doi:10.11887/j.cn.201904019 http://journal.nudt.edu.cn

全球导航卫星系统诱导式欺骗检测*

周 蔓,李 洪,王楚涵,马天翊,陆明泉
(清华大学 电子工程系,北京 100084)

摘 要:随着全球导航卫星系统的广泛应用,其安全性问题也逐渐成为人们关注的焦点。为了对目前最具隐蔽性的诱导式欺骗技术进行检测,提出一种对两路导航信号同时进行处理的 combo-signal 模型,并提出基于这种信号处理模型来对诱导式欺骗信号进行检测的方法;分析了该方法的检测门限;采用北斗的 B1I 和 B1C 信号在实现了 combo-signal 处理模型的软件接收机上对该检测方法进行了验证,实验结果证明该方法可以有效地对诱导式欺骗进行检测,统计得到的检测概率跟前面的分析结果一致。

关键词:全球导航卫星系统;安全性;诱导式欺骗;combo-signal 模型
中图分类号:TN96 **文献标志码**:A **文章编号**:1001-2486(2019)04-129-07

Induced spoofing detection of global navigation satellite system

ZHOU Meng, *LI Hong*, *WANG Chuhan*, *MA Tianyi*, *LU Mingquan*
(Department of Electronic Engineering, Tsinghua University, Beijing 100084, China)

Abstract: With the wide applications of the global navigation satellite system, the security problem of it has gradually become the focus of attention. In order to detect the induced spoofing, the most covert spoofing technology for satellite navigation systems, a combo-signal model which processes two satellite navigation signals simultaneously was proposed. Based on this signal-processing model, a method to detect induced spoofing signals was proposed. Then the detection threshold of the method was analyzed. An experiment with the BeiDou B1I and B1C signals and a software receiver implementing this combo-signal model was used to verify this method. The experimental results show that this method can effectively detect the induced spoofing. The statistics of the detection probability are consistent with the analysis.

Keywords: global navigation satellite system; security; induced spoofing; combo-signal model

全球导航卫星系统(Global Navigation Satellite System, GNSS)的安全性研究已经成为导航系统发展的重点研究问题。在社会经济领域,GNSS 的应用涉及交通、电力、通信、金融等各方各面。GNSS 的安全性和可用性关系着巨大的产业价值。如果 GNSS 信号被干扰,轻则导致 GNSS 用户体验下降,重则造成无法弥补的经济损失。而 GNSS 欺骗,不同于其他类型的干扰,它是一种恶意的破坏,有可能带来灾难性的后果,甚至威胁到人们的人身安全。

为了证明 GNSS 脆弱性[1-3],越来越多的研究机构开始利用 GNSS 欺骗设备对依赖 GNSS 进行授时或导航的终端进行欺骗实验。其中,公开发表文献资料较多的有 Humphreys 及其研究小组,他们成功利用研制的全球定位系统(Global Position System,GPS)欺骗设备[4-5]对电网相位测量单元(Phasor Measurement Unit, PMU)进行欺骗,在开始发送欺骗信号的 1700 ms 后将 PMU 的相位解算结果拉偏 70°。并且,该团队在意大利附近的国际水域上同样通过伪造的 GPS 信号将一艘价值达 8000 万美元的私人游艇引导上偏离计划航线的方向,且航线的偏离并没有触发船舶导航设备的告警。

GNSS 欺骗技术通常有自主生成式、转发式和诱导式三种。自主生成式欺骗[6]利用公开的导航信号接口文件,自主生成导航信号,类似信号模拟源,并用较大的功率夺取接收机的控制权,这种欺骗方式成本低,实现简单,但是生成的欺骗信号与真实信号相差甚远,因此很容易被检测出来。转发式欺骗[7]将接收到的真实信号复制加上延迟后作为欺骗信号转发出来,这种欺骗主要针对接口文件不公开的导航信号,但为了夺取控制权,依然需要提高欺骗信号的功率,并打断接收机的跟踪状态,使其重新进入捕获状态,可以采用功率

* **收稿日期**:2018-03-30
基金项目:国家自然科学基金面上基金资助项目(61571255)
作者简介:周蔓(1980—),女,湖南长沙人,博士研究生,E-mail: maggice-sun@163.com;
陆明泉(通信作者),男,教授,博士,博士生导师,E-mail: lumq@mail.tsinghua.edu.cn

检测法对其进行检测。诱导式欺骗技术是现有的欺骗技术里唯一可以不改变接收机跟踪状态夺取控制权的一种欺骗方式,所以极具隐蔽性,很难用功率检测法等常规方法检测出来,目前对它的检测方法主要有 Delta Metric、Ratio Metric 等[8-9],其基本思想是检测其在欺骗过程中引起的码环信号畸变,但是这种检测手段很难将多径信号与欺骗信号区分开来,因此虚警概率较高。

本文提出一种对两路 GNSS 信号同时进行处理的 combo-signal 模型,这种模型把两路信号等价成一个二进制偏移载波(Binary Offset Carrier, BOC)信号,对新的 BOC 信号进行处理,这使得接收机能够获得比单独处理一路信号更多的观测量,并据此对诱导式欺骗信号固有的载波频率变化进行检测。

