doi:10.11887/j.cn.202102006 http://journal.nudt.edu.cn

无人机位置欺骗诱导策略*

史鹏亮[1],王晓宇[2],薛 瑞[1]
(1. 北京航空航天大学 电子与信息工程学院,北京 100191;2. 中国电子科技集团公司第二十研究所,陕西 西安 710068)

摘 要:针对"黑飞"无人机的有效管控及处置问题,提出基于卫星导航定位位置欺骗的无人机诱导策略。结合目标无人机的精确位置信息,利用生成式导航欺骗干扰技术向目标发射虚假的卫星导航定位信号,使目标无人机飞行控制系统得到错误的位置信息,改变飞行姿态,进而偏离预设运动轨迹。通过无人机诱导试验验证了所提策略的正确性和有效性。

关键词:导航欺骗干扰;位置欺骗;无人机诱导
中图分类号:TN95 **文献标志码**:A **文章编号**:1001-2486(2021)02-040-07

Induction strategy for unmanned aerial vehicle position spoofing

SHI Pengliang[1], *WANG Xiaoyu*[2], *XUE Rui*[1]
(1. School of Electronics and Information Engineering, Beihang University, Beijing 100191, China;
2. The 20th Research Institute of China Electronics Technology Group Corporation, Xi'an 710068, China)

Abstract: An induction strategy based on position spoofing for UAV (unmanned aerial vehicle) was presented to solve the problem of effective control and disposal of unauthorized UAV. The target UAV navigation and control systems got the fictitious position information caused by the spoofing signals that were produced by combination of accurate position information of the target and the induction strategy. The target UAV changed its flying attitudes and deviation from the pre-specification air route. Experimental results demonstrate the validity and effectiveness of the proposed induction strategy.

Keywords: navigation deception jamming; position spoofing; unmanned aerial vehicle induction

近年来,无人机技术快速发展,广泛应用于应急救援、军事作战、遥感测绘、农业植保等诸多领域,在国防建设和经济发展中具有巨大的应用价值[1]。由于无人机体积较小、价格低廉、操控简单,如果被不法分子利用将会给社会稳定及安全保卫工作带来极大的挑战。全球已经发生多起无人机非法进入敏感空域的事件。因此,如何采取有效的措施反制无人机已成为国内外的研究热点问题和难点问题。

国内外反制无人机的技术手段主要可以分为物理击落、生物抓捕和电磁干扰三大类[2]。物理击落技术主要采用网枪、火炮或者高能激光烧毁等手段对无人机进行处置,造价较高,且坠落的无人机如果携带危险物品,可能会产生更严重的次生危害。生物抓捕即训练老鹰等飞禽将无人机作为猎物抓捕并带回鸟巢,但训练成本高昂且缺乏稳定性。电磁干扰手段主要通过切断或压制无人机控制、定位及图传信号,迫使无人机返航、悬停或原地降落[3-4],在技术上较为容易实现,成本也相对较低。无人机处于飞行状态时,经常使用卫星导航信号测量值来修正自身位置[5-7],因此可以通过发送欺骗卫导信号的方法,使目标无人机获得错误位置及速度,导航系统输出错误的状态量,从而完成对状态估计量的控制。文献[8]针对欺骗干扰对无人机导航系统的诱导可行性进行了分析及试验验证。结果表明:虽然无人机本身具有一定的欺骗防护能力,但当欺骗实施方知晓无人机的运动状态时可以实现对无人机的诱导。文献[9]设计了一种借助软件接收机和真实信号以产生欺骗干扰信号的方法,该方法实用性强,无须昂贵的硬件设备,降低了欺骗干扰实施的复杂度和成本。但随着技术的发展,无人机抗干扰能力也在逐步增强[10-14],更多的时候,普通干扰最多能使无人机作业失败,但对于被干扰后无人机下一步将采取何等动作则较难判断,难以达到防范目的。

* 收稿日期:2020-01-11
基金项目:国家重点研究发展计划资助项目(2017YFB0503401)
作者简介:史鹏亮(1979—),男,湖南永兴人,高级工程师,博士研究生,E-mail:pl_s@sohu.com

