http://bhxb.buaa.edu.cn jbuaa@buaa.edu.cn
DOI: 10.13700/j.bh.1001-5965.2019.0303

同步式 GPS 欺骗干扰信号生成技术研究与设计

柳亚川，寇艳红*
（北京航空航天大学 电子信息工程学院，北京 100083）

摘 要：出于对“低、慢、小”无人机进行导航定位诱骗的实际需求，在实验室原有的异步生成式 GPS 欺骗干扰源的基础上，研制了一种小型化的同步生成式 GPS 欺骗干扰源。首先，在异步生成式 GPS 欺骗干扰源射频信号模型的基础上，考虑到干扰源信号处理延时、欺骗信号的传播延时、无人机上目标接收机所接收真实卫星信号状态以及无人机运动模型，建立了对同步欺骗信号仿真时间和状态参数进行精确计算的数学模型。其次，通过本地授时型接收机提供驯服后的基准时钟和秒脉冲(1PPS)信号，实现欺骗干扰信号与真实卫星信号系统时的同步，并通过高阶直接数字频率合成(DDS)技术精确控制信号参数，保证欺骗信号到达目标接收机接收天线相位中心时与真实信号的相位状态在成功诱骗所允许的误差范围之内。最后，通过商用接收机和无人机进行了实验验证，在无人机上目标接收机正常跟踪真实卫星信号的前提下，开启同步生成式 GPS 欺骗干扰源发射欺骗信号，能够使目标接收机逐渐偏离正常定位测速结果而产生受控的定位测速结果。结果验证了同步信号模型和所设计同步信号生成电路的正确性，且表明同步生成式 GPS 欺骗干扰源能够实现对商用接收机和无人机导航定位的诱骗。

关 键 词：GPS 欺骗干扰源；同步生成式；时基同步；同步信号模型；无人机(UAV)诱骗
中图分类号：V249；TN972+.3
文献标志码：A **文章编号**：1001-5965(2020)04-0814-08

目前，无人机技术日趋成熟，应用迅速增多，飞行频次和飞行范围急剧增加，在提供方便的同时对于飞行安全提出了巨大的挑战[1]。民用无人机价格低廉、购买途径众多、操作门槛低、对起飞环境要求低，当前出现了大量黑飞无人机，一些未经审核的黑飞事件造成了严重的恶性影响，因此有必要对无人机实施监测，必要时进行强制管控。从 GPS 欺骗干扰技术着手管制无人机，具有较强的威胁性和隐蔽性，正逐渐成为当下无人机管制研究领域的热点之一[2]。

GPS 欺骗式干扰可分为转发式欺骗干扰和生成式欺骗干扰[3-5]，前者通过对真实卫星信号的延迟和转发达到欺骗目的，后者则通过自主生成携带虚假导航信息的卫星导航信号实现欺骗。根据所生成欺骗信号是否与真实卫星信号同步，又可将生成式欺骗干扰分为异步生成式与同步生成式欺骗干扰[6-8]。异步生成式欺骗干扰技术相对较为成熟，可由卫星导航射频信号模拟器实现，但一般需要借助于压制式干扰阻断接收机对真实卫星信号的跟踪，在确保干扰区域内接收机重新进入搜索捕获状态后才可有效实施欺骗干扰；而同步生成式欺骗干扰则可在接收机正常跟踪真实卫星信号的状态下无需压制而引导接收机逐渐偏离真实信号，控制目标接收机的定位测速，因而更难以被目标接收机所察觉。由于同步生成式欺骗干扰技术较为复杂，目前公开的相关文献中，大多只

收稿日期：2019-06-17；**录用日期**：2019-11-17；**网络出版时间**：2019-11-25 14:03
网络出版地址：kns.cnki.net/kcms/detail/11.2625.V.20191125.1339.002.html
* **通信作者**. E-mail：kouy@buaa.edu.cn

引用格式：*柳亚川，寇艳红. 同步式 GPS 欺骗干扰信号生成技术研究与设计[J]. 北京航空航天大学学报，2020，46(4)：814-821. LIU Y C，KOU Y H. Research and design of synchronous GPS spoofing signal generation technology [J]. Journal of Beijing University of Aeronautics and Astronautics，2020，46(4)：814-821 (in Chinese).*

是通过理论分析和软件仿真对欺骗干扰进行验证[9-11],缺乏真实场景下的设计验证以及实验测试[12]。

本文旨在研究同步式 GPS 欺骗干扰信号生成技术,建立了同步 GPS 欺骗信号的数学模型,给出了信号参数仿真、信号同步及诱骗方法;在此基础上,基于数字信号处理(Digital Signal Processing,DSP)芯片和现场可编程逻辑门阵列(Field Programmable Gate Array,FPGA)架构研制了一种小型化的同步生成式 GPS 欺骗干扰源。最终通过室内商用接收机测试和室外商用无人机测试,在接收机和无人机锁定真实卫星信号以及不使用高功率干扰压制的前提下,开启干扰源,发射欺骗信号,成功诱使接收机和无人机逐渐偏离真实定位测速结果而输出预设的定位测速结果,从而验证了信号模型和诱骗方法的正确性以及所设计同步式 GPS 欺骗干扰源设备的有效性。

