



无人机隐蔽导航欺骗攻击设计

张康康^{1*}, 姜斌¹, 周琪², 王彪¹, 张根瀚¹, 黄杰²

1. 南京航空航天大学, 南京 210016

2. 中国航空工业集团公司西安飞行自动控制研究所, 西安 710076

* E-mail: zhang.kangkang@nuaa.edu.cn

收稿日期: 2025-11-20; 接受日期: 2026-02-06; 网络版发表日期: 2026-03-13

直升机动力学全国重点实验室专项基金项目(编号: ZAG25006-05)和中央基本科研业务费项目(编号: NS2025009)资助

摘要 本文基于无人机动力学系统右半平面极点诱导出Kalman滤波器非最小相位零点的原理以及非最小相位零点对发散信号的阻止作用, 研究针对无人机的导航欺骗攻击的隐蔽性问题. 考虑无人机不稳定的纵向运动及其常见的基于Kalman滤波器的 χ^2 异常检测器, 本文基于纵向动力学系统的右半平面极点导致的Kalman滤波器非最小相位零点设计攻击注入方向和攻击信号时变特性, 并严格证明了该攻击是隐蔽的且会导致无人机纵向运动严重偏离预设轨迹. 揭示了右半平面极点在Kalman滤波器结构中诱导非最小相位零点的内在机理, 并据此系统性构造了在 χ^2 检测框架下统计意义上完全隐蔽、但对纵向飞行状态具有显著破坏性的导航欺骗攻击. 最后, 基于一款Aerosonde无人机的仿真结果验证了所设计的导航欺骗攻击的隐蔽性.

关键词 导航欺骗攻击, 攻击隐蔽性, 无人机

1 引言

无人机作为低空经济载体, 在多种应用场景如低空快递、森林防火以及道路电力系统巡查中得到广泛应用. 其安全性成为制约无人机大量拓展应用的关键因素^[1]. 无人机高度依赖通信链路, 与导航系统通信是利用全球导航卫星系统, 实现定位目的. 然而, 该通信网络信息编码格式公开, 恶意的导航欺骗攻击成为影响无人机安全的重要因素^[2-4]. 欺骗攻击的隐蔽性为无人机对抗恶意攻击带来巨大挑战. 在低空经济运行环境中, 由于飞行高度低、任务密集、容错空间有限, 一旦无人机在导航欺骗攻击作用下产生持续性位置或

高度偏移, 极易引发飞行安全事故, 其潜在危害性较传统高空或单机运行场景更为突出. 本文关注针对无人机的导航欺骗攻击, 研究该攻击的隐蔽性原理及隐蔽攻击对无人机产生的影响.

2011年瑞士苏黎世联邦理工大学研究对民用、军用GPS的欺骗攻击, 分析了攻击成功的条件及其在实践中的局限性, 即识别攻击者需要从哪个位置和以何种精度生成欺骗信号以便成功地被接收机捕获. 该实验在实验室中进行, 采用Spirent GSS7700 GPS模拟器模拟真实和虚假GPS信号, 并通过电缆发送给GPS接收机, 以消除传输信号信道的影响^[5]. 2012年加拿大卡尔加里大学舒立克工程学院的定位导航团队分析了卫

引用格式: 张康康, 姜斌, 周琪, 等. 无人机隐蔽导航欺骗攻击设计. 中国科学: 技术科学, 2026, 56: 518–531

Zhang K K, Jiang B, Zhou Q, et al. Stealthy navigation spoofing attack for unmanned aerial vehicles (in Chinese). Sci Sin Tech, 2026, 56: 518–531, doi: 10.1360/SST-2025-0363