本文设计了一种通过生成全球导航卫星系统（Global Navigation Satellite System，GNSS）欺骗信号的无人机诱导系统，提出基于卫星导航位置欺骗的无人机诱导策略，该策略针对传统诱骗方法信号精度低，虚假欺骗信号隐蔽性差等问题，在生成虚假欺骗信号时，同时考虑无人机的位置坐标、飞行速度、状态等信息融合计算高精度诱骗信号，减小了 1 码片精度所带来的较大误差。此外，所提方法采用小幅度逐步拉偏策略，实现诱骗信号的无缝切入，提升诱骗信号的隐蔽性。

1　基于生成式欺骗的无人机诱导系统

1.1　生成式欺骗原理

生成式 GNSS 欺骗技术通过产生虚假卫星导航信号，达到欺骗卫星导航接收机的目的，分为直接生成式和准生成式两种方法[4, 10]。

直接生成式利用基站、网络等手段获取卫星系统星历，根据仿真时刻生成欺骗坐标点上方的可见卫星信号，达到欺骗卫导接收机的目的。直接生成式可以生成任意坐标地点的虚假信号，但利用基站、网络更新的星历往往具有滞后性，实时性较差。

准生成式利用卫星导航接收机实时接收可见卫星星历、时间等参数，产生相应卫星的伪随机码，并调制接收到的导航电文。采用逐步拉偏的诱导策略，计算期望的虚假位置坐标及速度[15]，根据本地接收的卫星信号星历计算不同卫星信号的发送时刻，并朝无人机定向播发欺骗信号，达到欺骗卫导接收机的目的。

1.2　无人机诱导系统

采用准生成式欺骗方式产生的卫星信号与天上真实的卫星信号具有相同的星历。这种欺骗信号避免了星历参数的跳变，因此在对无人机欺骗干扰时具有巨大的优势。基于准生成式 GNSS 欺骗方法对无人机实施诱导，实质是切入机载卫星导航接收机的跟踪环路，使其跟踪到发射的虚假卫星信号上，进而导致错误的测量或定位结果。

所提无人机诱导系统采用基于准生成式 GNSS 欺骗方法，可自主生成与真实信号极度相似的欺骗信号，结合探测设备传送的目标位置信息[16-17]，自动生成干扰策略，对目标实施定向诱导，其原理如图 1 所示。

系统工作原理如下：雷达或光电探测设备提供目标无人机的位置速度信息。即时信号接收单元实时接收真实卫星信号，完成卫星信号的捕获、跟踪、解算、定位与导航信息存储输出，并传送给数学仿真模块。数学仿真模块基于星历信息和目标无人机位置，实时计算生成欺骗干扰信号的控制参数。信号生成模块根据数学仿真模块产生的控制参数生成包括干扰卫星的观测数据和导航电文信息的欺骗信号。功率控制模块依据干扰控制软件设定参数对干扰发射信号进行功率控制，以满足诱导信号功率要求。最后通过发射天线将欺骗信号播发给目标无人机，造成其定位错误，达到诱导目的。

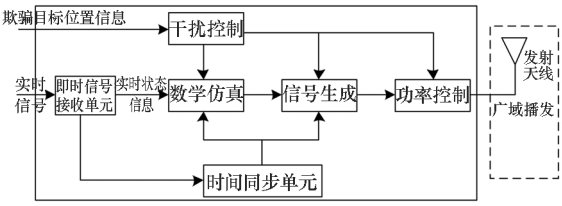


图 1　生成式欺骗干扰设备原理

Fig. 1　Principle of generative spoofing device

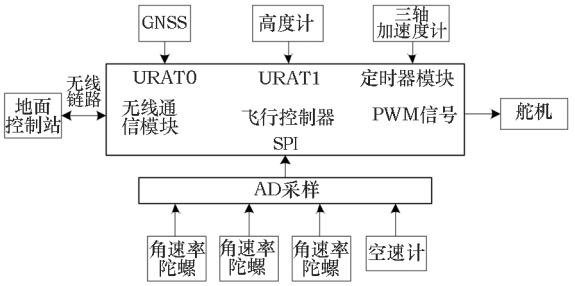
无人机诱导系统产生的诱导信号要实现无人机机载接收机跟踪环路的隐蔽式切入，需要保证诱导信号与真实卫星信号的精密同步，包括时间基准的同步、星历的同步和信号生成的同步。所提无人机诱导系统内置卫导接收机和恒温晶振，利用接收机对晶振进行驯服，保证生成的时频基准信号（10 MHz 和 1 PPS）与真实卫星系统的时间同步，同时利用内置接收机获取卫星的星历、钟差、电离层等信息，实现卫星信号导航信息的同步。在发射诱导信号的过程中，采用延迟滤波器时延控制方法[18-19]，计算各个卫星信号的时延量，精确调整后发射给无人机。