1 combo-signal 处理模型

现代 GNSS 的每颗卫星通常都能利用频率复用技术发射多个中心频率不一样的导航信号,接收机可以通过同时处理这些信号来获得更为精准的定位授时结果,例如:利用载波通过电离层的延时与频率平方成反比的特性来设计多频接收机,准确地消除电离层延迟[6-7];或者是对多个频点的测量值进行组合,进行双差或三差定位,消除接收机钟差和载波测量的整周模糊度,提高定位解算和授时精度[10-12]。然而这些处理方式都是对每个频点的信号单独进行处理,无法利用信号之间的相互关系来检测欺骗信号。

如果一对导航信号的时钟源同步,则其载波频率和相位之间的相对关系是已知的,充分利用两者之间的频率和相位关系可以检测到诱导式欺骗信号引起的载波环变化。设这样一组同步的导航信号为(s_1, s_2),且 s_1, s_2 可以用式(1)表示:

$$\begin{cases} s_1(t) = A_1 c_1(t-\tau)\cos(2\pi f_1 t - 2\pi f_1 \tau + \phi_1) \\ s_2(t) = A_2 c_2(t-\tau)\cos(2\pi f_2 t - 2\pi f_2 \tau + \phi_2) \end{cases} \tag{1}$$

其中:$t-\tau$ 代表信号传输时间;f_1、f_2 分别代表两个信号到达接收机时载波的中心频率;A_1、A_2 分别代表两个信号的幅度;ϕ_1、ϕ_2 分别代表两个信号到达接收机时的载波相位;c_1、c_2 分别代表两路信号上面加载的伪码。

如果令 $f'_1 = (f_1 + f_2)/2$, $\phi'_1 = (\phi_1 + \phi_2)/2$, $f'_2 = (f_1 - f_2)/2$, $\phi'_2 = (\phi_1 - \phi_2)/2$,则式(1)与式(2)等价。

$$\begin{cases} s_1(t) = A_1 c_1(t-\tau)\cos[2\pi(f'_1 + f'_2)t - \\ \qquad 2\pi(f'_1 + f'_2)\tau + \phi'_1 + \phi'_2] \\ s_2(t) = A_2 c_2(t-\tau)\cos[2\pi(f'_1 - f'_2)t - \\ \qquad 2\pi(f'_1 - f'_2)\tau + \phi'_1 - \phi'_2] \end{cases} \tag{2}$$

所以接收机接收到的信号可以表示成式(3)。

$$\begin{aligned} s(t) = {} & A_1 c_1(t-\tau)\cos[2\pi(f'_1 + f'_2)(t-\tau) + \phi'_1 + \\ & \phi'_2] + A_2 c_2(t-\tau)\cos[2\pi(f'_1 - f'_2)(t-\tau) + \\ & \phi'_1 - \phi'_2] \end{aligned} \tag{3}$$

如果将式(3)中前后两项的系数进行归一处理,就可以构造出一个新的 BOC 信号,如式(4)所示,其主载波的中心频率为 f'_1,副载波的中心频率为 f'_2。

$$\begin{aligned} s(t) = {} & \cos(2\pi f'_1 t - 2\pi f'_1 \tau + \phi'_1) + \\ & \cos(2\pi f'_2 t - 2\pi f'_2 \tau + \phi'_2) \end{aligned} \tag{4}$$

将可以这样处理的一组导航信号称为一组 combo-signal,这种处理技巧使得接收机只要能同时获取两路同步信号,就可以当成 BOC 信号来处理,从而利用 BOC 调制和解调的优势,对欺骗信号进行检测。实际上,GNSS 中,这样的同步信号有很多,而最适合当成 BOC 信号来处理的有:GPS 的 L1C 与 L1I,Galileo 的 E5A 与 E5B,BD 的 B1C 与 B1I 等。这些信号由同一颗卫星的相同时钟源产生,并经过同样的传播路径到达接收机,因此信号的传播延迟也相同。

对比传统的双路二进制相移键控跟踪(Dual Binary phase shift keying Tracking, DBT)算法,combo-signal 信号的上下两个边带有明显的非对称性,其功率和伪随机码都不相同,因此需要增加归一化处理。对式(3)做相关后,可以得到上下边带的相关值如式(5):

$$\begin{cases} R_u^{\mathrm{d}} = R_u(\Delta\tau)\exp[\mathrm{j}(\Delta\theta + \Delta\varphi)] \\ R_l^{\mathrm{d}} = R_l(\Delta\tau)\exp[\mathrm{j}(\Delta\theta - \Delta\varphi)] \end{cases} \tag{5}$$