星导航欺骗干扰的类型,建立了卫星导航欺骗信号的模型,在卡尔加里大学搭建的欺骗实验环境中进行了目标接收机欺骗信号接收^[6,7]。美国芝加哥伊利诺伊理工学院在2014年提出了一种针对INS/GPS组合的无人机欺骗攻击方法^[8]。仿真结果表明,如果攻击者对用户的轨迹有着绝对的了解,那么在产生较大位置误差的同时,也能够不被监视器检测到。在布拉格召开的“Virtus Bulletin 2015”安全大会上,惠普安全研究的Oleg Oetrovsky展示了允许攻击者欺骗无人飞行器的一些视频资料和场景。该实验只针对飞往预先设定路线的无人机,但是地面站可以与无人机进行实时通信,改变原定的飞行计划。2017年美国弗吉尼亚理工大学联合Microsoft研究所和电子科学技术大学,提出了一种基于道路导航的单次GPS欺骗攻击方法^[9]。该方法首先从OpenStreetMap中提取和解析公共离地数据的道路网络拓扑结构,并基于导航路径输入和相应约束条件搜索可行的欺骗路径;然后利用可编程无线电平台构建便携式GPS欺骗器;最后依据道路网络拓扑结构的物理约束性,选取可欺骗位置点发动一次位置欺骗攻击,使得受害者的实际当前位置欺骗到错误位置点,进而依据原始路径指引受害者到另外一个目标点。2018年美国北达科他大学的Eric Hroton和Prakash Ranganathan^[10]开发了一种GPS欺骗设备,并详细介绍了利用该设备攻击安卓手机以及大疆公司经纬Matrice 100四旋翼无人机所采取的步骤,以及分析了在欺骗干扰下安卓手机和四旋翼无人机导航定位的偏移效果。中国浙江大学工业控制科技国家重点实验室学者在2016年描述了一种利用GPS欺骗攻击将装备有故障检测器的无人机驱动到任意目标地的场景。在该欺骗场景中,攻击者可以通过操作窃听攻击来获得无人机每个时刻的位置、速度和加速度,进而将欺骗攻击问题转化为约束优化问题,即在故障检测器的约束下求解最优的虚假卫星信号使得无人机最终达到点与预计期望的欺骗目标点之间的误差最小^[11]。但是该场景仅考虑了纯卫星导航模式,且其模拟仍处于仿真验证状态。国内在外针对基于GPS欺骗干扰实施GPS/INS组合导航系统的轨迹欺骗上也进行了一些研究,史密等人^[12]在建立松耦合组合导航模型和GPS欺骗模型的基础上,利用多维泰勒分析的方法推导了转发时延与GPS欺骗偏差的解析关系,进而结合卡尔曼滤波分析了GPS欺骗偏差对组合导航定位结果的影响。

研究导航欺骗攻击的隐蔽性是一个新的课题,相关理论和应用成果非常有限。隐蔽性是指攻击能够在不触发无人机onboard异常监测与诊断系统(如基于残差的 χ^2 检测器)的情况下,使关键飞行状态发生偏移的一种特性。Henrik Sandberg^[13]强调传输零点在隐蔽攻击实现中的核心作用,指出非最小相位系统对执行器通道上特定方向和频率的攻击具有阻隔作用。攻击者可以利用系统的传输零点结构,选择特定频率(即系统传递函数的零点对应的频率)注入欺骗攻击信号,使异常检测机构不能检测该攻击,而被攻击系统输出却发生明显偏移。另外,在几何控制的背景下,当攻击信号作用在系统状态的某一子空间中,且该子空间同时属于系统的弱不可观空间与受控不变子空间的交集,攻击信号可被设计为使攻击检测残差长期保持在检测器的容忍阈值以下,从而实现隐蔽^[14,15]。实现隐蔽导航欺骗攻击需要解决的理论问题是如何从输出通道注入攻击信号实现对闭环系统的隐蔽攻击。但是该理论问题还未得到充分的研究。从攻击注入的通道来看,隐蔽导航欺骗攻击的基本原理类似于针对滤波器的隐蔽攻击问题。该攻击从测量输出通道注入到滤波器,被观测系统的稳定性成为决定隐蔽欺骗攻击存在的重要条件,甚至是充要条件^[16,17]。当系统稳定时难以实施既隐蔽又能造成估计误差持续发散的攻击;而对于不稳定系统,攻击者则可构造隐蔽攻击,使系统状态估计发生严重偏离且不被检测器察觉^[16]。因此,系统的不稳定性为隐蔽攻击提供了安全漏洞。在稳定系统中,攻击虽隐蔽,但误差协方差趋于稳态;而在不稳定系统中,攻击不仅隐蔽,更可能导致估计误差发散。由此可见,系统稳定性在很大程度上决定了攻击能否隐蔽且产生显著破坏作用^[17]。