2　无人机诱导策略

基于生成式 GNSS 欺骗的无人机诱导系统的关键是生成能够诱导无人机飞至指定位置的 GNSS 导航信号。为此，本节在分析无人机飞控原理的基础上，提出基于位置欺骗的诱导策略。

2.1　无人机飞控原理

一般无人机飞控系统主要由飞控与管理计算机、系统传感器、伺服舵机三大部分组成。其中：系统传感器包括陀螺、加速度计、空速计、高度计和 GNSS 传感器等；飞控与管理计算机和伺服舵机共同实现航向、俯仰角、倾斜角、飞行高度的稳定与控制及侧向偏离控制和自动协调转弯控制。无人机飞控原理如图 2 所示[2]。



URAT：通用异步控制器　PWM：脉冲宽度调制
SPI：串行外设接口

图 2　无人机飞控原理

Fig. 2　Principle of UAV flight control system

无人机飞行过程中，飞控系统不断从 GNSS 接收机[20]等传感器获取飞机实际位置和航向信息，再根据遥控器指令或设定的航线，计算偏航距和航向控制量，使相应舵面偏转、飞机回到设定航线。

影响无人机自身定位的最关键因素就是无人机的机载 GNSS 接收机，如图 3 所示，当无人机悬停于某一点 P_1 上空时，如果此时无人机受风力、动力等因素的影响，位置飘移至 P_1'，机载接收机定位后发现位置变化，便会控制飞控系统使其飞回悬停点。同理，在无人机按自身的导航点 $P_1 \rightarrow P_2 \rightarrow P_3 \rightarrow P_4$ 飞行的过程中，如果机载接收机发现无人机偏离了航向，便会修正航向使无人机飞回到正确的航线上。

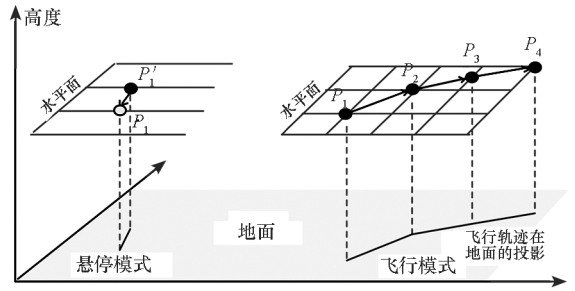


图 3　无人机位置修正示意图

Fig. 3　Schematic diagram of UAV position modification

因此，可以利用无人机的这一特点，产生虚假 GNSS 导航信号并发射给无人机，使其机载接收机定位出错误位置，无人机便会向“正确”位置进行修正，从而达到诱使无人机偏离航向甚至飞向诱骗坐标点的目的。

2.2　基于位置欺骗的诱导策略

以悬停模式为例，如图 4 所示，当无人机在 P_1 位置悬停时，给它一个错误的定位信息 P_1'，飞控系统会控制无人机沿 $P_1' \rightarrow P_1$ 方向移动修正“偏差”，实际上无人机会从 P_1 点沿 $P_1 \rightarrow P_2$ 方向移动至 P_2 点。如果维持 P_1' 定位信息不变，飞控系统会控制无人机一直沿 $P_1 \rightarrow P_2$ 方向飞行。飞行模式与悬停模式类似，当无人机收到错误定位信息 P_1' 时，无人机会修正自身航向，从而偏离航线。

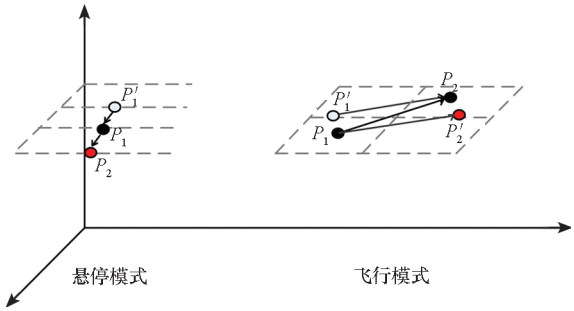


图 4　位置欺骗诱导原理

Fig. 4　Inducement principle of position spoofing

当无人机飞行到 P_1 点时，机载接收机利用式(1)来计算自身的位置坐标(x_1, y_1, z_1)：

$$\rho_i = \sqrt{(x_{si}-x_1)^2+(y_{si}-y_1)^2+(z_{si}-z_1)^2} + ct_u + I + T \tag{1}$$