其中,$\Delta\theta$ 代表载波相位差,$\Delta\varphi$ 代表副载波相位差,R_{u}、R_{l} 分别代表上下边带相关函数,$R_{\mathrm{u}}^{\mathrm{d}}$、$R_{\mathrm{l}}^{\mathrm{d}}$ 分别代表上下边带相关积分结果。设 w_{u} 和 w_{l} 分别为上下两个边带的功率占比。式(5)中,载波和副载波相位差耦合在一起,可以将式中的相关值对功率分别归一化后,分别求和求差,得到解耦后的载波和副载波相关值表达式为:

$$\begin{cases} R_{\mathrm{c}} = [w_{\mathrm{u}} R_{\mathrm{u}}(\Delta\tau) + w_{\mathrm{l}} R_{\mathrm{l}}(\Delta\tau)]\cos(\Delta\varphi)\exp(\mathrm{j}\Delta\theta) \\ R_{\mathrm{s}} = [w_{\mathrm{u}} R_{\mathrm{u}}(\Delta\tau) + w_{\mathrm{l}} R_{\mathrm{l}}(\Delta\tau)]\cos(\Delta\theta)\exp(\mathrm{j}\Delta\varphi) \end{cases} \tag{6}$$

由式(6)可以看出,通过上下边带的功率倒数对相关值加权,实现了载波和副载波相位差的

解耦,然后使用四象限反正弦鉴相器实现独立鉴相和跟踪,表达式如下所示:

$$\Delta\theta = \arctan2(\mathrm{Im}(R_c),\mathrm{Re}(R_c)) \quad (7)$$

$$\Delta\varphi = \arctan2(\mathrm{Im}(R_s),\mathrm{Re}(R_s)) \quad (8)$$

综上,通过单独的载波环和副载波环分别驱动载波相位和副载波相位的估计值,使之与同相支路对齐,此时上下两个边带的相位也分别对齐,从而实现双边带的载波相位的锁定与跟踪,而且可以得到两路信号的载波相位值和频率值。在这种处理模式下,如果检测到欺骗信号,可以切换到单边带模式,达到反欺骗的效果;而不存在欺骗信号时,可以同时处理双边带信号,从而提高定位精度。

2　基于 combo-signal 模型的诱导式欺骗检测技术

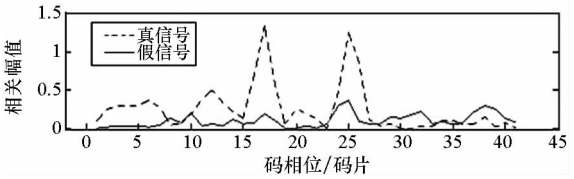
2.1　诱导式欺骗过程分析

典型的诱导式欺骗方法过程如图 1 所示。欺骗信号首先会以极低的功率进入接收机处理环路,使其隐藏在噪声和多径信号中,如图 1(a)所示。然后缓慢地接近真实信号,直到载波相位和码相位跟真实信号对齐。在对齐之后,增加欺骗信号功率,使其略高于真实信号,占据接收机处理环路的主导权,如图 1(b)所示。最后,缓慢地偏离真实信号,使得接收机的载波环路和码环产生的本地码相位逐渐偏离真实信号的相位,如图 1(c)所示,当真实信号与本地码的相位偏差超过环路鉴相器的牵引范围后,接收机的控制权就会完全转移到欺骗信号上,此时,欺骗信号可以随意篡改伪距和导航电文,使得接收机得到错误的定位解算结果。

通过对诱导式欺骗过程的分析可以发现,典型的诱导型欺骗信号在欺骗过程中,为了使本地码的相位发生偏移,它的相位会发生规律性的改变。对于同时接收一对 combo-signal 的接收机来说,如果欺骗信号仅对其中一路信号进行攻击,那么这种规律性的改变可以通过两路信号之间固有的频率和相位相关性检测出来,这就为欺骗信号的检测提供了思路和方法。下面将对此进行详细分析。

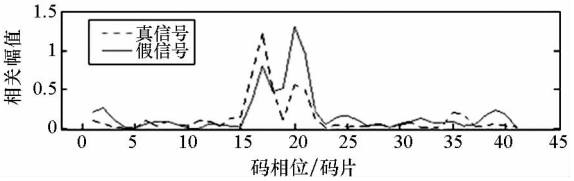
2.2　检测模型

假设:攻击方可以准确获得目标机的速度信息,这对于大多数欺骗场景是可以实现的,例如静态接收机、匀速行进的轮船车辆等;欺骗发生时,接收机是处于对真实信号的稳定跟踪状



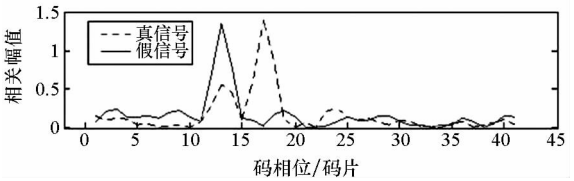
(a) 假信号低功率接近真实信号

(a) Spoofing signal closes real signal with low power



(b) 假信号与真信号对齐并提高功率

(b) Spoofing signal aligns with real signal and increases power



(c) 假信号远离真实信号

(c) Spoofing signal aways from real signal

图 1　诱导式欺骗过程示意

Fig. 1　Process of induced spoofing

态下。因此,在欺骗初始阶段,真实信号的载波频率、欺骗信号的载波频率与接收机产生的本地载波频率,三者一致。但是,通常情况下,欺骗信号的载波相位很难做到跟真实信号的载波相位对齐,两者之间的相位存在差异,将真实信号到达接收机时的载波相位记为 θ_r,欺骗信号到达接收机时的载波相位记为 θ_s,接收机复制的本地载波相位记为 θ_0。锁相环的鉴相结果如式(9)所示:

