文章编号：2095-4980(2024)05-0476-09

牵引式欺骗对矢量跟踪环路的影响

张欣然，梁涛涛，陈懋霖

(中国工程物理研究院 电子工程研究所，四川 绵阳 621999)

摘　要：牵引式欺骗能够在不引起跟踪环路失锁的条件下诱使接收机跟踪欺骗信号，是一种隐蔽性很高的欺骗干扰方式。对于标量接收机，由于其跟踪环路相互独立，因此针对单个信号进行牵引式欺骗时，不会受其他信号的影响。而矢量接收机的跟踪环路通过接收机状态耦合，存在相互影响，即牵引式欺骗对矢量和标量跟踪环路的影响存在差异。本文基于无噪声且欺骗信号与真实信号载波频率和载波相位相等的假设条件，分析牵引式欺骗对矢量跟踪环路的影响，推导出欺骗成功条件，并利用信号源模拟器和软件接收机对分析结果进行验证。研究结果表明，对矢量跟踪环路成功实施牵引式欺骗的条件较标量跟踪环路更为严苛，反映出矢量跟踪环路固有的抗欺骗干扰能力。

关键词：全球导航卫星系统；矢量跟踪；牵引式欺骗；抗欺骗

中图分类号：TN961　　**文献标志码：**A　　**doi：**10.11805/TKYDA2024006

Influence of traction spoofing on vector tracking loop

ZHANG Xinran，LIANG Taotao，CHEN Maolin

(Institute of Electronic Engineering，China Academy of Engineering Physics，Mianyang Sichuan 621999，China)

Abstract：Traction spoofing is a highly covert type of spoofing interference that can induce the receiver to track spoofing signals without causing the tracking loop to lose lock. For scalar receivers, the tracking loops are independent of each other, so the traction spoofing for a single signal will not be affected by the signals of other channels. All tracking loops of vector receiver are coupled through receiver state and have mutual influence, which means that traction spoofing has different influence on vector and scalar tracking loops. Based on the assumption that there is no noise and the carrier frequency and carrier phase of the spoofing signal and the corresponding authentic signal are equal, this paper analyzes the influence of traction spoofing on the vector tracking loop, derives the success condition of spoofing, and verifies the analysis results by using the signal source simulator and software receiver. The results show that the conditions for successfully implementing traction spoofing on vector tracking loop are more stringent than those of scalar tracking loop, which reflects the inherent anti-spoofing capability of vector tracking loop.

Keywords：Global Navigation Satellite System(GNSS)；vector tracking；traction spoofing；anti-spoofing

全球导航卫星系统(GNSS)能够在全天候、全天时、全球范围内为用户提供连续的定位、导航和授时服务，是当前应用最为广泛的无线电定位系统[1]，但在获得广泛应用的同时，GNSS 服务也面临着一系列挑战[2]。一方面，由于发射功率受限以及路径损耗严重，GNSS 信号到达地面时的功率非常低，导致其抗压制干扰能力较弱；另一方面，由于结构公开，GNSS 民用信号容易被伪造，对 GNSS 接收机实施欺骗干扰成为可能。欺骗干扰是近十多年兴起的一种新的干扰方式，通过诱使接收机跟踪处理伪造的信号，误导接收机的状态估计。相对于传统的压制干扰，欺骗干扰隐蔽性更强，潜在危害性更高，因而受到越来越多的关注。

如果欺骗信号在目标接收机工作之前已经存在，且功率高于对应的同一卫星的真实信号，接收机一般会捕获跟踪欺骗信号。如果目标接收机已经跟踪真实信号，则需要先通过压制干扰使接收机环路失锁，重新进入捕

收稿日期：2024-01-04；修回日期：2024-04-04

获模式，但跟踪环路失锁会降低欺骗干扰的隐蔽性[3]。针对这一问题，科研人员提出了牵引式欺骗方法[4−5]。牵引式欺骗首先生成与真实信号基本同步的信号，即载波频率、载波相位以及导航电文等都基本一致；之后，欺骗信号的伪码相位会从逐渐接近到逐渐远离真实信号；由于欺骗信号功率更高，跟踪环路在这一过程中会由锁定真实信号逐渐转为锁定欺骗信号。牵引式欺骗过程不会引起跟踪环路失锁，因此相较于一般的欺骗干扰方式更难被检测，隐蔽性更强。

目前，大部分GNSS接收机都采用独立跟踪处理信号的标量跟踪环路。不同于标量跟踪环路，矢量跟踪环路利用GNSS信号的一致性[6]，通过扩展卡尔曼滤波器(Extended Kalman Filter，EKF)实现对所有信号的联合跟踪。已有研究表明，矢量跟踪环路具有比标量跟踪环路更好的跟踪灵敏度[7−8]和动态特性[9]，并且在抗压制干扰[10]和抑制多径[11]性能等方面也具有优势。矢量跟踪技术已成为当前卫星导航领域具有广阔发展和应用前景的关键技术之一[12]。

已有研究基于无噪声且欺骗信号与真实信号载波频率和载波相位相等的假设条件，分析了牵引式欺骗对标量跟踪环路的影响[13]。由于标量跟踪环路相互独立，因此针对单个信号进行牵引式欺骗时，不会受其他信号的影响；而矢量跟踪环路存在相互影响，即牵引式欺骗对矢量和标量跟踪环路的影响存在差异。本文基于相同的假设条件，分析牵引式欺骗对矢量跟踪环路的影响，得出对矢量跟踪环路成功实施牵引式欺骗的条件较标量跟踪环路更为严苛。在基于GNSS信号源模拟器搭建的牵引式欺骗场景中进行测试，对分析结果进行验证。

1　系统模型

牵引式欺骗主要针对伪码相位进行牵引，本文的分析基于如图1所示的矢量延迟锁定环(Vector Delay Lock Loop，VDLL)[14]，并参考已有文献对牵引式欺骗过程模型进行简化。假设不存在噪声，且欺骗信号与真实信号的载波频率和载波相位相等，只关注伪码相位跟踪误差在牵引式欺骗过程中的变化[13]。