式中：ρ_i 为接收机观测到第 i 颗卫星的伪距；x_{si}，y_{si}，z_{si}为第 i 颗卫星的位置坐标；t_u 为接收机的钟差；I，T 分别为信号通过电离层和对流层所引起的误差，可通过大气模型求出；c 为光速。欺骗设备通过调整不同虚假卫星信号的发送时刻来改变伪距 ρ_i，从而使机载接收机利用式(1)计算出错误的位置 $P_1'(x_2, y_2, z_2)$。

通常情况下，欺骗设备与无人机距离不会非常远，因此大气层所带来的延迟效应几乎相同，消除公共误差后，可以得到每颗卫星的伪距改变量为：

$$\Delta\rho_i = \sqrt{(x_{si}-x_1)^2+(y_{si}-y_1)^2+(z_{si}-z_1)^2} - \sqrt{(x_{si}-x_2)^2+(y_{si}-y_2)^2+(z_{si}-z_2)^2} \tag{2}$$

卫星信号伪距的修改，在硬件上通过调整信号的发送时刻来实现。因此，当欺骗设备将修改过发送时刻的虚假信号辐射给无人机后，通过功率调整，迫使无人机对真实卫星信号的跟踪环路失锁，锁定到欺骗信号，从而完成对无人机的欺骗。

设 $R = \sqrt{(x_2-x_1)^2+(y_2-y_1)^2+(z_2-z_1)^2}$，为欺骗位置 P_1' 与无人机原位置 P_1 的距离。从式(2)可以看出，R 增大将导致 $\Delta\rho_i$ 相应增大。以 GPS L1 信号来说，一个码片对应的伪距为 300 m 左右，当 $\Delta\rho_i > 300$ m 时，欺骗信号与无人机卫导接收机的相关峰将会与真实信号的相关峰产生两个分离的峰值，如图 5(a)所示。此时，加大欺骗

信号功率并不会使欺骗信号的相关峰的宽度 τ_n 变宽,因此很难对真实信号的相关峰产生影响,接收机会保持对真实卫星的跟踪。为了使接收机跟踪到欺骗信号,可以先对无人机发射大功率干扰迫使其信号失锁,再撤去干扰加入欺骗信号,由于欺骗信号的功率远大于真实卫星信号,无人机的卫导接收机在信号重补的过程中会首先对欺骗信号进行捕获跟踪,从而实现对无人机的诱导。但是这种情况容易在接收机端产生巨大的位置跳变,使得接收机很容易对欺骗信号加以剔除。

一般情况下,接收机的码跟踪环路需要计算超前滞后相关峰来完成对码频率的跟踪。考虑有欺骗信号存在的情况下,超前滞后相关器的相关函数如式(3)~(4)所示[21]。

$$R_E(\varepsilon)=\alpha_1 R\left(\varepsilon+\frac{d}{2}\right)+\alpha_2 R\left(\varepsilon-\Delta\tau+\frac{d}{2}\right)\cos(\Delta\varphi) \tag{3}$$

$$R_L(\varepsilon)=\alpha_1 R\left(\varepsilon-\frac{d}{2}\right)+\alpha_2 R\left(\varepsilon-\Delta\tau-\frac{d}{2}\right)\cos(\Delta\varphi) \tag{4}$$

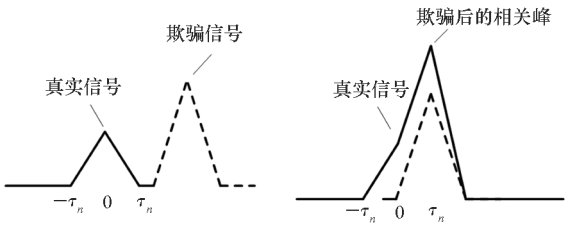
其中:d 为超前、滞后相关器的本地扩频码生成间隔;$\Delta\tau$ 为欺骗信号与真实信号的时延差;$\Delta\varphi$ 为欺骗信号的频率误差;α_1,α_2 分别为真实卫星信号与欺骗信号的信号幅值。