$$\begin{aligned} u_d(t) &= [u_r(t) + u_s(t)]u_0(t) \\ &= U_0\cos(\omega_0 t + \theta_0)[U_r\sin(\omega_r t + \theta_r) + \\ &\quad U_s\sin(\omega_s t + \theta_s)] \\ &= \frac{1}{2}U_rU_0\{\sin[(\omega_r + \omega_0)t + \theta_r + \theta_0] + \\ &\quad \sin[(\omega_r - \omega_0)t + \theta_r - \theta_0]\} + \\ &\quad \frac{1}{2}U_sU_0\{\sin[(\omega_s + \omega_0)t + \theta_s + \theta_0] + \\ &\quad \sin[(\omega_s - \omega_0)t + \theta_s - \theta_0]\} \end{aligned} \quad (9)$$

其中,$u_r(t)$、$u_s(t)$和 $u_0(t)$分别代表真实信号、欺骗信号和本地复现信号,U_0、U_r 和 U_s 分别代表本地复现信号、真信号和假信号的振幅,ω_0、ω_r 和 ω_s 分别代表三个信号的频率。

信号 $u_d(t)$经过环路滤波器后,高频信号被

滤除,此时输出信号为:

$$u_f(t)=\frac{1}{2}U_rU_0\sin[(\omega_r-\omega_0)t+\theta_r-\theta_0]+\frac{1}{2}U_sU_0\sin[(\omega_s-\omega_0)t+\theta_s-\theta_0] \quad (10)$$

数控振荡器(Numerically Controlled Oscillator, NCO)将根据 $u_f(t)$ 调整本地复制载波 $u_0(t)$ 的频率,最终使得 $u_f(t)$ 趋近于0,此时接收机进入锁定状态。当载波环里只有真实信号存在时,根据式(10),$u_f(t)=0$ 时,$\theta_r=\theta_0$,本地载波对齐,完成锁相。而在真实信号与欺骗信号同时存在时,根据式(10),$u_f(t)=0$ 时会有:

$$U_r\sin[(\omega_r-\omega_0)t+\theta_r-\theta_0]+U_s\sin[(\omega_s-\omega_0)t+\theta_s-\theta_0]=0 \quad (11)$$

根据前面的假设,欺骗信号、真实信号的载波频率都与本地信号的载波频率一致,即 $\omega_r=\omega_s=\omega_0$,式(11)可以进一步简化为:

$$U_r\sin(\theta_r-\theta_0)+U_s\sin(\theta_s-\theta_0)=0 \quad (12)$$

此时,本地载波将不再与真实信号对齐,其相位将是 θ_r 与 θ_s 之间的一个值。如果 $\theta_r-\theta_0$,$\theta_s-\theta_0$ 足够小,则 $\sin(\theta_r-\theta_0)\approx\theta_r-\theta_0$,$\sin(\theta_s-\theta_0)\approx\theta_s-\theta_0$,可以得到:

$$\theta_0=\frac{U_r\theta_r+U_s\theta_s}{U_r+U_s}=\frac{\theta_r+\eta\theta_s}{1+\eta} \quad (13)$$

其中,$\eta=U_s/U_r$ 为欺信比。

由于一组 combo-signal 产生的时钟源一致,而且两路导航信号到接收机的传输路径基本相同,因此,这两路信号的相位可以表述如下:

$$\theta_2(t)=g(\theta_1(t))=(f_2-f_1)t+\theta_2(0)-\theta_1(0)-2\pi N \quad (14)$$

其中:f_1,f_2 分别表示组成 combo-signal 的两路信号的中心频率;$\theta_1(0)$,$\theta_2(0)$ 分别表示两路信号的初始相位,因为两路信号同源,所以可以认为 $\theta_2(0)-\theta_1(0)$ 约等于0;N 代表整周模糊度。

在接收机同时处理这两路信号的情况下,假设欺骗信号对中心频率为 f_1 的信号进行了攻击,将这两路信号的锁相结果做差将得到:

$$\begin{cases}\theta_2-\theta_1'=g(\theta_1)-\dfrac{\theta_1+\eta\theta_s}{1+\eta}\\ \theta_2-\theta_1=g(\theta_1)-\theta_1\end{cases} \quad (15)$$

