, Tsinghua University, Beijing 100084, China;*

2. *Beijing National Research Center for Information Science and Technology (BNRist), Beijing 100084, China*

* Corresponding author. E-mail: lihongee@tsinghua.edu.cn

Abstract With the increasing applications of the Global Navigation Satellite System (GNSS) and the rising threat of spoofing attacks in daily life, it is necessary to conduct anti-spoofing research for commercial receivers. In this paper, we propose a direction-finding method of the GNSS spoofer for commercial receivers. This method fully utilizes the Doppler measurements and clock drift information provided by motion receivers in the horizontal plane. The double difference measurement is constructed to extract the Doppler information generated by the receiver's motion, which is later used to determine the direction of the spoofer. In this paper, the maximum likelihood estimation of the azimuth and elevation of the spoofer is given, and the Cramer-Rao lower bound is derived, with the factors affecting the performance of angle estimation analyzed. We conduct field experiments to estimate the arrival direction of the deception signal broadcast by the helical antenna. The test results show the effectiveness of the proposed method.

Keywords GNSS, spoofing, DOA, Doppler, MLE