当接收机采用 $E-L$ 鉴别函数作为码鉴别函数时,假设模拟源产生的欺骗信号频率相位与真实卫星相同,即 $\Delta\varphi=0$,那么鉴相函数对真实卫星信号时延的估计误差为:

$$\varepsilon=\begin{cases}\dfrac{\alpha\Delta\tau}{1+\alpha} & 0<\Delta\tau\leqslant(1+\alpha)\dfrac{d}{2}\\ \dfrac{\alpha d}{2} & (1+\alpha)\dfrac{d}{2}<\Delta\tau\leqslant\dfrac{\alpha d}{2}+T_c-\dfrac{d}{2}\\ \dfrac{\alpha}{2-\alpha}\left(\dfrac{d}{2}+T_c-\Delta\tau\right) & \dfrac{\alpha d}{2}+T_c-\dfrac{d}{2}<\Delta\tau\leqslant T_c+\dfrac{d}{2}\\ 0 & T_c+\dfrac{d}{2}<\Delta\tau\end{cases} \tag{5}$$

其中:T_c 为 1 码片的长度;$\alpha=\alpha_2/\alpha_1$。可以看出:当欺骗信号与真实信号的伪距差大于 1.5 码片时,欺骗信号无法对真实卫星的跟踪环路造成任何影响;同时,当伪距差大于 1 码片时,鉴别误差较小,并且不会随着 α 的增加而变大。

所以,为了破坏无人机对真实卫星的跟踪,欺骗位置的距离 R 应满足伪距变化量小于 1 码片的要求,如图 5(b)所示。欺骗信号的加入会导致真实信号的相关峰淹没在欺骗信号中,达到诱使无人机跟踪欺骗信号的目的。



(a) 未加入干扰的信号　(b) 加入干扰的信号
(a) Signals without interference　(b) Signals with interference

图 5　逐步拉偏示意图
Fig. 5　Schematic diagram of gradual spoofing

3　试验方案设计与试验验证

3.1　无人机诱导试验方案

无人机诱导试验方案如图 6 所示,试验设备主要包括探测跟踪设备、欺骗干扰设备以及显控设备。其中探测跟踪设备可以是雷达或光电探测设备,可对“低慢小”无人机进行有效探测和稳定跟踪。干扰设备为生成式导航欺骗设备,在探测设备引导下,向目标发射诱导信号。