考虑以上的研究现状,本文基于无人机纵向运动固有的不稳定性以及工程中普遍采用的基于Kalman滤波的 χ^2 异常检测框架,利用纵向动力学系统右半平面极点所诱导的Kalman滤波器非最小相位零点,系统性地构造了攻击注入方向与攻击信号的时间演化特性,并严格证明了该攻击在理论上可实现完全隐蔽,同时会驱使无人机纵向状态逐渐偏离参考轨迹。最后,通过Aerosonde固定翼无人机的高保真仿真验证了所设计导航欺骗攻击的隐蔽性与危害性,进一步表明现有监测机制在应对此类结构性安全威胁时存在显著不

足. 因此, 本文从控制系统结构层面揭示隐蔽导航欺骗攻击的可实现机理, 不仅具有理论意义, 也为低空经济场景下无人机导航安全风险评估与防御机制设计提供了重要参考. 与现有隐蔽攻击研究主要侧重于信号注入策略或检测器规避方法不同, 本文从无人机纵向动力学本体特性出发, 揭示了系统不稳定模态在Kalman滤波器检测结构中所诱导的关键非最小相位特征, 并据此刻画了隐蔽导航欺骗攻击得以成立的结构条件. 本文的分析不仅给出了攻击构造方法, 更从系统层面阐明了隐蔽性与破坏性并存的内在机理, 为理解无人机导航系统的结构性安全风险提供了新的理论视角.

2 纵向动力学模型与风扰动模型耦合建模

与将无人机建模为一般线性系统不同, 本文从固定翼无人机纵向动力学本体特性出发, 关注其在工程实践中普遍存在的固有不稳定模态及其对导航安全的影响.

2.1 纵向动力学方程的建立条件

在机体坐标系 $\mathcal{F}^b$ 下, 无人机的六自由度运动方程可表示为

$$m\dot{\mathbf{V}}^b + \boldsymbol{\omega}^b \times (m\mathbf{V}^b) = \mathbf{F}^b, \quad \mathbf{J}\dot{\boldsymbol{\omega}}^b + \boldsymbol{\omega}^b \times (\mathbf{J}\boldsymbol{\omega}^b) = \mathbf{M}^b, \quad (1)$$

其中 $\mathbf{V}^b = [u, v, w]^T$ 为机体速度向量, $\boldsymbol{\omega}^b = [p, q, r]^T$ 为角速度向量, $\mathbf{F}^b$ 与 $\mathbf{M}^b$ 分别表示机体下的合力与力矩. 无人机纵向动力学模型描述飞行器在对称飞行条件下(即无侧滑、无滚转)沿机体对称平面的平移与俯仰运动, 是固定翼无人机六自由度运动方程的一个重要子系统. 该模型主要用于研究如下纵向运动特性, 如: 飞行速度、攻角、俯仰角、俯仰角速度以及高度之间的动态耦合关系和推力、升降舵偏角等控制输入对纵向运动响应的影响. 建立纵向线性模型, 需要以下假设与近似: (1) 对称小扰动飞行假设, 即飞机仅在机体对称平面内运动, 忽略侧滑、滚转与偏航的耦合; (2) 定常配平点线性化, 在给定配平飞行状态附近, 对式(1)进行一阶线性化以及对气动力与力矩由配平点处的气动导数线性近似; (3) 相对气流驱动, 气动力由相对气流(空速矢量)决定, 若存在风扰动, 应以

$\mathbf{V}_a = \mathbf{V}_g - \mathbf{V}_w$ 替代地速; (4) 惯性与质量常数, 飞行器质心位置与转动惯量在短小时内保持不变, 机体刚性结构不考虑弹性变形; (5) 小角度近似, 攻角与俯仰角偏离配平值较小, 便于采用 $\sin\alpha \approx \alpha$, $\cos\alpha \approx 1$ 的线性化处理, 其中 α 表示攻角.