可以发现,当欺骗信号进入载波环后,这个差值将发生跳变。另外,诱导式欺骗信号的特征是,为了夺取接收机的控制权,其信号会慢慢迁移,表现在载波信号上就是载波相位会以一定速率发生变化,如式(16)所示。

$$\begin{cases}\theta_s(t)=\theta_s(0)+f_1t+f_et\\ \theta_1'(t)=\dfrac{\theta_1(t)+\eta[\theta_s(0)+f_et]}{1+\eta}\\ \theta_2(t)-\theta_1(t)=(f_2-f_1)t-2\pi N\\ \theta_2(t)-\theta_1'(t)=\theta_2(t)-\dfrac{\theta_1(t)+\eta[\theta_s(0)+vt]}{1+\eta}\\ =(f_2-f_1)t+\dfrac{\eta}{1+\eta}f_et-2\pi N+\eta\dfrac{\theta_1(0)-\theta_s(0)}{1+\eta}\end{cases} \quad (16)$$

对式(16)中最后一个等式求导得到

$$\frac{\mathrm{d}[\theta_2(t)-\theta_1'(t)]}{\mathrm{d}t}=(f_2-f_1)+\frac{\eta}{1+\eta}f_e \quad (17)$$

其中,f_e 代表欺骗信号的牵引速度。式(17)表明下边带的载波相位差在出现开始的跳变之后,其斜率也会发生变化,由之前的 f_2-f_1 变成 $(f_2-f_1)+\frac{\eta}{1+\eta}f_e$,叠加了一个欺骗信号牵引速度的加权值。如果欺骗的是上边带信号,同样会有类似的结果。因此,如果上下边带的载波相位差出现跳变,且相位差的变化率同时出现跳变,可以初步判定受到了诱导式欺骗攻击。以北斗系统的 B1I 和 B1C 信号为例进行仿真,在仿真时刻 $t=300$ ns时,加入针对 B1C 信号的诱导式欺骗信号,图2展示了欺骗攻击发生时两路信号载波相位差所发生的变化。从图2中可以明显地看到两路信号的载波相位差在仿真时刻 $t=300$ ns 的地方出现了跳变,且相位差的斜率在此之后也发生了改变。

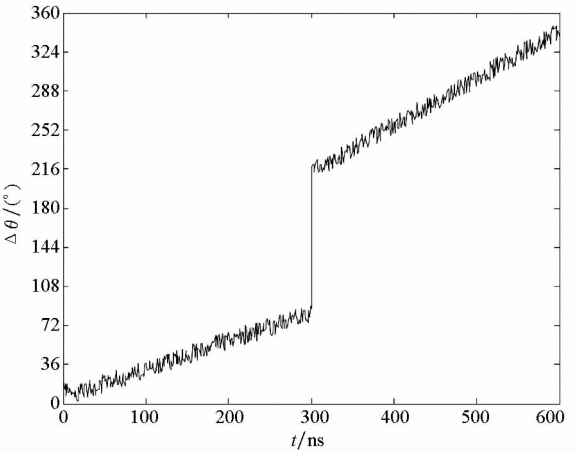


图2 欺骗攻击过程中两路载波相位差变化

Fig. 2 Phase difference change of two carriers in spoofing attack

f_2-f_1 对于一对 combo-signal 来说是已知,因此可以采用 NP(Neyman-Pearson)检测[13]来检测诱导式欺骗攻击是否存在。检测模型如式(18)所示。

$$\begin{cases} H_0: \dfrac{\mathrm{d}[\theta_2(t)-\theta_1(t)]}{\mathrm{d}t} = f_2 - f_1 \\ H_1: \dfrac{\mathrm{d}[\theta_2(t)-\theta_1(t)]}{\mathrm{d}t} = f_2 - f_1 + \dfrac{\eta}{1+\eta} f_e \end{cases} \tag{18}$$

其中,H_0 代表欺骗攻击不存在,H_1 代表欺骗攻击存在。

2.3　检测门限

根据第 1 节提出的 combo-signal 处理模型可以知道 f_1,f_2 是采用独立的载波环进行跟踪,因此可以认为两者的观测量分别为相互独立的、满足均值为 $\overline{f_1}$ 和 $\overline{f_2}$、方差为 σ_{FLL} 的高斯分布。$\overline{f_1}$ 和 $\overline{f_2}$ 为上下边带载波的理论中心频率。σ_{FLL} 为锁频环导致的热噪声频率抖动,根据文献[14]其可以由式(19)进行估算。

$$\sigma_{\mathrm{FLL}} = \frac{1}{2\pi T_{\mathrm{coh}}} \sqrt{\frac{4FB_{\mathrm{L}}}{C/N_0}\left(1+\frac{1}{T_{\mathrm{coh}} \cdot C/N_0}\right)} \tag{19}$$