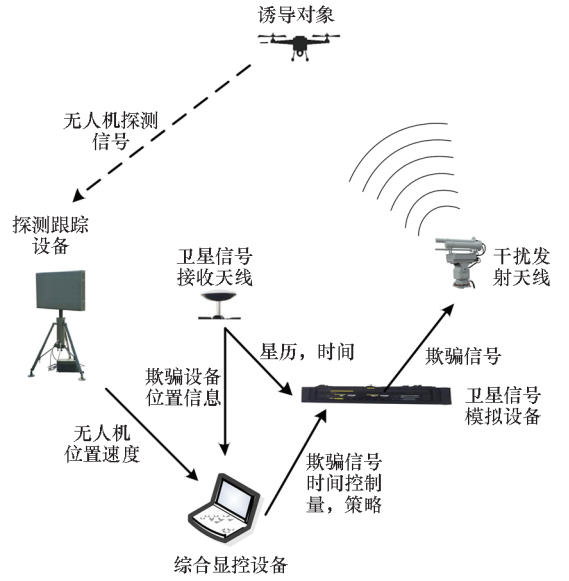


图 6　无人机诱导试验方案示意图
Fig. 6　Scheme of UAV induction experiments

系统工作流程如图 7 所示。

步骤 1:设备启动,完成初始化,确认状态符合诱导要求。

步骤 2:根据探测设备上报的无人机位置制定诱骗策略,产生对应的诱导信号,并通过天线辐射给目标无人机。

步骤 3:观察无人机是否受到干扰,实时修正控制参数,若无效则返回步骤 2。

步骤 4:无人机到达指定区域,停止发射干扰

信号,或发射迫降信号,使目标降落。

步骤 5:结束诱骗。

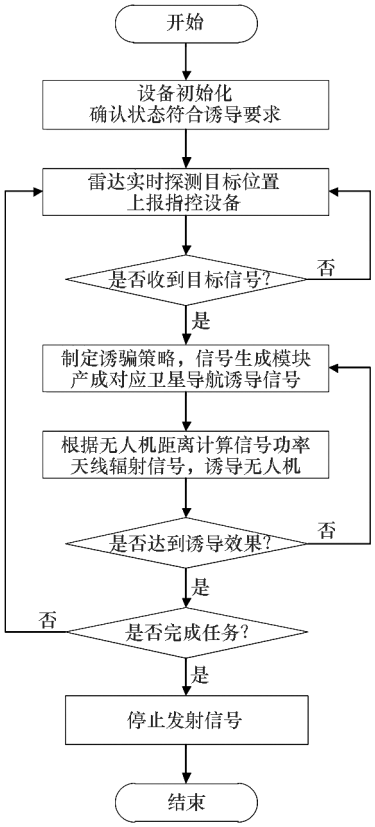


图 7　无人机诱导试验流程

Fig. 7　Flow of UAV induction experiments

3.2　试验验证

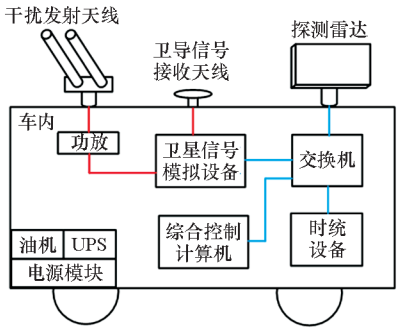
根据上述诱导策略和试验方案开展诱导无人机试验验证。设备采用车载架设方式,如图 8 所示。

使用探测设备实时获取目标无人机的位置信息,并给出每秒位置速度信息,诱导对象为四旋翼无人机。试验环境见表 1。

无人机使用民码 GPS 信号进行导航,控制人员操作无人机以 10 m/s 速度从 2 km 外向防御区飞来。设置的诱导点位置坐标为(105.750 975° E, 38.891 892° N, 1 678 m)。

(a) 无人机诱导设备外观

(a) Appearance of UAV spoofing equipment



(b) 无人机诱导设备内部组成

(b) Internal composition of UAV spoofing equipment

图 8　无人机诱导设备

Fig. 8　UAV spoofing equipment

表 1　诱导设备架设点

Tab. 1　Installation location of spoofing equipment

试验时间	2019 年 7 月 4 日
试验地点	阿拉善巴彦浩特附近某实验场
干扰目标	大疆 精灵 4pro
防御中心点	105.755 938° E, 38.885 027° N

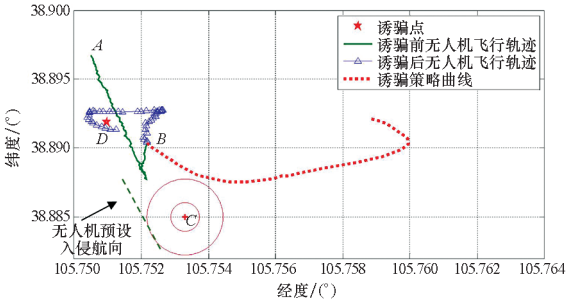
共进行了两次试验,结果分别如图 9(a)和图 9(b)所示。图 9(a)图中:雷达探测到无人机由点 A 向点 B 飞行;图中五角星所在的点 D 为设置的期望将无人机诱导至指定位置的坐标点;图中绿色虚线为无人机预设的入侵航向,可以看出,如果不对无人机进行诱导,无人机将飞入防御区域;因此,当无人机抵近防御点范围圈 500 m 时开启诱导设备,图中组成红色点线的点为无人机接收诱导信号后,机载接收机的定位坐标;$B-D$ 曲线为无人机接收到虚假卫星导航信号后的飞行轨迹曲线。从图 9(a)中可以看出,无人机导航设备被欺骗,无人机飞向诱导坐标点 D。

图 9(b)和图 9(c)分别给出了第二次诱导过程中,无人机的飞行经纬度坐标,无人机与防御点的距离以及与诱骗点的距离。从图 9(b)中可以看出,无人机在 $A-B$ 段的飞行过程中,欺骗设备未开机,雷达探测到无人机此时正在向防御圈 C 进行突防,无人机与防御范围的距离如图 9(c)图所示,可以看出,无人机在突防过程中,由 1 400 m 逐渐接近至 200 m。

当无人机接近到只有 200 m 时,雷达进行入侵告警,综合指控设备进行威胁判断后,设置诱骗点 D,并且开机辐射欺骗信号。无人机收到欺骗信号后,机载接收机定位到虚假坐标处。欺骗设备不断根据雷达探测到无人机坐标信息逐步缓慢