1　同步生成式 GPS 欺骗干扰

1.1　GPS 欺骗干扰源总体设计

在实验室已有的异步生成式 GPS 欺骗干扰源基础上[13],本文所设计的便携式小型化同步生成式 GPS 欺骗干扰源组成框图如图 1 所示(1PPS 为秒脉冲),主要由信号处理模块、参考接收模块、上变频及射频调理模块、上位机主控模块组成。信号处理模块采用 DSP + FPGA 的架构,完成欺骗信号仿真计算并生成中频欺骗信号;参考接收模块以某款授时型接收机为基础,完成干扰源系统时和真实卫星系统时的同步,并提供时基信号、时间信息、位置信息和导航参数等给信号处理模块;上变频及射频调理模块完成中频信号的上变频和信号调理;上位机主控模块实现人机交互以及与导航诱骗系统中其他组件(如目标侦测系统)的数据交互和命令控制。

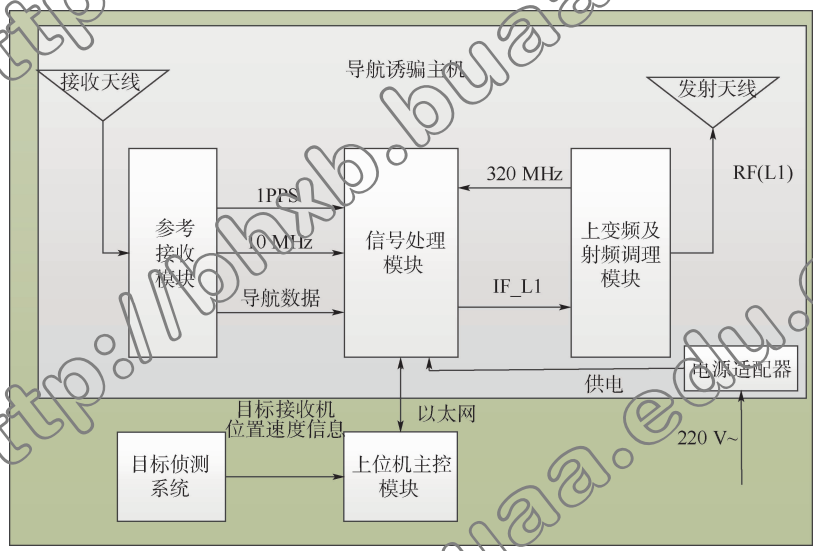


图 1　同步生成式 GPS 欺骗干扰源组成框图

Fig. 1　Block diagram of synchronous generator GPS spoofer

1.2　同步生成式 GPS 欺骗干扰信号的生成

1.2.1　欺骗信号模型

在 GPS 系统时 t 时刻欺骗干扰源所发射的射频信号可表示为[13-14]

$$x_{\mathrm{RF}}(t) = \sum_{j=1}^{N(t)} \sqrt{2P_{\mathrm{s}}^{j}(t)}\, C^{j}(t-\tau^{j}(t)) \cdot D^{j}(t-\tau^{j}(t)) \cos(\phi^{j}(t)) + n(t) \quad (1)$$

式中:t 为信号发射时刻的 GPS 系统时;$N(t)$ 为对应 t 时刻的目标接收机处可见卫星数;$P_{\mathrm{s}}^{j}(t)$ 为第 j 颗可见星信号功率;$C^{j}(t-\tau^{j}(t))$ 为第 j 颗可见星的伪随机码;$\tau^{j}(t)$ 为 t 时刻伪随机码传播延时;$D^{j}(t-\tau^{j}(t))$ 为第 j 颗可见星导航电文数据;$\phi^{j}(t)$ 为第 j 颗可见星载波相位;$n(t)$ 为随机噪声。

1.2.2　初始同步阶段的信号参数计算

同步生成式 GPS 欺骗干扰源能够生成当前目标接收机所有可见星的同步欺骗信号,欺骗信号到达目标接收机天线相位中心处的功率、码相位、载波多普勒和载波相位与真实信号的对齐误差要限制在一定的范围之内。同步生成式 GPS 欺骗干扰源根据本地授时型接收机提供的信息和时基信号计算并控制所仿真各历元时刻各颗卫星欺骗信号的功率、码相位、载波多普勒和载波相位参数,生成相应的射频欺骗信号通过发射天线向目标空域发射出去。

1)功率

图2为功率估计示意图,其中r_{sj}为卫星发射

http://bhxb.buaa.edu.cn

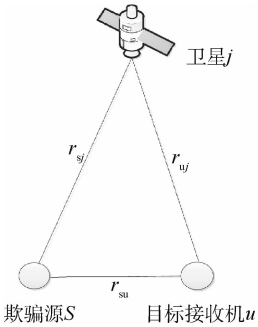


图 2 功率计算示意图

Fig. 2 Schematic diagram of power calculation

天线相位中心到欺骗干扰源接收天线相位中心的距离,r_{uj}为卫星发射天线相位中心到目标接收机接收天线相位中心的距离,r_{su}为欺骗干扰源发射天线相位中心到目标接收机接收天线相位中心的距离。干扰源与目标接收机均使用全向接收天线。