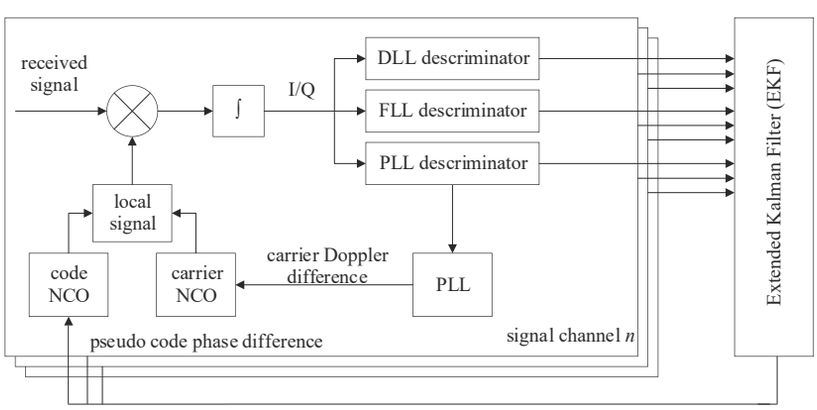

Fig.1 Vector Delay Lock Loop
图1 矢量延迟锁定环

信号通道n对应的真实信号、欺骗信号和本地信号依次记为S_n^{r}、S_n^{h}和S_n^{l}，定义真实信号的伪码相位跟踪误差δC_n^{rl}、载波频率跟踪误差δf_n^{rl}、载波相位跟踪误差$\delta\varphi_n^{\mathrm{rl}}$为真实信号和本地信号的参数差值；欺骗信号的伪码相位跟踪误差δC_n^{hl}、载波频率跟踪误差δf_n^{hl}和载波相位跟踪误差$\delta\varphi_n^{\mathrm{hl}}$为欺骗信号和本地信号的参数差值，如式(1)~(2)所示。

$$\begin{cases}\delta C_n^{\mathrm{rl}}=C_n^{\mathrm{r}}-C_n^{\mathrm{l}}\\ \delta f_n^{\mathrm{rl}}=f_n^{\mathrm{r}}-f_n^{\mathrm{l}}\\ \delta\varphi_n^{\mathrm{rl}}=\varphi_n^{\mathrm{r}}-\varphi_n^{\mathrm{l}}\end{cases}\tag{1}$$

$$\begin{cases}\delta C_n^{\mathrm{hl}}=C_n^{\mathrm{h}}-C_n^{\mathrm{l}}\\ \delta f_n^{\mathrm{hl}}=f_n^{\mathrm{h}}-f_n^{\mathrm{l}}\\ \delta\varphi_n^{\mathrm{hl}}=\varphi_n^{\mathrm{h}}-\varphi_n^{\mathrm{l}}\end{cases}\tag{2}$$

对于EKF，系统状态$\boldsymbol{\alpha}_{\mathrm{u}}$包括接收机的三维位置$(x_{\mathrm{u}},y_{\mathrm{u}},z_{\mathrm{u}})$、钟差$\delta t_{\mathrm{u}}$、三维速度$(vx_{\mathrm{u}},vy_{\mathrm{u}},vz_{\mathrm{u}})$以及钟漂$b_{\mathrm{u}}$：

$$\boldsymbol{\alpha}_{\mathrm{u}}=\left[\boldsymbol{\alpha}_1\quad\boldsymbol{\alpha}_2\right]^{\mathrm{T}}\tag{3}$$

式中：

$$\begin{cases}\boldsymbol{\alpha}_1=\left[x_{\mathrm{u}}\quad y_{\mathrm{u}}\quad z_{\mathrm{u}}\quad c\delta t_{\mathrm{u}}\right]^{\mathrm{T}}\\ \boldsymbol{\alpha}_2=\left[vx_{\mathrm{u}}\quad vy_{\mathrm{u}}\quad vz_{\mathrm{u}}\quad cb_{\mathrm{u}}\right]^{\mathrm{T}}\end{cases}\tag{4}$$

式中c为光速。系统观测量$\boldsymbol{\beta}$为：

$$\boldsymbol{\beta}=\left[\boldsymbol{\beta}_{\mathrm{D}}\quad\boldsymbol{\beta}_{\mathrm{F}}\right]^{\mathrm{T}}\tag{5}$$

式中：

$$\begin{cases}\boldsymbol{\beta}_{\mathrm{D}}=\left[\widehat{\rho}_1\quad\widehat{\rho}_2\quad\cdots\quad\widehat{\rho}_N\right]^{\mathrm{T}}\\ \boldsymbol{\beta}_{\mathrm{F}}=\left[\widehat{f}_{\mathrm{d},1}\quad\widehat{f}_{\mathrm{d},2}\quad\cdots\quad\widehat{f}_{\mathrm{d},N}\right]^{\mathrm{T}}\end{cases}\tag{6}$$

式中$\widehat{\rho}_n$和$\widehat{f}_{\mathrm{d},n}$分别为伪距测量值和载波多普勒频移测量值，满足式(7)：

$$\begin{cases}\widehat{\rho}_n=\rho_n^{\mathrm{r}}-\dfrac{c}{f_{\mathrm{c}}}\left(\Delta\widehat{C}_n-\delta C_n^{\mathrm{rl}}\right)\\ \widehat{f}_{\mathrm{d},n}=f_{\mathrm{d},n}^{\mathrm{r}}+\Delta\widehat{f}_n-\delta f_n^{\mathrm{rl}}\end{cases}\tag{7}$$

式中：ρ_n^{r}和$f_{\mathrm{d},n}^{\mathrm{r}}$分别为真实信号对应的伪距和载波多普勒频移；$\Delta\widehat{C}_n$和$\Delta\widehat{f}_n$为延迟锁相环(Delay Locked Loop，DLL)鉴别器和频率锁定环(Frequency Locked Loop，FLL)鉴别器输出；f_{c}为伪码速率。定义$\boldsymbol{\beta}_{\mathrm{D}}$和$\boldsymbol{\alpha}_{\mathrm{u}}$、$\boldsymbol{\beta}_{\mathrm{F}}$和$\boldsymbol{\alpha}_{\mathrm{u}}$之间的关系为：

$$\begin{cases}\boldsymbol{\beta}_{\mathrm{D}}=\boldsymbol{h}_{\mathrm{D}}\left(\boldsymbol{\alpha}_{\mathrm{u}}\right)\\ \boldsymbol{\beta}_{\mathrm{F}}=\boldsymbol{h}_{\mathrm{F}}\left(\boldsymbol{\alpha}_{\mathrm{u}}\right)\end{cases}\tag{8}$$