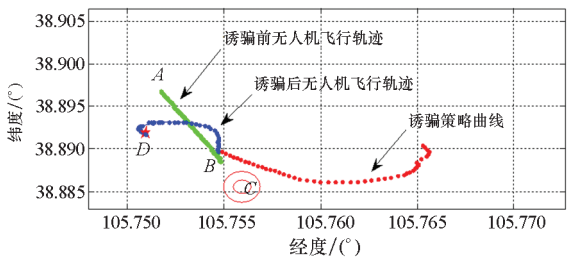
调整欺骗信号，最终形成如图 9(b)中红色曲线所示的欺骗策略曲线。此时的红色曲线即为机载接收机的定位结果，无人机根据机载接收机不断调整自身位置，最终被欺骗后偏离航线，实际飞行轨迹如蓝色曲线所示。

图 9(d)给出了整个过程中无人机与诱骗点的水平距离，从图中可以看出，开启诱导后，通过逐步拉偏，无人机与诱骗点的距离逐渐减小至 10 m左右，达到很好的诱导效果。



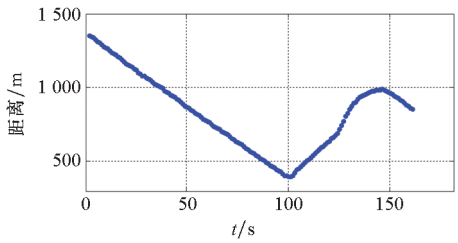
(a) 无人机诱导实验 1

(a) Results of UAV spoofing experiment 1



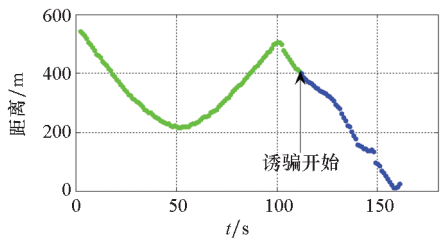
(b) 无人机诱导实验 2

(b) Results of UAV spoofing experiment 2



(c) 无人机与防御点实时距离

(c) Distance between UAV and defense point



(d)无人机与诱骗点实时距离

(d) Distance between UAV and induced

图 9　无人机诱导试验结果

Fig. 9　Results of UAV spoofing experiment

4　结论

本文提出的无人机诱导策略，根据无人机飞控特点，基于无人机的位置生成 GPS 虚假卫星导航信号，通过虚假位置坐标的实时逐步修改，能够有效地将利用民用导航信号的无人机诱导至设定的区域附近，达到较高的诱导精度。后续将进一步研究针对多种导航体制和飞行模式的诱导试验，以及同其他反制手段的配合方法，研究作用距离更远、覆盖范围更广、管制效果更为突出的综合性的反无人机系统。

参考文献(References)

[1] 高萍，王古常，郑幸，等. 无人机空域飞行的现状及发展趋势[C]. 第五届中国无人机大会论文集，2014：627－630.
GAO Ping, WANG Guchang, ZHENG Xing, et al. The current situation and development trend of UAV airspace flight[C]// Proceedings of the Fifth China UAV Conference, 2014: 627－630. (in Chinese)

[2] 施林，刘伟. 基于卫星导航欺骗干扰的无人机管制技术[J]. 指挥信息系统与技术，2017，8(1)：22－26.
SHI Lin, LIU Wei. UAV management and control technology based on satellite navigation spoofing jamming[J]. Command Information System and Technology, 2017, 8(1): 22－26. (in Chinese)

[3] 李豹，许江宁，朱银兵，等. 卫星导航欺骗干扰技术研究进展[J]. 海洋测绘，2018，38(5)：69－72.
LI Bao, XU Jiangning, ZHU Yinbing, et al. Review of technologies for satellite navigation spoofing [J]. Hydrographic Surveying and Charting, 2018, 38(5): 69－72. (in Chinese)

[4] ZILLIAC G G, DEGANI D, TOBAK M. Asymmetric vortices on a slender body of revolution[J]. AIAA Journal, 1991, 29(5): 667－675.