通常 r_{sj}和 r_{uj}均远大于 r_{su},到达欺骗干扰源接收天线相位中心和目标接收机接收天线相位中心的卫星信号功率近似相等,因此由干扰源处卫星信号功率估计目标接收机处卫星信号功率。

干扰源仿真的第 j 颗可见星信号功率计算公式为

$$P_s^j(t) = P_u^j(t) + \Delta P^j(t) - G_T(t) + 20\lg\frac{4\pi r_{su}(t)}{\lambda} \tag{2}$$

式中:$P_u^j(t)$为 t 时刻真实卫星信号功率,可由本地授时型接收机估计;$\Delta P^j(t)$为根据同步诱骗策略需要添加的欺骗信号相对于真实卫星信号功率的增量;$G_T(t)$为欺骗干扰源发射天线增益;λ 为信号波长。

2)码相位

t 时刻干扰源所仿真第 j 颗可见星的码相位延迟可由下式进行估计:

$$\tau^j(t) = \frac{1}{c}\left|p_{sv}^j(t_T^j(t)) - p_u(t+\tau_{su})\right| + \tau_{iono}^j(t) + \tau_{trop}^j(t) + \tau_{rel}^j(t) + \Delta\tau^j(t) \tag{3}$$

$$\tau^j(t) = t + \tau_{su} - t_T^j(t) \tag{4}$$

式中:c 为光速;$t_T^j(t)$为所仿真的第 j 颗可见星信号从卫星发射的时刻(GPS 系统时);$p_{sv}^j(t_T^j(t))$为卫星信号发射时刻的卫星位置;$\tau_{su} = r_{su}/c$ 为从欺骗干扰源发射天线相位中心到目标接收机接收天线相位中心的信号传播时间;$p_u(t+\tau_{su})$为 GPS 系统时 $t+\tau_{su}$时刻(目标接收欺骗信号时刻)的目标无人机天线相位中心位置;$\tau_{iono}^j(t)$为电离层延迟;$\tau_{trop}^j(t)$为对流层延迟;τ_{rel}^j为相对论效应引起的延迟;$\Delta\tau^j(t)$为根据同步诱骗策略需要添加的欺骗信号相对真实卫星信号码相位的增量。

式(3)与式(4)的右端有两对参数的计算存在相互依赖关系,需要通过二分法迭代求解[14]。在实现时基同步后可精确读取干扰源信号发射时刻 t,τ_{su}可以由已事先测定的干扰源发射天线相位中心位置 $p_s(t)$与 $t+\tau_{su}$时刻的接收天线相位中心位置 $p_u(t+\tau_{su})$计算,即 $\tau_{su} = (p_s(t) - p_u(t+\tau_{su}))/c$,其中 τ_{su}与 $p_u(t+\tau_{su})$的计算可以采用二分法迭代得到,迭代误差控制在伪距控制误差之内;之后,将 τ_{su}代入式(4),再将式(4)代入式(3)消去 $\tau^j(t)$,用二分法迭代计算得出卫星信号发射时刻 $t_T^j(t)$和卫星信号发射时刻卫星的位置 $p_{sv}^j(t_T^j(t))$;$\tau_{iono}^j(t)$计算模型为 Klobuchar 模型;$\tau_{trop}^j(t)$计算模型为改进的 Hopfield 模型;τ_{rel}^j的计算式为

$$\tau_{rel}^j = Fe\sqrt{A}\sin(E_k(t)) \tag{5}$$

式中:$F = -4.442\,807\,633\times10^{-10}$ s/m;e 为卫星轨道偏心率;A 为卫星轨道的半长轴;$E_k(t)$为卫星轨道的偏近点角[15]。

在初始同步与功率增强阶段,以及动态调整阶段,码相位增量 $\Delta\tau^j(t)$的取值不同,具体分析见 1.2.3 节。

区别于普通模拟器,如图 3 所示,同步生成式 GPS 欺骗干扰源需要精确控制到达目标的信号状态,相应地需要精确控制欺骗信号发射时刻(GPS 系统时)。由于扰源本地授时型接收机可以获得其接收天线接收真实卫星信号的时刻,而该时刻到干扰源发射天线发射欺骗信号时刻的延时 t_d(称为诱骗系统信号处理延时)则可事先标定,然后在信号产生过程中予以补偿。