结合式(3)~(6)和(8)，$\boldsymbol{\beta}$与$\boldsymbol{\alpha}_{\mathrm{u}}$之间的测量关系矩阵$\boldsymbol{H}$可表示为：

$$\boldsymbol{H}=\frac{\partial\boldsymbol{\beta}}{\partial\boldsymbol{\alpha}_{\mathrm{u}}^{\mathrm{T}}}=\begin{bmatrix}\partial\boldsymbol{\beta}_{\mathrm{D}}/\partial\boldsymbol{\alpha}_{\mathrm{u}}^{\mathrm{T}}\\ \partial\boldsymbol{\beta}_{\mathrm{F}}/\partial\boldsymbol{\alpha}_{\mathrm{u}}^{\mathrm{T}}\end{bmatrix}=\begin{bmatrix}\boldsymbol{H}_{\mathrm{D}}\\ \boldsymbol{H}_{\mathrm{F}}\end{bmatrix}=\begin{bmatrix}\partial\boldsymbol{\beta}_{\mathrm{D}}/\partial\boldsymbol{\alpha}_1^{\mathrm{T}} & \partial\boldsymbol{\beta}_{\mathrm{D}}/\partial\boldsymbol{\alpha}_2^{\mathrm{T}}\\ \partial\boldsymbol{\beta}_{\mathrm{F}}/\partial\boldsymbol{\alpha}_1^{\mathrm{T}} & \partial\boldsymbol{\beta}_{\mathrm{F}}/\partial\boldsymbol{\alpha}_2^{\mathrm{T}}\end{bmatrix}=\begin{bmatrix}\boldsymbol{H}_{\mathrm{D1}} & \boldsymbol{H}_{\mathrm{D2}}\\ \boldsymbol{H}_{\mathrm{F1}} & \boldsymbol{H}_{\mathrm{F2}}\end{bmatrix}\tag{9}$$

进一步对$\boldsymbol{H}$进行分析可以得出：

$$\begin{cases}\boldsymbol{H}_{\mathrm{D2}}=\boldsymbol{0}\\ \boldsymbol{H}_{\mathrm{F1}}\approx\boldsymbol{0}\end{cases}\tag{10}$$

EKF输出的伪码相位差$\Delta\tilde{C}_n$可表示为[15]：

$$\begin{bmatrix}\Delta\tilde{C}_1\\ \Delta\tilde{C}_2\\ \vdots\\ \Delta\tilde{C}_N\end{bmatrix}=\begin{bmatrix}\Delta\widehat{C}_1\\ \Delta\widehat{C}_2\\ \vdots\\ \Delta\widehat{C}_N\end{bmatrix}-\frac{c}{f_{\mathrm{c}}}\left[\boldsymbol{h}_{\mathrm{D}}\left(\boldsymbol{\alpha}_{\mathrm{u}}\right)-\boldsymbol{\beta}_{\mathrm{D}}\right]\tag{11}$$

VDLL利用$\left(\Delta\tilde{C}_1,\Delta\tilde{C}_2,\cdots,\Delta\tilde{C}_N\right)$驱动各信号通道的码数控振荡器(Numerically Controlled Oscillator，NCO)生成本地伪码信号。由于假设不存在噪声，且欺骗信号与真实信号的载波频率和载波相位相等，当VDLL稳定时，$\Delta\tilde{C}_n$等于0，δf_n^{rl}、$\delta\varphi_n^{\mathrm{rl}}$、$\delta f_n^{\mathrm{hl}}$和$\delta\varphi_n^{\mathrm{hl}}$也等于0。可推导出VDLL的稳态公式为：

$$\begin{bmatrix}\Delta\tilde{C}_1\\ \Delta\tilde{C}_2\\ \vdots\\ \Delta\tilde{C}_N\end{bmatrix}=\begin{bmatrix}\Delta\widehat{C}_1\\ \Delta\widehat{C}_2\\ \vdots\\ \Delta\widehat{C}_N\end{bmatrix}-\left(\boldsymbol{I}-\boldsymbol{W}_{\mathrm{D}}\right)\begin{bmatrix}\Delta\widehat{C}_1-\delta C_1^{\mathrm{rl}}\\ \Delta\widehat{C}_2-\delta C_2^{\mathrm{rl}}\\ \vdots\\ \Delta\widehat{C}_N-\delta C_N^{\mathrm{rl}}\end{bmatrix}=\boldsymbol{0}\tag{12}$$

式中$\boldsymbol{W}_{\mathrm{D}}$定义为：$\boldsymbol{W}_{\mathrm{D}}=\boldsymbol{H}_{\mathrm{D1}}\left(\boldsymbol{H}_{\mathrm{D1}}^{\mathrm{T}}\boldsymbol{H}_{\mathrm{D1}}\right)^{-1}\boldsymbol{H}_{\mathrm{D1}}^{\mathrm{T}}$。

2　牵引式欺骗过程分析

2.1 矢量跟踪环路稳态分析

为更直观地对比基于标量和矢量跟踪环路进行牵引式欺骗的区别，本文考虑仅一个信号通道受到牵引式欺骗的情况。DLL 鉴别器采用典型的非相干超前滞后幅值鉴别方法[16]，此时鉴别器输出 $\Delta\widehat{C}_n$ 可表示为：

$$\Delta\widehat{C}_n=(1-d)\frac{R\left(d-\delta C_n^{\mathrm{rl}}\right)+\eta_n R\left(d-\delta C_n^{\mathrm{hl}}\right)-R\left(d+\delta C_n^{\mathrm{rl}}\right)-\eta_n R\left(d+\delta C_n^{\mathrm{hl}}\right)}{R\left(d-\delta C_n^{\mathrm{rl}}\right)+\eta_n R\left(d-\delta C_n^{\mathrm{hl}}\right)+R\left(d+\delta C_n^{\mathrm{rl}}\right)+\eta_n R\left(d+\delta C_n^{\mathrm{hl}}\right)} \tag{13}$$

式中：η_n 为欺骗信号幅度 A_n^{h} 和真实信号幅度 A_n^{r} 的比值：$\eta_n=A_n^{\mathrm{h}}/A_n^{\mathrm{r}}$；关系函数 $R(\cdot)$ 定义为：$R(\mu)=\max\left(1-|\mu|,0\right)$；$d$ 为相关器间距。

假设仅信号通道 m 受到牵引式欺骗，对于不存在欺骗干扰的信号通道 $n(n\neq m)$，鉴别器输出 $\Delta\widehat{C}_n$ 等于真实信号的伪码相位跟踪误差 δC_n^{rl}，即 $\Delta\widehat{C}_n-\delta C_n^{\mathrm{rl}}=0$。代入式(12)，VDLL 的稳态公式可简化为：

$$\begin{bmatrix}\Delta\tilde{C}_1\\ \Delta\tilde{C}_2\\ \vdots\\ \Delta\tilde{C}_N\end{bmatrix}=\begin{bmatrix}\Delta\widehat{C}_1\\ \Delta\widehat{C}_2\\ \vdots\\ \Delta\widehat{C}_N\end{bmatrix}-\left(\boldsymbol{I}-\boldsymbol{W}_{\mathrm{D}}\right)\begin{bmatrix}0\\ \vdots\\ \Delta\widehat{C}_m-\delta C_m^{\mathrm{rl}}\\ \vdots\\ 0\end{bmatrix}=\boldsymbol{0} \tag{14}$$