本文考虑飞机稳定在配平飞行点, 飞机在恒速、恒姿态、恒高度条件下的稳态飞行状态. 假设 $v = 0$ 飞行方向始终位于机体对称平面内, 飞机没有侧滑; $p = 0$ 飞机没有滚转运动, 机翼保持水平; $r = 0$ 飞机没有偏航运动, 机头指向航迹方向; $\phi = 0$ 飞机保持零滚转姿态, 不产生侧向倾斜. 另外, 为提高物理可解释性与控制设计便利性, 将状态由 w 改写为攻角 α . 在配平点附近, 有(由 $\alpha = \tan^{-1}(w/u)$ 线性化)

$$\dot{\alpha} = \frac{1}{V_a^* \cos\alpha^*} \dot{w}, \quad w = V_a^* \cos\alpha^* \alpha. \quad (2)$$

在这些假设下, 六自由度的运动方程(1)退化为五个状态量的纵向动力学子系统

$$\mathbf{x}_{\text{lon}} = [u, \alpha, q, \theta, h]^T, \quad (3)$$

其中 u 为机体轴向速度分量, α 为攻角, q 为俯仰角速度, θ 为俯仰角, h 为高度. 控制输入为

$$\mathbf{u}_{\text{lon}} = [\delta_e, \delta_t]^T, \quad (4)$$

其中 δ_e 和 δ_t 分别对应升降舵偏角与油门控制输入. 因此, 可获得以 α 为状态的飞机纵向线性模型:

$$\dot{\mathbf{x}}_{\text{lon}} = \mathbf{A}_{\text{lon}} \mathbf{x}_{\text{lon}} + \mathbf{B}_{\text{lon}} \mathbf{u}_{\text{lon}}, \quad (5)$$

其中

$$\mathbf{A}_{\text{lon}} = \begin{bmatrix} X_u & X_w V_a^* \cos\alpha^* & X_q & -g \cos\theta^* & 0 \\ \frac{Z_u}{V_a^* \cos\alpha^*} & \frac{Z_w}{V_a^* \cos\alpha^*} & \frac{Z_q}{V_a^* \cos\alpha^*} & -\frac{g \sin\theta^*}{V_a^* \cos\alpha^*} & 0 \\ M_u & M_w & M_q & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ \sin\theta^* & -V_a^* \cos\theta^* \cos\alpha^* & 0 & u^* \cos\theta^* + w^* \sin\theta^* & 0 \end{bmatrix}, \quad (6)$$

$$\mathbf{B}_{\text{lon}} = \begin{bmatrix} X_{\delta_e} & X_{\delta_t} \\ \frac{Z_{\delta_e}}{V_a^* \cos\alpha^*} & 0 \\ M_{\delta_e} & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}. \quad (7)$$

表1对式(5)~(7)出现的量逐一说明. 具体表达式见表1, 这些导数量化了气动力和力矩对速度、角速率以及舵面输入的线性灵敏度, 是由非线性气动模型在定常配平点处一阶线性化得到的. 它们构成了纵向状态空间矩阵的主要元素, 用于描述速度、攻角、俯仰角和高度之间的线性动态关系. 需要指出的是, 该纵向动力学模型中出现的右半平面极点并非人为假设, 而是由无人机气动特性、配平状态及纵向耦合效应共同决定的固有不稳定模态, 在实际固定翼无人机中具有普遍性.