3)载波多普勒

同步生成式 GPS 欺骗干扰源需要控制产生的第 j 颗卫星欺骗信号的载波多普勒为

$$f_{d,s}^j(t) = f_{d,u}^j(t) - f_{d,su}(t) + \Delta f_d^j(t) \tag{6}$$

$$\Delta f_d^j(t) = f_{d,u'}^j(t) - f_{d,u}^j(t) \tag{7}$$

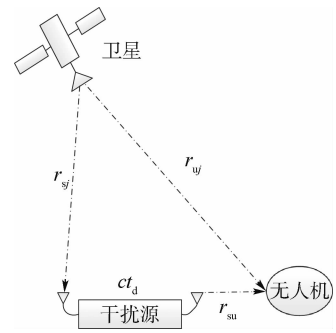


图 3 码相位计算示意图

Fig. 3 Schematic diagram of code phase calculation

http://bhxb.buaa.edu.cn

式中:$f_{d,u}^{j}(t)$为目标接收机真实位置与该颗卫星之间的多普勒频移;$f_{d,su}(t)$为干扰源与目标接收机真实位置之间多普勒频移;$\Delta f_{d}^{j}(t)$为根据同步诱骗策略需要叠加的欺骗信号相对于真实卫星信号载波多普勒频移增量;$f_{d,u'}^{j}(t)$为根据同步诱骗策略计算的目标接收机欺骗位置与该颗卫星之间的多普勒频移。可根据卫星位置、目标接收机真实位置和目标接收机欺骗位置计算距离变化率从而计算$f_{d,u}^{j}(t)$、$f_{d,su}(t)$和$f_{d,u'}^{j}(t)$,或者由卫星速度、目标接收机真实速度和目标接收机欺骗速度计算$f_{d,u}^{j}(t)$、$f_{d,su}(t)$和$f_{d,u'}^{j}(t)$,本文设计中采用第 1 种方法。

1.2.3　信号同步及诱骗方法

1)时基同步

欺骗信号与真实卫星信号同步精度取决于干扰源的欺骗信号参数计算和控制精度以及干扰源控制信号发送时刻的精度。时基同步是为了保证欺骗干扰源与真实卫星系统时保持时间上的同步,并能够标定和校准从接收卫星信号到发送欺骗信号的时延t_{d}。

为了实现时基同步的功能,本文方案采用一个本地授时型接收机,能够提供精度满足要求的驯服后的基准时钟和 1PPS 信号。干扰源通过本地授时型接收机读取当前 GPS 时,并利用 1PPS 信号和 10 MHz 时钟作为 FPGA 数字信号合成和射频模块信号输出的时基和时钟源,实现干扰源本地时钟和真实卫星系统时的同步;同时依据 1.2.1 节的欺骗信号模型和信号参数估计方法,计算导航观测量和电文参数,并通过高阶直接数字频率合成(Direct Digital Synthesis,DDS)技术精确控制信号状态,高阶 DDS 使用 FPGA 片内资源,进行多级调整,精确地模拟由卫星和接收机相对运动引起的多普勒变化,保证欺骗信号到达目标接收机接收天线相位中心时与真实信号的相位状态在成功诱骗所允许的误差范围之内。

2)目标接收机跟踪环路的俘获

为了避免欺骗信号被目标接收机识别,可将欺骗干扰源俘获目标接收机跟踪环路的过程分为以下 2 个阶段[16]:①初始同步与功率增强阶段,②动态调整阶段。如图 4 所示,在初始同步与功率增强阶段,初始的欺骗信号功率应低于真实卫星信号功率,此时 $\Delta P^{j}(t)<0$,信号相位误差与多普勒误差状态应保持在一定范围内,欺骗位置和接收机真实位置 $p_{u}(t+\tau_{su})$ 一致,此时码相位增量 $\Delta\tau^{j}(t)$ 和 $\Delta f_{d}^{j}(t)$ 为 0;随后逐步通过增加欺骗信号的功率,即逐渐增大$\Delta P^{j}(t)$,最终使欺骗信号功率高于真实卫星信号功率[16],使欺骗信号获得目标接收机跟踪环路的主导权。为了确保欺骗信号功率升高过程中不易引起目标接收机警觉,并且能稳定控制目标接收机跟踪环路,应保证功率升高过程平稳且缓慢,以一定的增速持续足够长的时间直至功率最终达到某一合适值。

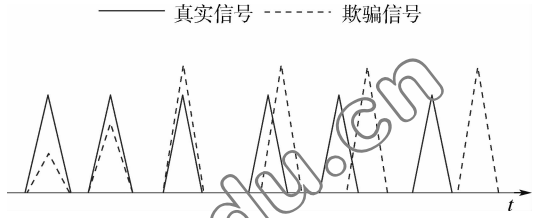


图 4　欺骗信号俘获跟踪环路示意图

Fig. 4　Schematic diagram of tracking loop captured by spoofing signal

在俘获目标接收机跟踪环路主导权之后,进入动态调整阶段,通过对欺骗信号所仿真目标接收机动态进行调整,此时欺骗位置不再为 $p_{u}(t+\tau_{su})$,而是根据设定的欺骗轨迹,改变干扰源欺骗信号仿真的欺骗位置,根据 1.2.2 节的推导公式计算码相位和载波多普勒,调整码相位增量 $\Delta\tau^{j}(t)$ 和载波多普勒增量 $\Delta f_{d}^{j}(t)$,牵引目标接收机跟踪环路逐步脱离真实卫星信号,完成整个诱骗过程。

鉴于目前大多数 GPS 接收机所采用的 3 阶或 3 阶以下载波跟踪锁相环路(PLL),以及恒定速度的突变会引起欺骗信号多普勒突变,易被接收机检测识别[15],因此本设计欺骗信号采用初始速度为 0 的匀加速动态调整策略,并在速度达到最大值后,保持不变,即

$$v(t)=\begin{cases}at & at\leqslant v_{\max}\\ v_{\max} & at>v_{\max}\end{cases} \tag{8}$$