可得鉴别器输出 $\Delta\widehat{C}_m$ 的稳态值为：

$$\Delta\tilde{C}_m=\Delta\widehat{C}_m-\gamma_m\left(\Delta\widehat{C}_m-\delta C_m^{\mathrm{rl}}\right)=0\Rightarrow\Delta\widehat{C}_m=\frac{\gamma_m}{\gamma_m-1}\delta C_m^{\mathrm{rl}} \tag{15}$$

式中 $\gamma_m\in(0,1)$ 为影响因子，为矩阵 $\boldsymbol{I}-\boldsymbol{W}_{\mathrm{D}}$ 的第 m 个对角线元素，其大小体现了其他通道信号对信号通道 m 的影响程度。

2.2 牵引式欺骗过程模型

对于牵引式欺骗，可以将欺骗信号与真实信号伪码相位对齐作为初始状态，如图 2 所示，欺骗信号的伪码相位逐渐远离真实信号的过程为牵引过程。如果牵引式欺骗成功，随着欺骗信号的相关峰与真实信号的相关峰逐渐分离，环路最终将仅跟踪欺骗信号。

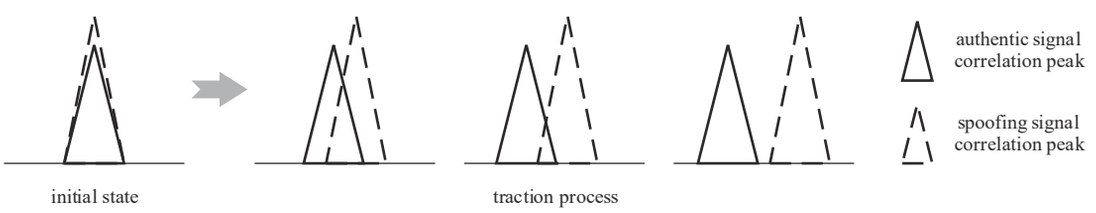

Fig.2 Diagram of the traction spoofing process
图2 牵引式欺骗过程示意图

假设仅对信号通道 m 进行牵引式欺骗，牵引式欺骗过程如下：

初始状态：欺骗信号和真实信号的伪码相位相等，此时，δC_m^{rl} 和 δC_m^{hl} 都等于零，EKF 输出的 $\Delta\tilde{C}_m$ 也等于 0。

第 1 步：假设系统当前已处于稳定状态，$\Delta\tilde{C}_m=0$。进行下一次牵引，欺骗信号相关峰远离真实信号相关峰，$|\delta C_m^{\mathrm{hr}}|$ 增加，此时本地信号伪码相位 C_m^{l} 尚未改变，δC_m^{rl} 不变，δC_m^{hl} 变化，$\Delta\tilde{C}_m\neq0$，系统状态不稳定，进入第 2 步。

第 2 步：如果 $\Delta\tilde{C}_m>0$，C_m^{l} 增加；如果 $\Delta\tilde{C}_m<0$，C_m^{l} 减小，不断调整 C_m^{l} 使 $\Delta\tilde{C}_m=0$，系统状态再次稳定，则执行第 1 步。

最终状态：一旦 $|\delta C_m^{\mathrm{rl}}|$ 和 $|\delta C_m^{\mathrm{hl}}|$ 其中之一大于等于 $(1+d)$ 个码片，将不再对 DLL 鉴别器输出产生影响。牵引式欺骗的最终状态分为欺骗失败和欺骗成功：

1) 欺骗失败：$\delta C_m^{\mathrm{rl}}=0$ 且 $|\delta C_m^{\mathrm{hl}}|\geqslant1+d$。欺骗信号不影响 DLL 鉴别器输出，信号通道 m 仅跟踪真实信号，最终本地信号伪码相位与真实信号完全对齐。

2) 欺骗成功：$\left|\delta C_m^{\mathrm{rl}}\right| \geqslant 1+d$ 且 $\left|\delta C_m^{\mathrm{hl}}\right| \leqslant d$。真实信号不影响 DLL 鉴别器输出，信号通道 m 仅跟踪欺骗信号。但由于欺骗信号不与其他真实信号一致，最终本地信号的伪码相位不与欺骗信号对齐。

需要说明的是，在欺骗成功之后，若欺骗信号相关峰继续远离真实信号相关峰，环路最终将会失锁。因此，只要存在欺骗成功的时刻，即认为欺骗是成功的。

2.3 欺骗成功条件

基于牵引式欺骗过程，分析对单个信号通道成功实施牵引式欺骗的条件。鉴于 δC_m^{hr} 的正负不会影响分析结果，因此仅分析 $\delta C_m^{\mathrm{hr}} \geqslant 0$ 的情况。当 $\delta C_m^{\mathrm{hr}} \geqslant 0$ 时：$\delta C_m^{\mathrm{rl}} \leqslant 0$，$\delta C_m^{\mathrm{hl}} \geqslant 0$。另外，相关器间距 d 设为 0.5 码片，这是一种典型的相关器间距大小。当 $\delta C_m^{\mathrm{rl}} \leqslant 0$ 时，$R\left(d-\delta C_m^{\mathrm{rl}}\right)$ 和 $R\left(d+\delta C_m^{\mathrm{rl}}\right)$ 与 δC_m^{rl} 的关系为：

$$
\begin{aligned}
R\left(d-\delta C_m^{\mathrm{rl}}\right) &= \begin{cases} 0.5+\delta C_m^{\mathrm{rl}} & -0.5 \leqslant \delta C_m^{\mathrm{rl}} \leqslant 0 \\ 0 & -1.5 < \delta C_m^{\mathrm{rl}} < -0.5 \\ 0 & \delta C_m^{\mathrm{rl}} \leqslant -1.5 \end{cases} \\
R\left(d+\delta C_m^{\mathrm{rl}}\right) &= \begin{cases} 0.5-\delta C_m^{\mathrm{rl}} & -0.5 \leqslant \delta C_m^{\mathrm{rl}} \leqslant 0 \\ 1.5+\delta C_m^{\mathrm{rl}} & -1.5 < \delta C_m^{\mathrm{rl}} < -0.5 \\ 0 & \delta C_m^{\mathrm{rl}} \leqslant -1.5 \end{cases}
\end{aligned}
\tag{16}
$$