表 1 纵向模型系数

Table1 Parameters of longitudinal model

符号	计算公式	物理意义
X_u	$\frac{u^* \rho S}{m} (C_{X_0} + C_{X_\alpha} \alpha^* + C_{X_{\delta_e}} \delta_e^*) - \frac{\rho S w^* C_{X_\alpha}}{2m} + \frac{\rho S c C_{X_q} u^* q^*}{4m V_a^*} - \frac{\rho S_{\text{prop}} C_{\text{prop}} u^*}{m}$	前向气动力对前向速度的敏感度
X_w	$-q^* + \frac{w^* \rho S}{m} (C_{X_0} + C_{X_\alpha} \alpha^* + C_{X_{\delta_e}} \delta_e^*) + \frac{\rho S C_{X_q} w^* q^*}{4m V_a^*} + \frac{\rho S C_{X_\alpha} u^*}{2m} - \frac{\rho S_{\text{prop}} C_{\text{prop}} w^*}{m}$	前向力随垂向速度的变化(迎角耦合)
X_q	$-w^* + \frac{\rho V_a^* S C_{X_q} c}{4m}$	俯仰角速度引起的附加阻力导数
X_{δ_e}	$\frac{\rho V_a^* S C_{X_{\delta_e}}}{2m}$	升降舵对前向力的影响
X_{δ_t}	$\frac{\rho S_{\text{prop}} C_{\text{prop}} k^2 \delta_t^*}{m}$	油门偏差导致的推力变化
Z_u	$q^* + \frac{u^* \rho S}{m} (C_{Z_0} + C_{Z_\alpha} \alpha^* + C_{Z_{\delta_e}} \delta_e^*) + \frac{u^* \rho S C_{Z_q} q^* c}{4m V_a^*} - \frac{\rho S C_{Z_\alpha} w^*}{2m}$	升力方向气动力对前向速度的导数
Z_w	$\frac{w^* \rho S}{m} (C_{Z_0} + C_{Z_\alpha} \alpha^* + C_{Z_{\delta_e}} \delta_e^*) + \frac{\rho w^* S C_{Z_q} q^* c}{4m V_a^*} + \frac{\rho S C_{Z_\alpha} u^*}{2m}$	升力对垂向速度的导数
Z_q	$u^* + \frac{\rho V_a^* S C_{Z_q} q^*}{4m}$	俯仰角速度对升力的影响
Z_{δ_e}	$\frac{\rho V_a^* S C_{Z_{\delta_e}}}{2m}$	升降舵偏角对升力的导数
M_u	$\frac{u^* \rho S c}{J_y} (C_{m_0} + C_{m_\alpha} \alpha^* + C_{m_{\delta_e}} \delta_e^*) + \frac{\rho S c^2 C_{m_q} q^* u^*}{4 J_y V_a^*} - \frac{\rho S c C_{m_\alpha} w^*}{2 J_y}$	俯仰力矩对前向速度的敏感度
M_w	$\frac{w^* \rho S c}{J_y} (C_{m_0} + C_{m_\alpha} \alpha^* + C_{m_{\delta_e}} \delta_e^*) + \frac{\rho S c^2 C_{m_q} q^* w^*}{4 J_y V_a^*} + \frac{\rho S c C_{m_\alpha} u^*}{2 J_y}$	俯仰力矩随垂向速度的变化
M_q	$\frac{\rho V_a^* S c^2 C_{m_q}}{4 J_y}$	俯仰阻尼导数
M_{δ_e}	$\frac{\rho V_a^* S c C_{m_{\delta_e}}}{2 J_y}$	升降舵偏角对俯仰力矩的影响

2.2 机体坐标系下的风扰动模型

为描述大气湍流与阵风对飞行器的影响, 假设地面风速 $\mathbf{V}_w$ 可分解为稳态分量与阵风分量

$$\mathbf{V}_w^b = \mathbf{R}_v^b(\phi, \theta, \psi) \mathbf{V}_{ws}^i + \mathbf{V}_{wg}^b, \quad (8)$$

其中 $\mathbf{V}_{ws}^i = [w_n, w_e, w_d]^T$ 为惯性系中的稳态风, $\mathbf{V}_{wg}^b = [u_w, v_w, w_w]^T$ 为机体系下的阵风分量, $\mathbf{R}_v^b(\phi, \theta, \psi)$ 为惯性系到机体系的旋转矩阵. 纵向运动仅涉及纵向平面内分量, 故考虑 $[u_w, w_w]^T$, 阵风通常由Dryden湍流模型生

成, 其传递函数为

$$H_u(s) = \sigma_u \sqrt{\frac{2V_a}{L_u}} \frac{1}{s + \frac{V_a}{L_u}}, \quad (9)$$

$$H_w(s) = \sigma_w \sqrt{\frac{3V_a}{L_w}} \frac{s + \frac{V_a}{L_w}}{\left(s + \frac{V_a}{L_w}\right)^2}, \quad (10)$$

其中 σ_u , σ_w 为沿机体 x , z 方向的湍流强度, L_u , L_w 为空间相关尺度, V_a 为名义空速. 上述滤波器可写成状态空间形式:

$$\dot{\mathbf{x}}_g = \mathbf{A}_g \mathbf{x}_g + \mathbf{B}_g \mathbf{n}, \quad \begin{bmatrix} u_w \\ w_w \end{bmatrix} = \mathbf{C}_g \mathbf{x}_g, \quad (11)$$

其中, $\mathbf{n} = [n_u, n_w]^T$ 为高斯白噪声.