式中:$v_{\max}$为最大速度;a 为加速度,其大小受限于接收机 PLL 噪声带宽以及 PLL 更新周期。

欺骗信号动态调整过程,若加速度和最大速度增大,则需增大欺骗信号的功率保证成功欺骗目标接收机[16],因此欺骗信号加速度和最大速度不应设置过大。

2　实验分析

为了验证上述模型的正确性及方法和设计的可行性,本文首先在室内利用商用接收机进行了静态诱骗实验,然后在室外利用商用无人机分别进行了静态和动态诱骗实验。其中室外无人机动态诱骗实验参数具体设置见 2.2 节无人机动态诱

http://bhxb.buaa.edu.cn

骗测试部分;而室内商用接收机及室外无人机静态诱骗实验参数设置如下:

1)初始同步与功率增强阶段

欺骗信号初始仿真位置为目标接收机真实位置 $p_u(t+\tau_{su})$,仿真的接收机动态速度为 0,加速度为 0;初始欺骗信号功率低于真实卫星信号功率,功率增加速率为 2 dB/s,持续时间为 8 s。

2)动态调整阶段

欺骗信号功率保持初始同步阶段最大功率,改变欺骗信号所仿真的目标无人机的动态,在地心固地坐标系(ECEF)直角坐标系下 x 方向初始速度为 0,加速度为 0.2 m/s^2,最大速度为 3.8 m/s,y 方向和 z 方向速度恒为 0。

2.1 室内商用接收机诱骗测试

1)码相位同步精度测试

使用 2 个商用接收机(Trimble Mini-T^{TM} GG 和 NovAtel OEM615)分别接收真实卫星信号和干扰源欺骗信号,输出秒脉冲,使用 TDS3052B 示波器测试 2 个秒脉冲的对齐精度,接收干扰源欺骗信号接收机输出的秒脉冲与接收真实卫星信号接收机输出的秒脉冲对齐误差的测试结果截图如图 5所示,测试阶段为初始同步与功率增强阶段。

多次测试结果表明 2 个接收机输出的秒脉冲对齐误差小于 100 ns,即 0.1 个码片;这保证了干扰源产生的欺骗信号与真实卫星信号到达目标接收机时的时间同步[2,10,17]。

2)载噪比测试

在一定的热噪声背景下,卫星信号绝对功率的变化直接体现在射频信号载噪比的变化上[18],本文通过测试接收机接收信号载噪比变化验证欺骗信号功率变化对接收机跟踪环路的影响,测试阶段为初始同步与功率增强阶段。

采用北京卫信杰科技发展有限公司的 W220 接收机作为室内测试的目标接收机,其射频输入端同时连接干扰源射频输出与实验室屋顶天线;起初只接收真实卫星信号,待接收机稳定输出

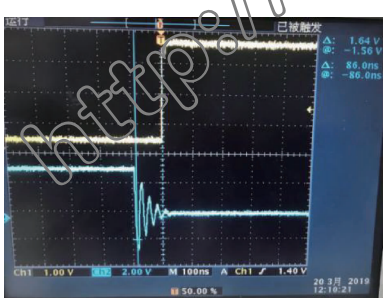


图 5 秒脉冲误差测试结果

Fig. 5 Test results of 1PPS error

真实坐标(39.978 635°N,116.344 224°E,70 mH)后,在不对此接收机进行压制干扰的前提下,开启干扰源,首先输出低功率的同步欺骗信号,可观察到接收机定位不受影响,定位没有中断;然后在第 5 s开始逐步增加干扰信号功率,每秒增加 2 dB,持续 8 s,随后保持功率不变。读取接收机所记录的每秒一次的可见星 PRN8、PRN21、PRN26 载噪比如图 6 所示。

以 PRN8 载噪比为例,由图 6 可见,在第 1 ~ 4 s干扰源发射低功率欺骗信号,接收机所跟踪真实卫星信号的载噪比均不超过 43 dB · Hz;第 5 ~ 6 s 欺骗信号功率增加但仍低于真实卫星信号功率,接收机跟踪环路保持锁定真实卫星信号,所估计载噪比没有明显变化;第 7 ~ 12 s 欺骗信号功率高于真实卫星信号功率,接收机跟踪环路锁定欺骗信号,因此接收机所估计载噪比随欺骗信号功率提高而提高。值得注意的是,实验中发现欺骗信号高功率入侵诱骗成功的概率更高,而低功率入侵有时会引起定位中断,其原因是干扰源所发射欺骗信号很难做到与真实卫星信号载波相位完全同步,在相差较大甚至反相的情况下容易引起信号短暂失锁。

3)接收机定位测速诱骗测试

初始设置及信号功率变化与载噪比测试设置一致,随后从第 30 s 开始逐步增加干扰源所仿真目标在 ECEF 直角坐标系下 x 方向上的速度,初始速度为 0,加速度为 0.2 m/s^2,持续时间为 19 s,y 方向和 z 方向速度保持为 0,实验结果如图 7 所示。由图中可知,接收机定位测速结果与预设轨迹速度相吻合,接收机被成功诱骗到干扰源所预设的定位测速结果。