当 $\delta C_m^{\mathrm{hl}} \geqslant 0$ 时，$R\left(d-\delta C_m^{\mathrm{hl}}\right)$ 和 $R\left(d+\delta C_m^{\mathrm{hl}}\right)$ 与 δC_m^{hl} 的关系为：

$$
\begin{aligned}
R\left(d-\delta C_m^{\mathrm{hl}}\right) &= \begin{cases} 0.5+\delta C_m^{\mathrm{hl}} & 0 \leqslant \delta C_m^{\mathrm{hl}} \leqslant 0.5 \\ 1.5-\delta C_m^{\mathrm{hl}} & 0.5 < \delta C_m^{\mathrm{hl}} < 1.5 \\ 0 & \delta C_m^{\mathrm{hl}} \geqslant 1.5 \end{cases} \\
R\left(d+\delta C_m^{\mathrm{hl}}\right) &= \begin{cases} 0.5-\delta C_m^{\mathrm{hl}} & 0 \leqslant \delta C_m^{\mathrm{hl}} \leqslant 0.5 \\ 0 & 0.5 < \delta C_m^{\mathrm{hl}} < 1.5 \\ 0 & \delta C_m^{\mathrm{hl}} \geqslant 1.5 \end{cases}
\end{aligned}
\tag{17}
$$

根据 δC_m^{rl} 和 δC_m^{hl} 的不同取值范围，将 VDLL 划分出 4 种状态：状态 1:$-0.5 \leqslant \delta C_m^{\mathrm{rl}} \leqslant 0$ 和 $0 \leqslant \delta C_m^{\mathrm{hl}} \leqslant 0.5$；状态 2:$-0.5 \leqslant \delta C_m^{\mathrm{rl}} \leqslant 0$ 和 $0.5 < \delta C_m^{\mathrm{hl}} < 1.5$；状态 3:$-1.5 < \delta C_m^{\mathrm{rl}} < -0.5$ 和 $0 \leqslant \delta C_m^{\mathrm{hl}} \leqslant 0.5$；状态 4: $-1.5 < \delta C_m^{\mathrm{rl}} < -0.5$ 和 $0.5 < \delta C_m^{\mathrm{hl}} < 1.5$。

基于式(15)所示的稳态方程分析得出，从初始状态进入牵引过程，VDLL 必然经历状态 1。对于状态 1，δC_m^{hr} 增加，导致 $\left|\delta C_m^{\mathrm{rl}}\right|$ 和 $\left|\delta C_m^{\mathrm{hl}}\right|$ 均增加。$\left|\delta C_m^{\mathrm{rl}}\right|$ 和 $\left|\delta C_m^{\mathrm{hl}}\right|$ 持续增加，将会出现 3 种可能情况：

1) 若 $\left|\delta C_m^{\mathrm{rl}}\right| < \left|\delta C_m^{\mathrm{hl}}\right|$，VDLL 会从状态 1 进入状态 2；进入状态 2 后，δC_m^{hr} 增加导致 $\left|\delta C_m^{\mathrm{rl}}\right|$ 减小，因此 $\left|\delta C_m^{\mathrm{rl}}\right| < 0.5$，表明 VDLL 一直保持状态 b)直至 $\delta C_m^{\mathrm{hl}} \geqslant 1.5$，即欺骗失败。

2) 若 $\left|\delta C_m^{\mathrm{rl}}\right| = \left|\delta C_m^{\mathrm{hl}}\right|$，当 δC_m^{hr} 增加至 1 码片时，$\delta C_m^{\mathrm{rl}} = -0.5$ 且 $\delta C_m^{\mathrm{hl}} = -0.5$；之后，随着 δC_m^{hr} 增加，VDLL 进入状态 2，并一直保持状态 2 直至 $\delta C_m^{\mathrm{hl}} \geqslant 1.5$，即欺骗失败。

3) 若 $\left|\delta C_m^{\mathrm{rl}}\right| > \left|\delta C_m^{\mathrm{hl}}\right|$，VDLL 会从状态 1 进入状态 3；进入状态 3 后，VDLL 可能会一直保持状态 3 直至 $\delta C_m^{\mathrm{rl}} \leqslant -1.5$，此时欺骗成功；也可能会进入状态 4，$\delta C_m^{\mathrm{hr}}$ 增加使 $\left|\delta C_m^{\mathrm{rl}}\right|$ 减小及 $\left|\delta C_m^{\mathrm{hl}}\right|$ 增加，这时将不可能欺骗成功。

结合稳态方程，可得出 VDLL 在牵引式欺骗过程中的状态转换，如图 3 所示，其中，状态转换条件分别为：

条件 a：$\gamma_m \geqslant 0.5$ 或 $\begin{cases} \eta_m \leqslant \dfrac{1}{1-2\gamma_m} \\ \gamma_m < 0.5 \end{cases}$；

条件 b：$\begin{cases} \eta_m > \dfrac{1}{1-2\gamma_m} \\ \gamma_m < 0.5 \end{cases}$；

条件 c：$\begin{cases} \eta_m > \dfrac{1}{1-2\gamma_m} \\ \gamma_m \leqslant \dfrac{3-\sqrt{5}}{4} \end{cases}$ 或 $\begin{cases} \eta_m \geqslant \dfrac{3-6\gamma_m-\sqrt{(1-4\gamma_m)(8-8\gamma_m)}}{2\gamma_m} \\ \dfrac{3-\sqrt{5}}{4} < \gamma_m \leqslant 0.25 \end{cases}$；

条件 d：$\begin{cases} \dfrac{1}{1-2\gamma_m} < \eta_m < \dfrac{3-6\gamma_m-\sqrt{(1-4\gamma_m)(8-8\gamma_m)}}{2\gamma_m} \\ \dfrac{3-\sqrt{5}}{4} < \gamma_m \leqslant 0.25 \end{cases}$ 或 $\begin{cases} \eta_m > \dfrac{1}{1-2\gamma_m} \\ 0.25 < \gamma_m \leqslant 0.5 \end{cases}$。