2.3 纵向-风扰动耦合系统

空气动力由相对气流决定, 因此线性化后风扰动以加性扰动的形式进入纵向模型:

$$\dot{\mathbf{x}}_{\text{lon}} = \mathbf{A}_{\text{lon}} \mathbf{x}_{\text{lon}} + \mathbf{B}_{\text{lon}} \mathbf{u}_{\text{lon}} + \mathbf{E}_d \begin{bmatrix} u_w \\ w_w \end{bmatrix}, \quad (12)$$

其中风扰动输入矩阵为

$$\mathbf{E}_d = \begin{bmatrix} -X_u & -X_w \\ -Z_u & -Z_w \\ -M_u & -M_w \\ 0 & 0 \\ 0 & 0 \end{bmatrix}, \quad (13)$$

体现了风速在机体前向与法向方向上的影响.

3 基于导航量测的 χ^2 检测器

在实际无人机系统中, Kalman滤波器通常作为导航与状态估计的核心模块, 与纵向控制回路和高度保持任务直接耦合, 其残差信号被广泛用于异常检测与安全监测. 考虑风扰动, 本节将描述常见的基于Kalman滤波器的 χ^2 异常检测机构, 使用导航量测信号实时监控无人机纵向运动的异常情况. 首先, 将式(12)与Dryden湍流模型(11)联立, 可得增广状态空间形式:

$$\begin{bmatrix} \dot{\mathbf{x}}_{\text{lon}} \\ \dot{\mathbf{x}}_g \end{bmatrix} = \underbrace{\begin{bmatrix} \mathbf{A}_{\text{lon}} & \mathbf{E}_d \mathbf{C}_g \\ 0 & \mathbf{A}_g \end{bmatrix}}_A \underbrace{\begin{bmatrix} \mathbf{x}_{\text{lon}} \\ \mathbf{x}_g \end{bmatrix}}_x + \underbrace{\begin{bmatrix} \mathbf{B}_{\text{lon}} \\ 0 \end{bmatrix}}_B \mathbf{u}_{\text{lon}} + \underbrace{\begin{bmatrix} \mathbf{E}_d \mathbf{B}_g \\ \mathbf{B}_g \end{bmatrix}}_G \mathbf{n}, \quad (14)$$

其中 $\mathbf{n}$ 为高斯白噪声, 满足 $\mathbf{n}(t) \sim \mathcal{N}(0, \mathbf{Q})$.

小型固定翼无人机通常搭载惯性导航系统、全球导航卫星系统(global navigation satellite system, GNSS)、空速管以及气压高度计, 以获取姿态、速度与位置等飞行状态信息. 在纵向动力学中高度 h 由GNSS与气压高度计融合获得; 空速 u 由GNSS和惯性导航系统融合测量; 迎角 α 测量较为复杂, 小型无人机中无测量装置. 综合上述传感器配置, 定义系统的测量输出向量为

$$\mathbf{y} = [u \ h]^T.$$

我们考虑欺骗攻击信号是通过GNSS注入到无人机系统, 并假设可以任意影响被GNSS测量的 u 和 h . 那么攻击下的测量方程可以表示为

$$\mathbf{y} = \mathbf{C}\mathbf{x} + \mathbf{m} + \mathbf{a}, \quad (15)$$

其中 $\mathbf{m}$ 为测量噪声, 满足 $\mathbf{m}(t) \sim \mathcal{N}(0, \mathbf{R})$, $\mathbf{a}$ 为错误数据注入攻击信号. 我们假设过程噪声 $\mathbf{n}$ 与测量噪声 $\mathbf{m}$ 是相互独立的. 另外 $\mathbf{C} = [\mathbf{C}_{\text{lon}} \ \mathbf{0}]$ 为测量矩阵, 其中

$$\mathbf{C}_{\text{lon}} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

针对增广系统(14), 测量方程(15), 我们给出连续时间的Kalman滤波器为

$$\dot{\hat{\mathbf{x}}}(t) = \mathbf{A}\hat{\mathbf{x}}(t) + \mathbf{B}\mathbf{u}(t) + \mathbf{L}(\mathbf{y}(t) - \mathbf{C}\hat{\mathbf{x}}(t)), \quad (16)$$