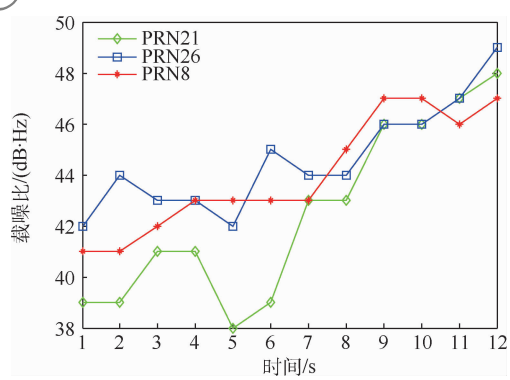


图 6 载噪比测试结果

Fig. 6 Test results of carrier to noise ratio

2.2 室外无人机诱骗测试

1)无人机静态诱骗测试

实验场地为北京航空航天大学,使用的无人机为大疆创新科技有限公司的 PHANTOM 4 PRO

http://bhxb.buaa.edu.cn

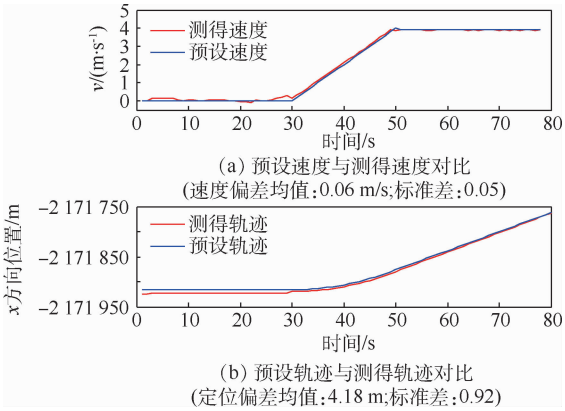


图 7　接收机定位测速结果与预设轨迹速度的比较

Fig. 7　Comparison of receiver position and velocity results with preset trajectory and velocity

无人机。首先使无人机接收真实卫星信号，在定位之后且不对无人机进行压制的前提下，打开干扰源发射欺骗信号，诱骗方法同室内测试相同。采用 DJI Assistant 2 调参软件来观测无人机传感器给出的飞行轨迹，软件所显示的无人机定位位置偏离起始点的距离随运行时间的变化如图 8 所示。可见无人机定位一直没有中断，在开启干扰源后逐步锁定到欺骗信号，从图 8 中的第 72 s 开始其输出的定位位置发生移动。由于无法从 DJI Assistant 2 软件导出无人机定位轨迹的记录数据，本文同时使用了 W220 接收机与无人机一起进行诱骗实验。图 9(a)对比了 W220 接收机定位轨迹和干扰源预设欺骗轨迹；图 9(b)对比了无人机偏离起始点距离(由图 8 读数绘制而成)以及 W220 接收机定位结果偏离起始点的距离。

由图 8 和图 9 可见，W220 接收机输出的定位测速结果与预设的欺骗轨迹相符合；无人机配套软件所输出偏离起始点的距离与接收机定位结果偏离起始点距离相符合，可说明在开启干扰源后，无人机定位未中断，由锁定真实卫星信号转而锁定欺骗信号，并且输出干扰源预设的欺骗轨迹，无人机欺骗成功。

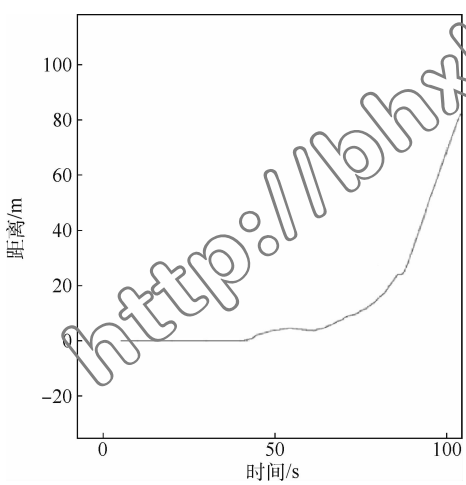


图 8　DJI Assistant 2 所显示无人机偏离起始点的距离

Fig. 8　Distance of UAV deviated from origin displayed by DJI Assistant 2

2）无人机动态诱骗测试

无人机动态诱骗实验设备及环境如图 10 所示，实验场地为北京市沙河非禁飞区，通过无人机定位，显示当地真实坐标为(40.176 698° N，116.269 926° E)。

图 11(a)为无人机动态诱骗实验的场景设计(V_{UAV} 为无人机初始速度，V_s 为欺骗速度)，图 11(b)～(d)给出了实验过程中无人机通过关键轨迹点的视频截图。

首先通过无人机遥控软件 DJI GO 4 预设无人机匀速由 A 点(40.176 698° N，116.269 926° E)飞往 B 点(40.176 582° N，116.269 952° E)，飞行速度为 0.3 m/s。在不对无人机进行压制干扰的前提下，开启干扰源，首先输出低功率的同步欺骗信号，可观察到无人机由预设的起始位置即图 11(b)中的 A 点向预设的 B 点方向正常飞行(若欺骗信号引起无人机接收机失锁，则无人机会悬停)，在飞行时刻第 5 s 开始逐步增加欺骗信号功率，每秒增加 2 dB，持续 8 s，随后保持功率不变，第 12 s 无人机飞行至 C 点(40.176 653° N，