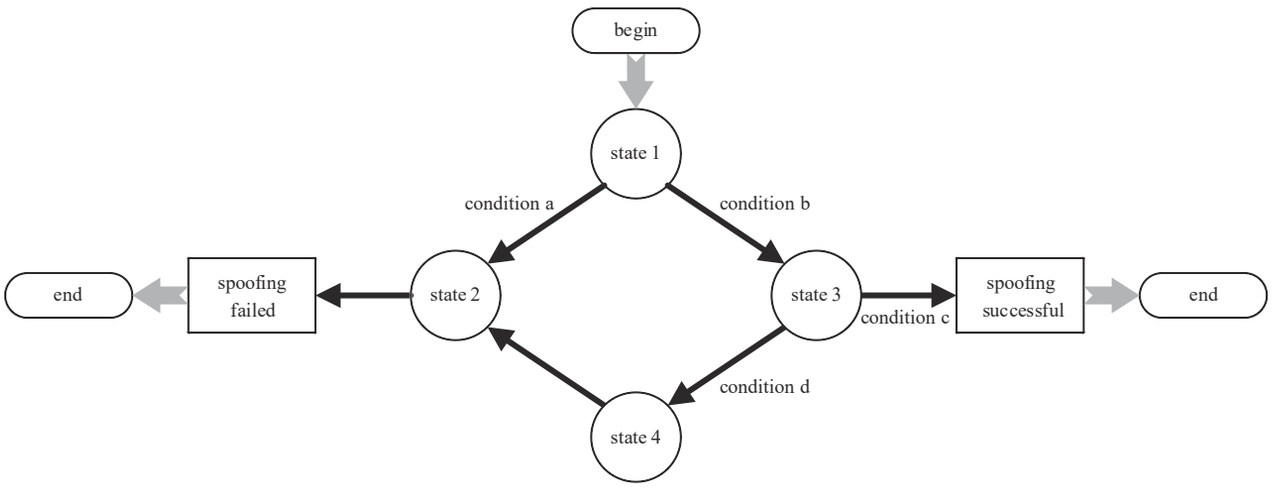

Fig.3 State transition of VDLL during traction spoofing
图3 VDLL在牵引式欺骗过程中的状态转换

由图3可以总结出对VDLL中单个信号成功实施牵引式欺骗的条件为：

$$\begin{cases}\eta_m > \dfrac{1}{1-2\gamma_m} \\ \gamma_m \leqslant \dfrac{3-\sqrt{5}}{4}\end{cases} \text{或} \begin{cases}\eta_m \geqslant \dfrac{3-6\gamma_m-\sqrt{(1-4\gamma_m)(8-8\gamma_m)}}{2\gamma_m} \\ \dfrac{3-\sqrt{5}}{4} < \gamma_m \leqslant 0.25\end{cases} \tag{18}$$

图4为标量和矢量跟踪环路对应的欺骗成功幅度比值η_m下限。标量跟踪环路成功实施牵引式欺骗的条件为：$\eta_m > 1$，且与γ_m的值无关；对矢量跟踪环路成功实施牵引式欺骗的条件更为严苛，当$\gamma_m \leqslant 0.25$时，矢量跟踪环路对η_m下限的要求更高；当$\gamma_m > 0.25$时，无论η_m为多少，都无法欺骗成功。

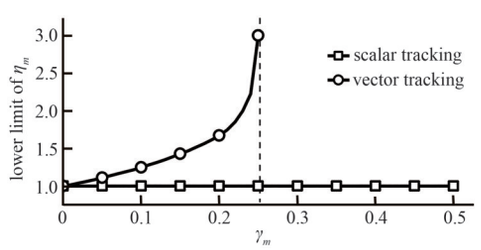

Fig.4 Lower limit of the ratio of spoofing success amplitude corresponding to scalar and vector tracking loops
图4 标量和矢量跟踪环路对应的欺骗成功幅度比值下限

3 试验验证

针对单个信号通道受到牵引式欺骗的情况，对标量和矢量跟踪环路的抗欺骗干扰能力进行测试。基于图5所示的半实物仿真测试平台进行仿真测试，信号由GNSS信号源模拟器生成，经存储器采样存储后，再由GNSS软件接收机进行处理。测试信号个数$N=5$，信号对应的卫星几何分布如图6所示，信号通道1~5分别处理伪随机噪声(Pseudo Random Noise，PRN) 2、PRN 12、PRN 17、PRN 23和PRN 28信号。相关器间距d设为0.5码片，相干积分时间T设为1 ms。

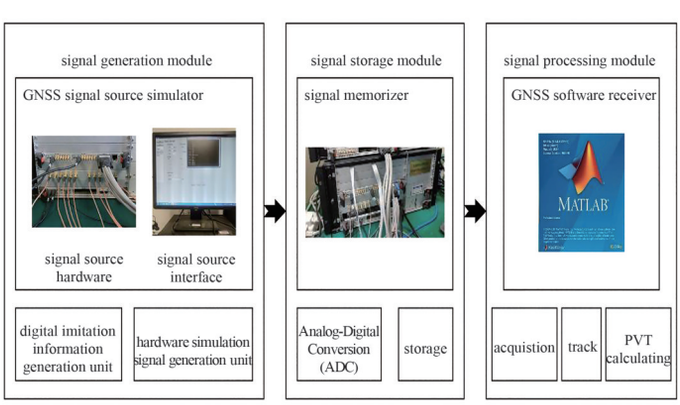

Fig.5 Simulation platform
图5 仿真平台

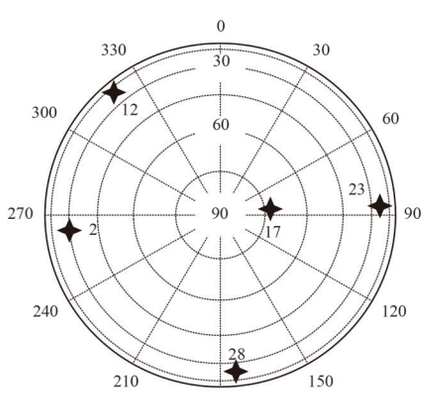

Fig.6 Geometry distribution of satellites
图6 卫星几何分布

分别对PRN 2、PRN 12和PRN 23信号进行牵引式欺骗测试。在0时刻，欺骗信号的伪码相位与真实信号对齐，之后欺骗信号以0.2码片每秒的速度逐渐远离真实信号，信号对应的影响因子以及分析得到的标量和矢量跟踪环路条件下的欺骗成功幅度比值下限如表1所示。牵引式欺骗过程中，真实信号的伪码相位跟踪误差δC_m^{rl}在不同幅度比值条件下的测试结果如图7所示。

表1 测试信号对应的影响因子和欺骗成功幅度比值下限

Table1 Influence factor and lower limit of the spoofing success ratio corresponding to the test signals

PRN number	influence factor	lower limit of amplitude ratio for scalar tracking	lower limit of amplitude ratio for vector tracking
PRN 2	$\gamma_1=0.444\,2$	1	cannot spoof successfully
PRN 12	$\gamma_2=0.230\,3$	1	2.000 9
PRN 23	$\gamma_4=0.135\,6$	1	1.372 1