其中:C/N_0 代表载噪比;F 在 C/N_0 高时取值为 1,否则取值为 2;B_{L} 代表锁频环的噪声带宽;T_{coh} 代表预检相干积分时间。

所以,欺骗信号不存在时,$f_2 - f_1$ 的观测量服从 $\mathrm{N}(\overline{f_2}-\overline{f_1}, 2\sigma_{\mathrm{FLL}}^2)$ 的正态分布;欺骗信号存在时,$f_2 - f_1$ 的观测量服从 $\mathrm{N}(\overline{f_2}-\overline{f_1}+\dfrac{\eta}{1+\eta}f_e, 2\sigma_{\mathrm{FLL}}^2)$ 的正态分布。根据第 2.2 节提出的检测模型,有两种方法确定检测门限:一种是根据式(20),将观测值在两种假设下的概率比 γ 作为判决量;一种是给定虚警概率 P_{fa},确定检测门限。下面分别计算两种方法得到的检测门限。

$$L(x) = \frac{p(x;H_1)}{p(x;H_0)} > \gamma \tag{20}$$

式(20)等效为:

$$\frac{p(x;H_1)}{p(x;H_0)} = \frac{\dfrac{1}{\sqrt{2\pi}}\exp\left\{-\dfrac{1}{4\sigma_{\mathrm{FLL}}^2}\left[x-\left(\overline{f_2}-\overline{f_1}+\dfrac{\eta}{1+\eta}f_e\right)\right]^2\right\}}{\dfrac{1}{\sqrt{2\pi}}\exp\left\{-\dfrac{1}{4\sigma_{\mathrm{FLL}}^2}[x-(\overline{f_2}-\overline{f_1})]^2\right\}} > \gamma \tag{21}$$

因此,判决最终等价于:

$$\exp\left\{\frac{1}{4\sigma_{\mathrm{FLL}}^2}\frac{\eta}{1+\eta}f_e\left[2x-2(\overline{f_2}-\overline{f_1})-\frac{\eta}{1+\eta}f_e\right]\right\} > \gamma \tag{22}$$

等式两边取对数得到:

$$\frac{1}{4\sigma_{\mathrm{FLL}}^2}\frac{\eta}{1+\eta}f_e\left[2x-2(\overline{f_2}-\overline{f_1})-\frac{\eta}{1+\eta}f_e\right] > \ln\gamma \tag{23}$$

即

$$x > \frac{2(1+\eta)\sigma_{\mathrm{FLL}}^2}{\eta f_e}\ln\gamma + \frac{\eta f_e}{2(1+\eta)} + (\overline{f_2}-\overline{f_1}) \tag{24}$$

令

$$\gamma' = \frac{2(1+\eta)\sigma_{\mathrm{FLL}}^2}{\eta f_e}\ln\gamma + \frac{\eta f_e}{2(1+\eta)} + (\overline{f_2}-\overline{f_1})$$

当 $f_2 - f_1$ 的观测量大于 γ' 时,判定欺骗信号存在。此时虚警概率和检测概率如式(25)、式(26)所示。

$$P_{\mathrm{fa}} = \Pr\{x > \gamma'; H_0\} = \frac{1}{2\sqrt{\pi}\sigma_{\mathrm{FLL}}}\int_{\gamma'}^{\infty} \mathrm{e}^{-\frac{[f-(f_2-f_1)]^2}{4\sigma_{\mathrm{FLL}}^2}}\mathrm{d}f \tag{25}$$

$$P_{\mathrm{d}} = \int_{\gamma'}^{\infty}\{x > \gamma'; H_1\} = \frac{1}{2\sqrt{\pi}\sigma_{\mathrm{FLL}}}\int_{\gamma'}^{\infty} \mathrm{e}^{-\frac{[f-(f_2-f_1+\frac{\eta}{1+\eta}f_e)]^2}{4\sigma_{\mathrm{FLL}}^2}}\mathrm{d}f \tag{26}$$

在实际应用中,通常用给定的虚警概率来确定检测门限。利用式(25)即可反解出检测门限 γ',再由式(26)计算检测概率。

从式(26)可以看出,在虚警概率固定情况下,检测概率成为欺信比 η 和欺骗信号牵引速度 f_e 及环路噪声均方差 σ_{FLL} 的函数。检测概率会随着 η 和 f_e 的增加而增加。而且,载噪比 C/N_0 越大,锁频环的噪声带宽 B_{L} 越小,预检相干积分时间 T_{coh} 越大,将导致均方差 σ_{FLL} 越小,同样会使得检测概率增大。

3　实验设计与结果

为了验证 combo-signal 模型的欺骗检测性能,采用北斗的 B1I 和 B1C 信号对其进行了仿真验证。北斗系统的 B1I 和 B1C 信号正是一组中心频点相近的 combo-signal,B1C 信号的中心频点为 1575.42 MHz,B1I 信号的中心频点为 1561.098 MHz,两者同时处理时,等价于一个 BOC(m,n)信号。其中,m = 7 为 B1C 和 B1I 信号中心频点之差的二分之一;n = 2 为扩频码速率。由于 B1I 和 B1C 信号还在实验验证阶段,无法使用真实的卫星信号进行试验,所以采用 MATRIX GNSS - 8440 多标准信号发生器作为 GNSS 信号模拟源对 B1I 和 B1C 信号进行仿真。