[5] 杨柳庆，肖前贵，牛妍，等. 基于渐消卡尔曼滤波器的定位系统设计[J]. 南京航空航天大学学报，2012，44(1)：134－138.
YANG Liuqing, XIAO Qiangui, NIU Yan, et al. Design of localization system based on reducing Kalman filter [J]. Journal of Nanjing University of Aeronautics & Astronautics, 2012, 44(1): 134－138. (in Chinese)

[6] WENDEL J, MEISTER O, SCHLAILE C, et al. An integrated GPS/MEMS-IMU navigation system for an autonomous helicopter[J]. Aerospace Science & Technology, 2016, 10(6): 527－533.

[7] 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.

[8] SEO S H, LEE B H, IM S H. Effect of spoofing on unmanned aerial vehicle using counterfeited GPS signal[J]. Journal of Positioning Navigation and Timing, 2015, 4(2): 57－65.

[9] BAZIAR A R, MOAZEDI M, MOSAVI M R. Analysis of single frequency GPS receiver under delay and combining

spoofing algorithm[J]. Wireless Personal Communications, 2015, 83: 1955 – 1970.

[10] YANG Y, ZHENG B R, YANG W, et al. Numerical computation of pressure distributions over conical forebody at high angles of attack [C]// Proceedings of 50th AIAA Aerospace Sciences Meeting Including the New Horizons Forum and Aerospace Exposition, 2012.

[11] 刘延斌, 苏五星, 闫抒升. 转发式欺骗信号干扰 GPS 接收机的效能分析[J]. 空军雷达学院学报, 2004, 18(4): 4 – 6.
LIU Yanbin, SU Wuxing, YAN Shusheng. Efficiency analysis of repeater deception jamming GPS repeater[J]. Journal of Air Force Radar Academy, 2004, 18(4): 4 – 6. (in Chinese)

[12] 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): 1884 – 1890.
HUANG Long, LYU Zhicheng, WANG Feixue. Spoofing pattern research on GNSS receivers [J]. Journal of Astronautics, 2012, 33(7): 1884 – 1890. (in Chinese)

[13] 王伟, 陶业荣, 王国玉, 等. GPS 欺骗干扰原理研究与建模仿真[J]. 火力与指挥控制, 2009, 34(6): 115 – 118.
WANG Wei, TAO Yerong, WANG Guoyu, et al. Study and simulation of GPS deception jamming[J]. Fire Control and Command Control, 2009, 34(6): 115 – 118. (in Chinese)

[14] 王上月, 高敬鹏, 王悦, 等. 基于时延控制的 GPS 转发欺骗干扰技术[J]. 导弹与航天运载技术, 2017, 352(2): 103 – 106.
WANG Shangyue, GAO Jingpeng, WANG Yue, et al. GPS repeater deception jamming technology based on delay control[J]. Missiles and Space Vehicles, 2017, 352(2): 103 – 106. (in Chinese)

[15] 张会锁, 高关根, 寇磊, 等. 利用轨迹诱导的欺骗式 GPS 干扰技术研究[J]. 弹箭与制导学报, 2013, 33(3): 149 – 152.
ZHANG Huisuo, GAO Guangen, KOU Lei, et al. Deceptive jamming technology of GPS based on the track induction method[J]. Journal of Projectiles, Rockets, Missiles and Guidance, 2013, 33(3): 149 – 152. (in Chinese)

[16] FERRANTE J. A Kalman filter-based radar track data fusion algorithm applied to a select ICBM case[C]// Proceedings of IEEE Radar Conference, 2004: 457 – 462.

[17] SHEPARD D, BHATTI J, HUMPHREYS T, et al. Evaluation of smart grid and civilian UAV vulnerability to GPS spoofing attacks [C]// Proceedings of 25th International Technical Meeting of the Satellite Division of the Institute of Navigation, 2012: 3591 – 3605.

[18] LORENZ R G, HELKEY R J, ABADI K K. Global positioning system receiver digital processing technique: US5134407[P]. 1992 – 07 – 28.

[19] JWO D J, CHUNG F C, YU K L. GPS/INS integration accuracy enhancement using the interacting multiple model nonlinear filters [J]. Journal of Applied Research and Technology, 2013, 11(4): 496 – 509.

[20] TSUI J B Y. Fundamentals of global positioning receivers: a software approach[M]. USA: John Wiley & Sons, 2005.

[21] 谢刚. GPS 原理与接收设计[M]. 北京: 电子工业出版社, 2009.
XIE Gang. GPS principle and receiving design[M]. Beijing: Publishing House of Electronics Industry, 2009. (in Chinese)