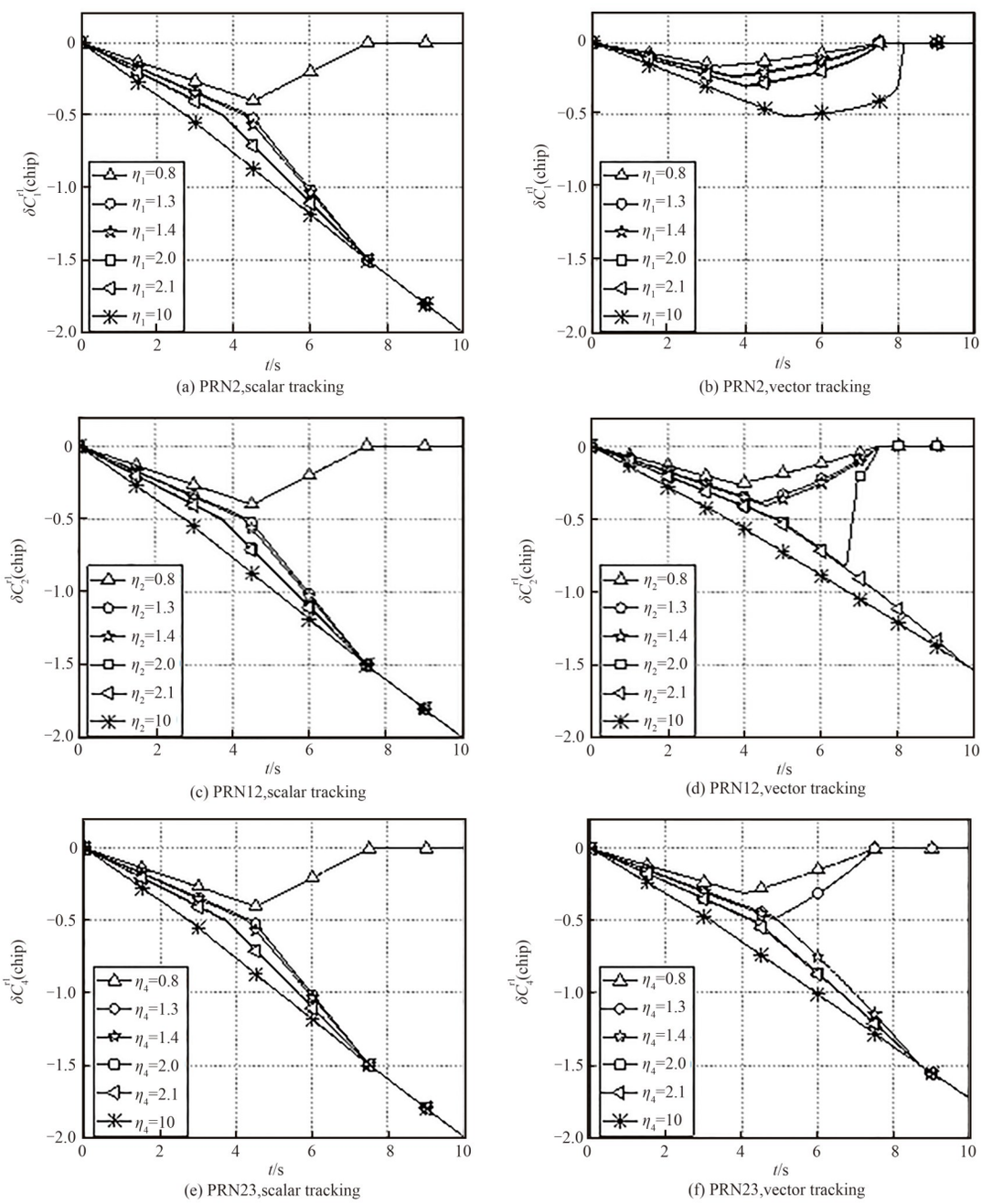

Fig.7 Variation of phase tracking error of authentic signal pseudo-code during traction spoofing

图7 牵引式欺骗过程中真实信号伪码相位跟踪误差的变化

测试结果显示：当采用标量跟踪环路时，对于PRN 2、PRN 12和PRN 23信号，由图7(a)、7(c)和7(e)可见，幅度比值为0.8时，真实信号与本地信号的伪码相位差最终趋于0，代表欺骗失败；幅度比值分别为1.3、1.4、2.0、2.1和10时，真实信号与本地信号的伪码相位差最终超出1.5码片，代表欺骗成功。当采用矢量跟踪环路时，对于PRN 2信号，由图7(b)可见，对于不同的幅度比值η_1，真实信号与本地信号的伪码相位差最终均趋于0，代表欺骗失败；对于PRN 12信号，由图7(d)可见，幅度比值η_2分别为0.8、1.3、1.4和2.0时，真实信号与本地信号的伪码相位差最终趋于0，代表欺骗失败；幅度比值η_3分别为2.1和10时，真实信号与本地信号的伪码相位差最终超出1.5码片，代表欺骗成功；对于PRN 23信号，由图7(f)可见，幅度比值η_4分别为0.8和1.3时，真实信号与本地信号的伪码相位差最终趋于0，代表欺骗失败；幅度比值η_4分别为1.4、2.0、2.1和10时，真实信号与本地信号的伪码相位差最终超出1.5码片，代表欺骗成功。另外，对比3组信号的测试结果可以发现，影响因子越大，矢量跟踪欺骗成功所要求的幅度比值越大，对标量跟踪则没有影响。

对标量跟踪环路成功实施牵引式欺骗的幅度比值下限为1，因此，只要幅度比值大于1，均可以欺骗成功。对矢量跟踪环路成功实施牵引式欺骗的幅度比值下限与对应的影响因子大小相关，结合表1和图7，由于PRN 2信号对应的影响因子$\gamma_1 > 0.25$，即使幅度比值设为较大值10，也无法欺骗成功；对于PRN 12和PRN 23信号，当幅度比值低于下限值时，欺骗失败；高于下限值时，欺骗成功。测试结果与理论分析吻合，表明所推导的欺骗成功条件是可靠的，并进一步验证了对矢量跟踪环路成功实施牵引式欺骗的难度较标量跟踪环路更大，且矢量跟踪环路中不同卫星信号的抗欺骗干扰能力存在差异，取决于卫星信号对应影响因子的大小，影响因子越大，抗欺骗干扰能力越强。

4　结论

本文在无噪声、且欺骗信号与真实信号载波频率和载波相位相等的假设条件下，建立了基于矢量跟踪环路的牵引式欺骗过程模型，并针对单个信号通道受到牵引式欺骗的情况，分析了牵引式欺骗过程中矢量跟踪环路的状态变化，推导出牵引式欺骗成功条件，证明了对矢量跟踪环路成功实施牵引式欺骗的条件较标量跟踪环路更为严苛。矢量跟踪环路利用了真实信号之间具有一致性、欺骗信号一般不与真实信号一致的特性，其本身具有一定的抗欺骗干扰能力，这是标量跟踪环路所不具备的。本文的研究工作对充分认识矢量跟踪环路的防欺骗潜力具有理论指导意义。

参考文献：

[1] 吴军伟,梁涛涛,王川. 一种高动态弱GNSS信号跟踪解调算法研究与实现[J]. 太赫兹科学与电子信息学报, 2023,21(11):1318-1323. (WU Junwei, LIANG Taotao, WANG Chuan. Research and implementation of tracking demodulation algorithm for high dynamic and weak GNSS signal[J]. Journal of Teraherz Science and Electronic Information Technology, 2023,21(11):1318-1323.) doi:10.11805/TKYDA20211322.