实验在清华大学软件接收机平台上进行,该平台实现了对 combo-signal 模型的处理。接收器设备配置包括:Intel(R) Core(TM) i7 - 6700K CPU,主频 4.00 GHz,内存 16.0 GB,NVIDIA GeForce GTX TITAN X GPU。另外,使用定制的信号采集器来实现下变频、采样和滤波,信号采样

率为120 MHz,前端带宽为50 MHz;预检测积分时间为100 ms;载波环路的等效噪声带宽设置为1 Hz,载噪比为30 dB。

3.1 检测概率验证与分析

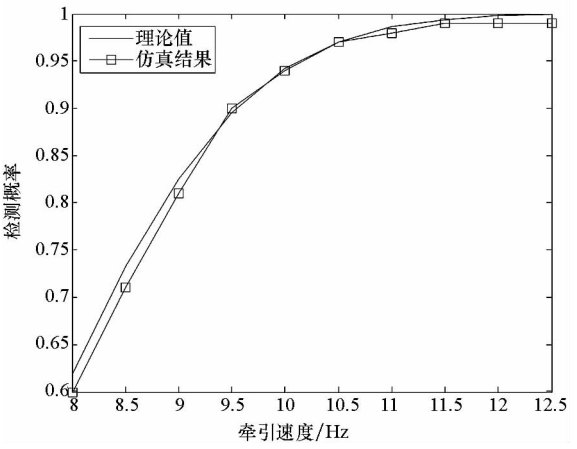
通过一组实验对前面分析得到的检测概率进行验证。在实验开始阶段,模拟源只产生一路信号,将其视为真实信号。当接收机收到这路信号并进入稳定跟踪状态后,模拟源开始发射欺骗信号。真假信号的载波相位之间有一个差值,而且此时欺骗信号的功率远低于真实信号。慢慢调整欺骗信号的载波相位使其与真实信号对齐;在对齐后,增加欺骗信号的功率,使其大于真实信号;再次调整欺骗信号的载波相位使其慢慢远离真实信号。这样就模拟了诱导式欺骗信号夺取接收机处理环路的整个过程。

设定虚警概率为 1×10^{-6},根据式(25)计算得到的检测门限为 $\gamma'=18.83$ Hz。固定欺信比为1.5,欺骗信号牵引速度即真假信号相对频率差 f_e 设置为8~12.5 Hz,间隔0.5 Hz。绘制与检测门限 γ' 对应的检测概率曲线,如图3(a)中的实线所示。在相同设置下用模拟信号重复100次得到检测概率的统计结果,如图3(a)中的带方框的折线所示。再将 f_e 固定为10 Hz,欺信比设置为1.1~2,间隔0.1。绘制与检测门限 γ' 对应的检测概率曲线,如图3(b)中的实线所示,在相同设置下用模拟信号重复100次得到检测概率的统计结果,如带方框的折线所示。

比较实验统计结果和理论曲线发现实验结果与理论曲线基本吻合。从图中可以看到,欺骗信号的牵引速度对检测概率的影响很大,欺信比取值为1.5、f_e 等于8 Hz时,检测概率只有62%;一旦 f_e 达到10 Hz以上,检测概率明显提高,可以达到90%以上。如果牵引速度取值为10 Hz,欺信比只要大于1.4,就可以有90%以上的检测概率。综上所述,该方法可以对欺信比大于1.4或牵引速度大于10 Hz的诱导式欺骗信号进行有效检测。

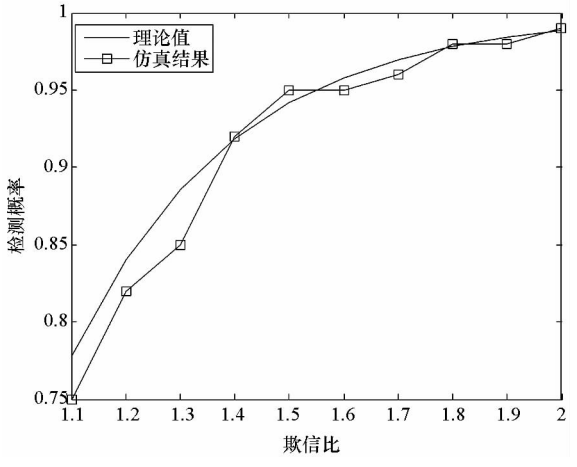
3.2 多径信号虚警概率改进验证

通过实验验证该检测算法在特定环境下可以将多径与欺骗信号区分开来,降低虚警概率。模拟源产生两路信号,一路作为真实信号,另一路为多径信号。多径信号与真实信号的载波相位之间存在一个固定差值,且功率低于真实信号,但频率与真实信号一致。分别采用基于combo-signal模型的检测算法、Delta Metric和Ratio Metric算法对信号进行检测,三种算法对欺骗信号的检测概率



(a) 牵引速度对检测概率的影响

(a) Influences of traction speed on detection probability



(b) 欺信比对检测概率的影响

(b) Influences of spoof-signal ratio on detection probability

图3 仿真结果与理论值比对

Fig. 3 Comparison of simulation results with theoretical values

设定为95%,在此条件下统计三种算法将多径信号误判为欺骗信号的概率。实验结果如图4所示,横坐标代表多径信号与真实信号的振幅比,纵坐标代表将多径信号误判为欺骗信号的概率。