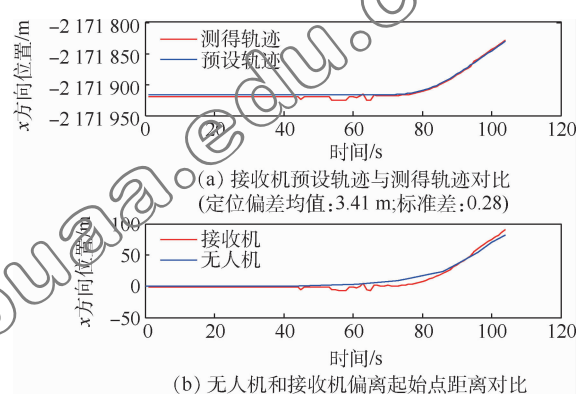


图 9　轨迹和偏离起始点的距离

Fig. 9　Trajectory and distance deviated from origin



图 10　无人机外场实验设备及环境

Fig. 10　UAV field experimental equipment and environment

http://bhxb.buaa.edu.cn

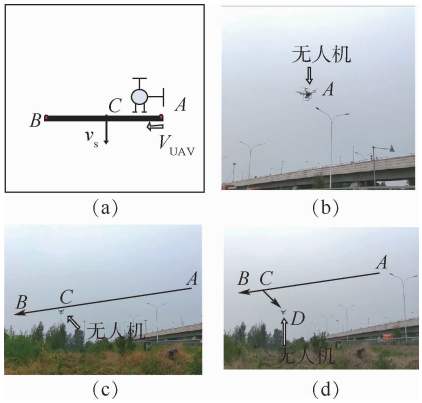


图 11 无人机动态诱骗实验场景

Fig. 11 Dynamic experimental scenario of UAV spoofing

116.269 930°E),如图 11(c)所示;随即逐步增大干扰源所仿真目标在东北天坐标系下的东向速度 V_e,初始速度为 0,加速度为 0.2 m/s^2,持续时间为 5 s,北向和天向速度为 0;可观测到无人机飞向 D 点(40.176 707°N,116.269 967°E),偏离预设飞行路径,如图 11(d)所示,说明欺骗信号获得了跟踪环路主导权,无人机诱骗成功。因为无法从 DJI Assistant 2 软件导出无人机定位信息,所以无法对无人机飞行轨迹进行进一步的数据分析。

值得注意的是,无人机导航飞控系统融合了卫星导航、惯性导航、视觉导航、气压计等多源传感器信息,无人机卫星导航接收机受到干扰源欺骗信号影响后,无人机仍然可以获取其余传感器信息,因此若要进一步控制无人机飞行轨迹,还需结合无人机导航飞控系统控制策略,这将是下一步研究工作的难点所在。

3 结 论

1)设计实现了一种小型化的同步生成式 GPS 欺骗干扰源,建立了同步式 GPS 欺骗干扰信号模型,给出了信号仿真参数的计算方法,采用时基同步的方法补偿了干扰源的处理时延,通过商用接收机验证了 GPS 欺骗干扰信号模型及同步设计的正确性。

2)给出了干扰信号俘获目标接收机跟踪环路过程中欺骗信号参数的调整方法,并通过商用接收机和无人机进行了静态和动态实验验证,结果表明该方法能够使干扰源在不需要压制干扰阻断目标接收机跟踪环路的情况下成功俘获跟踪环路的主导权,最终使目标接收机输出预设的定位测速结果,验证了该方法的可行性。

为了提高诱骗成功率,并能够诱骗无人机在防护区范围内飞往预设的诱骗位置,需要在本文工作基础上针对初始载波相位误差而优化诱骗策略,并进一步分析无人机导航飞控系统,结合其飞控策略和测控链路设定合理的诱骗策略,并通过动态飞行实验验证其效果。

参考文献(References)

[1] LOH R, BIAN Y, ROE T. UAVs in civil airspace: Safety requirements[C]// IEEE Aerospace and Electronic Systems. Piscataway, NJ: IEEE Press, 2009: 5-17.

[2] 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.

[3] AKOS D M. Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC)[J]. Journal of the Institute of Navigation, 2012, 59(4): 281-290.

[4] 高志刚,孟繁智. GPS 转发式欺骗干扰原理与仿真研究[J]. 遥控遥测,2011,32(6):44-47.
GAO Z G, MENG F Z. Principle and simulation research of GPS repeater deception jammng[J]. Journal of Telemetry, Tracking and Command, 2011, 32(6): 44-47(in Chinese).

[5] 庞晶,倪少杰,聂俊伟,等. GNSS 欺骗干扰技术研究[J]. 火力与指挥控制,2016,41(7):1-4.
PANG J, NI S J, NIE J W, et al. An overview to GNSS spoofing technologies[J]. Fire Control & Command Control, 2016, 41(7): 1-4(in Chinese).

[6] CAVALERI A, MOTELLA B, PINI M, et al. Detection of spoofed GPS signals at code and carrier tracking level[C]// Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC). Piscataway, NJ: IEEE Press, 2011: 1-6.

[7] JOVANOVIC A, BOTTERON C, FARINE P A. Multi-test detection and protection algorithm against spoofing attacks on GNSS receivers[J]. Position, Location & Navigation Symposium-plans, 2014, 7(4): 1258-1271.

[8] HUMPHREYS T E, LEDVINA B M, PSIAKI M L, et al. Assessing the spoofing threat: Development of a portable GPS civilian spoofer[C]// 21st International Technical Meeting of the Satellite Division of the Institute of Navigation. Manassas, VA: The Institute of Navigation, 2008: 2314-2325.