[2] 王斐. 基于多信号处理的GNSS反欺骗技术研究[D]. 北京:清华大学, 2018. (WANG Fei. Research on GNSS anti-spoofing technology based on multi-signal processing[D]. Beijing,China:Tsinghua University, 2018.)

[3] HUMPHREYS T E, LEDVINA B M, PSIAKI M L. Assessing the spoofing threat: development of a portable GPS civilian spoofer[C]// Proceedings of International Technical Meeting of the Satellite Division of the Institute of Navigation. Savannah,GA: Aerospace Engineering, 2008:2314-2325. doi:10.1117/12.820334.

[4] JAFARNIA-JAHROMI A, LIN T, BROUMANDAN A. Detection and mitigation of spoofing attacks on a vector-based tracking GPS receiver[J]. Journal of Global Positioning Systems, 2008(7):156-168. doi:10.5081/jgps.7.2.156.

[5] TIPPENHAUER N O,PÖPPER C,RASMUSSEN K B. On the requirements for successful GPS spoofing attacks[C]// Proceedings of ACM conference on computer and communications security. Chicago, Illinois, USA: Association for Computing Machinery, 2011:75-86. doi:10.1145/2046707.2046719.

[6] TAO Huiqi,WU Hailing,LI Hong,et al. GNSS spoofing detection based on consistency check of velocities[J]. Chinese Journal of Electronics, 2019,28(2):437-444.

[7] ZHANG Xinran, LI Hong, YANG Chun, et al. Signal quality monitoring-based spoofing detection method for Global Navigation Satellite System vector tracking structure[J]. IET Radar, Sonar & Navigation, 2020, 14(6): 944-953. doi: 10.1049/iet-rsn.2020.0021.

[8] WANG Qian, CUI Xiaowei, LIU Jing, et al. Quantitative analysis of the performance of vector tracking algorithms[J]. High Technology Letters, 2017,23(3):238-244. doi:10.3772/j.issn.1006-6748.2017.03.002.

[9] LASHLEY M, BEVLY D M, HUNG J Y. Performance analysis of vector tracking algorithms for weak GPS signals in high dynamics[J]. IEEE Journal of Selected Topics in Signal Processing, 2009,3(4):661–673. doi:10.1109/JSTSP.2009.2023341.

[10] LI Kui, ZHAO Jiaxing, WANG Xueyun, et al. Federated ultra–tightly coupled GPS/INS integrated navigation system based on vector tracking for severe jamming environment[J]. IET Radar, Sonar & Navigation, 2016, 10(6): 1030–1037. doi: 10.1049/iet–rsn.2015.0258.

[11] 刘婧,崔晓伟,陆明泉,等. 标量和矢量架构下GNSS接收机多径抑制性能比较[J]. 清华大学学报(自然科学版), 2013,53(7): 961–966. (LIU Jing, CUI Xiaowei, LU Mingquan, et al. Comparison of GNSS receiver multipath rejection performance in scalar and vector architectures[J]. Journal of Tsinghua University(Science and Technology), 2013,53(7):961–966.) doi:10.16511/j.cnki.qhdxxb.2013.07.012.

[12] 张瑞华. 基于阵列天线的GNSS矢量接收机抗干扰算法研究[D]. 天津:中国民航大学, 2018. (ZHANG Ruihua. Research on anti–jamming algorithm of GNSS vector receiver based on array antenna[D]. Tianjin, China: Civil Aviation University of China, 2018.) doi:10.27627/d.cnki.gzmhy.2018.000023.

[13] 周甍. GNSS诱导式欺骗技术性能研究[D]. 北京:清华大学, 2018. (ZHOU Meng. Research on performance of GNSS induced deception technology[D]. Beijing, China: Tsinghua University, 2018.)

[14] DIETMAYER K, KUNZI F, GARZIA F, et al. Real time results of vector delay lock loop in a light urban scenario[C]// 2020 IEEE/ION Position, Location and Navigation Symposium(PLANS). Portland, OR, USA: IEEE, 2020: 1230–1236. doi: 10.1109/PLANS46316.2020.9109832.

[15] CUNTZ M, KONOVALTSEV A, MEURER M. Concepts, development, and validation of multiantenna GNSS receivers for resilient navigation[J]. Proceedings of the IEEE, 2016,104(6):1288–1301. doi:10.1109/JPROC.2016.2525764.

[16] KAPLAN E, HEGARTY C. Understanding GPS:principles and applications[M]. Massachusetts:Artech House, 2005.

作者简介:

张欣然(1993–),女,博士,助理研究员,主要研究方向为卫星导航抗干扰.email:963453178 @qq.com.

梁涛涛(1988–),男,硕士,副研究员,主要研究方向为卫星导航及信号处理.

陈懋霖(1990–),男,博士,助理研究员,主要研究方向为低轨卫星导航与通信.

(上接第475页)

作者简介:

韩紫杰(1999–),女,在读硕士研究生,主要研究方向为卫星移动通信等.email:22125031@bjtu.edu.cn.

赵连奎(1971–),男,学士,高级工程师,主要研究方向为铁道信号等.

高 媛(1985–),女,硕士,副研究员,主要从事铁路通信技术及标准化研究.

苏昭阳(1998–),男,在读博士研究生,主要研究方向为卫星通信、无线信道建模等.

段相龙(2001–),男,在读硕士研究生,主要研究方向为卫星移动通信等.

周 涛(1988–),男,博士,教授,主要研究方向为通信信号处理、无线信道测量与建模等.

刘 留(1981–),男,博士,教授、博士生导师,主要研究方向为无线信道测量与建模、时变信道信号处理、5G关键技术、高铁宽带接入物理层关键技术等.

尹 毅(1981–),男,硕士,高级工程师,主要研究方向为数字移动通信、调度通信.