分析实验结果得到结论:本文提出的检测算法将多径信号误判为欺骗信号的概率远低于Delta Metric算法和Ratio Metric算法。这是由于多径信号与真实信号的载波相位差一直维持不变(在接收机和多径信号源之间的相对距离不发生改变的情况下成立),因此两路信号之间的频率差不会出现变化,检测算法不会发出预警。因此本文的算法对于改善该环境下的检测虚警概率显然是有效的。但在接收机和多径信号源之间的相对距离发生改变时,多径信号与真实信号之间也会出现频率差,本文所提出的检测算法就很难进行有效的区分了。在今后的工作中,可以进一步

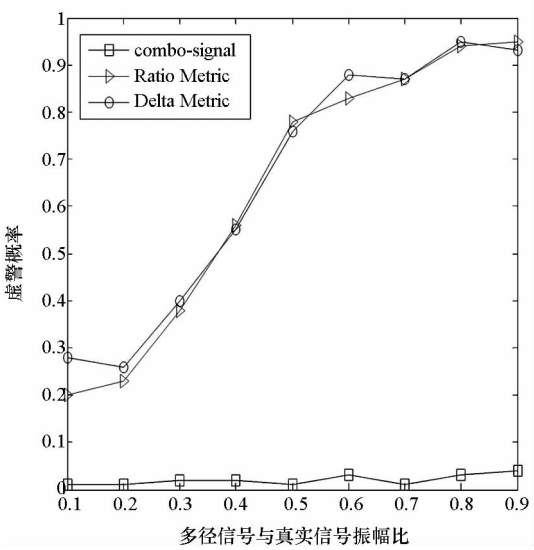


图 4 多径虚警概率对比

Fig. 4　Comparison of false alarm probability caused by multipath

研究该情况下算法的改进。

4　结论

本文提出的基于 combo-signal 处理模型的检测方法,有效利用了两路同源 GNSS 信号载波频率和相位的相对关系来检测诱导式欺骗攻击。实验结果表明该检测方法可以对大部分诱导式欺骗攻击进行有效检测,而且当接收机和多径信号源之间的相对距离不发生改变时,可以有效地将多径信号与欺骗信号区分开来,降低虚警概率。

参考文献(References)

[1] Carroll J V. Vulnerability assessment of the U. S. transportation infrastructure that relies on the global positioning system[J]. Journal of Navigation, 2003, 56(2): 185 – 193.

[2] Warner J S, Johnston R G. A simple demonstration that the global positioning system (GPS) is vulnerable to spoofing[J]. Journal of Security Administration, 2002, 25: 19 – 27.

[3] Shepard D P, Humphreys T E, Fansler A A. Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks[J]. International Journal of Critical Infrastructure Protection, 2012, 5(3/4): 146 – 153.

[4] Humphreys T E, Ledvina B M, Psiaki M L, et al. 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, 2008: 2314 – 2325.

[5] Shepard D. Characterization of receiver response to spoofing attacks[C]. Proceedings of International Technical Meeting of the Satellite Division of the Institute of Navigation, 2011, 10(1): 2608 – 2618.

[6] Hatch R R, Sharpe R T, Yang Y C. An innovative algorithm for carrier-phase navigation[C]//Proceedings of ION GNSS, Long Beach, CA, USA, 2004.

[7] Kaplan E D. Understanding GPS principles and applications[M]. 2nd ed. Boston, MA, USA: Artech House, 2006.

[8] Magiera J, Katulski R. Accuracy of differential phase delay estimation for GPS spoofing detection[C]//Proceedings of International Conference on Telecommunications and Signal Processing, 2013: 695 – 699.

[9] Bastide F, Chatre E, Macabiau C. GPS interference detection and identification using multi-correlator receivers[J]. Masui the Japanese Journal of Anesthesiology, 2001, 48(11): 1229 – 1231.

[10] Hofmann-Wellenhof B, Lichtenegger H, Collins J. Global positioning system (GPS): theory and practice[M]. Vienna, Austria: Springer, 1992.

[11] Greenspan R L, Ng A Y, Przyjemski J M, et al. Accuracy of relative positioning by interferometry with reconstructed carrier, GPS experimental results[C]//Proceedings of 3rd International Geodetic Symposium on Satellite Doppler Positioning, Las Cruces, NM, 1982.

[12] Paielli R A, McNally B D, Bach R E, et al. Carrier phase differential GPS for approach and landing: algorithms and preliminary result[C]//Proceedings of the 6th International Technical Meeting, ION GPS – 90, 1990.

[13] Kay S M. Fundamentals of statistical signal processing volume I: estimation theory[M]. Beijing: Publishing House of Electronics Industry, 2011.

[14] Betz J W, Kolodziejski K R. Extended theory of early-late code tracking for a bandlimited GPS receiver[J]. Journal of the Institute of Navigation, 2000, 47(3): 211 – 226.