[9] 黄龙,吕志成,王飞雪. 针对卫星导航接收机的欺骗干扰研究[J]. 宇航学报,2012,33(7):884-890.
HUANG L, LV Z C, WANG F X. Spoofing pattern research on GNSS receivers[J]. Journal of Astronautics, 2012, 33(7): 884-890(in Chinese).

[10] 陈碧,郭承军. GPS 欺骗干扰过程研究[J]. 科技通报,2016,32(10):164-169.
CHEN B, GUO C J. Study on GPS spoofing pattern process[J]. Bulletin of Science and Technology, 2016, 32(10): 164-169(in Chinese).

[11] 马克,孙迅,聂裕平. GPS 生成式欺骗干扰关键技术[J]. 航天电子对抗,2014,30(6):24-26.
MA K, SUN X, NIE Y P. Research on key technologies of GPS generated spoofing[J]. Aerospace Electronic Warfare, 2014, 30

http://bhxb.buaa.edu.cn

(6):24-26(in Chinese).

[12] 何亮,李炜,郭承军. 生成式欺骗干扰研究[J]. 计算机应用研究,2016,33(8):2405-2408.
HE L,LI W,GUO C J. Study on GPS generated spoofing attacks [J]. Application Research of Computers,2016,33(8):2405-2408(in Chinese).

[13] 寇艳红. GNSS 软件接收机与信号模拟器系统研究[D]. 北京:北京航空航天大学,2006:55.
KOU Y H. Research on GNSS software receiver and signal simulator[D]. Beijing:Beihang University,2006:55(in Chinese).

[14] 李铭涵. 生成式 GPS 欺骗无人机干扰源设计与实现[D]. 北京:北京航空航天大学,2018:14.
LI M H. Research and implementation of a GPS signal generator spoofing UAVs[D]. Beijing:Beihang University,2018:14(in Chinese).

[15] 谢刚. GPS 原理与接收机设计[M]. 北京:电子工业出版社,2009:79.
XIE G. Principles of GPS and receiver design[M]. Beijing: Publishing House of Electronics Industry,2009:79(in Chinese).

[16] 樊鼎. GPS 同步生成式欺骗干扰及检测方法研究[D]. 北京. 北京航空航天大学,2018:9-12.
FAN D. Design of GNSS multiplexing signal quality monitoring receiver[D]. Beijing:Beihang University,2018:9-12(in Chinese).

[17] ZHOU M,LIU Y,XIE L,et al. Performance analysis of spoofing signal ratio for receiver-spoofer[C]// Proceedings of the 2017 International Technical Meeting of the Institute of Navigation. Washington,D. C.:INST Navigation,2017:898-911.

[18] 潘虹田. GNSS 信号质量监测接收机设计[D]. 北京. 北京航空航天大学,2016:8.
PAN H C. Design of GNSS signal quality monitoring receiver [D]. Beijing:Beihang University,2016:8(in Chinese).

作者简介:

柳亚川　男,硕士研究生。主要研究方向:卫星导航。

寇艳红　女,博士,副教授,硕士生导师。主要研究方向:卫星导航、无线通信、数字信号处理。

Research and design of synchronous GPS spoofing signal generation technology

LIU Yachuan, KOU Yanhong*

(School of Electronic and Information Engineering, Beihang University, Beijing 100083, China)

Abstract: In order to meet the actual requirements of navigation spoofing of "low, slow, small" UAV, a miniaturized synchronous GPS spoofer has been developed based on our asynchronous GPS generator spoofer. Firstly, based on asynchronous GPS generator spoofer RF signal model, considering the spoofer signal processing delay, the spoofing signal propagation delay, the status of the authentic satellite signal received by the UAV receiver, and the dynamic model of the UAV, established the mathematical model to accurately calculate the simulation time and state parameters of the synchronous spoofing signal. Secondly, a local timing receiver is employed to provide the disciplined reference clock and 1 pulse per second (1PPS) signal to synchronize the spoofing signal with the authentic system time, and high-order direct digital synthesis(DDS) technology is applied to accurately control the signal parameters and ensure that the difference between the spoofing signal and the authentic signal is within the tolerances allowed for successful spoofing when the spoofing signal reaches the phase center of the receiving antenna of the target receiver. Finally, the test results using a popular commercial UAV and a commercial receiver are presented. When the UAV receiver tracks the authentic satellite signal, the synchronous GPS spoofer begins to transmit the spoofing signal, which gradually deviates the target receiver from its normal measurements and makes it output the position and velocity results under control. The results verify the established synchronous signal model, the designed synchronous signal generation circuit, and indicate the synchronous GPS spoofer can achieve navigation spoofing of commercial UAV and commercial receiver.

Keywords: GPS spoofer; synchronous generator; time base synchronization; synchronous signal model; unmanned aerial vehicle (UAV) spoofing

Received: 2019-06-17; **Accepted**: 2019-11-17; **Published online**: 2019-11-25 14:03

URL: kns.cnki.net/kcms/detail/11.2625.V.20191125.1339.002.html

* **Corresponding author**. E-mail: kouy@buaa.edu.cn

http://bhxb.buaa.edu.cn