其中增益矩阵

$$\mathbf{L} = \mathbf{P}\mathbf{C}^T \mathbf{R}^{-1}, \quad (17)$$

且误差协方差矩阵 $\mathbf{P}$ 满足Riccati方程

$$\mathbf{A}\mathbf{P} + \mathbf{P}\mathbf{A}^T + \mathbf{E}\mathbf{Q}\mathbf{E}^T - \mathbf{P}\mathbf{C}^T \mathbf{R}^{-1} \mathbf{C}\mathbf{P} = \mathbf{0}. \quad (18)$$

定义滤波误差为 $\mathbf{e}(t) = \mathbf{x}(t) - \hat{\mathbf{x}}(t)$, 其动态方程为

$$\dot{\mathbf{e}}(t) = (\mathbf{A} - \mathbf{L}\mathbf{C})\mathbf{e}(t) + \mathbf{E}\mathbf{n}(t) - \mathbf{L}\mathbf{m}(t) - \mathbf{L}\mathbf{a}(t). \quad (19)$$

据此可得连续时间残差为

$$\mathbf{r}(t) = \mathbf{y}(t) - \mathbf{C}\hat{\mathbf{x}}(t) = \mathbf{C}\mathbf{e}(t) + \mathbf{m} + \mathbf{a}. \quad (20)$$

在系统正常工作条件下, 残差均值为零, 其协方差为

$$\mathbf{S} \triangleq \mathbb{E}[\mathbf{r}(t)\mathbf{r}^T(t)] = \mathbf{C}\mathbf{P}\mathbf{C}^T + \mathbf{R}. \quad (21)$$

为消除量纲与相关性影响, 对残差进行标准化(白化):

$\mathbf{S}^{-1/2}\mathbf{r}(t) \sim \mathcal{N}(0, 1)$. 由此构造检测统计量

$$J(t) \triangleq \mathbf{r}^T(t)\mathbf{S}^{-1}\mathbf{r}(t) \sim \chi_p^2. \quad (22)$$

其中自由度 p 等于测量维数. 因此, 我们具有如下的异常决策规则:

$$\begin{cases} H_0: J(t) \sim \chi_p^2, & \text{系统正常, 无故障或攻击,} \\ H_1: J(t) \not\sim \chi_p^2, & \text{系统故障, 存在故障或攻击,} \end{cases} \quad (23)$$

给定显著性水平 β , 可通过 χ^2 分布的上分位点确定检测阈值

$$J_{th} = \chi_p^2(1 - \beta). \quad (24)$$

那么, 可得到

$$\mathbb{P}\{J(t) > J_{th} \mid H_0\} = \beta. \quad (25)$$

即在正常状态下, 检测统计量 $J(t)$ 超过 J_{th} 的概率不超过 β . 据此得到检测判据

$$\begin{cases} J(t) \leq J_{th}, & H_0, \text{系统正常,} \\ J(t) > J_{th}, & H_1, \text{系统异常.} \end{cases} \quad (26)$$

连续时间残差 $\mathbf{r}(t)$ 反映了系统输出与滤波预测输出之间的差异, 在模型准确且噪声服从高斯分布时, $\mathbf{r}(t)$ 仅包含噪声信息. 当系统受到故障或攻击时, $\mathbf{r}(t)$ 的均值或方差偏离理论值, 导致 $J(t)$ 的期望显著增大. 因此, 卡方检测器通过监测标准化残差能量的异常增长, 实现了从统计意义上对系统健康状态的判别.

4 隐蔽导航欺骗攻击设计

本节针对建立的无人机与风耦合的纵向增广模型(14), 测量方程(15)和 χ^2 异常检测器, 设计式(15)中的隐蔽导航欺骗攻击 $\mathbf{a}$. 在给出隐蔽导航欺骗攻击的形式化定义之前, 本文首先通过图1总结无人机基于GNSS导航的纵向闭环控制结构, 并明确风扰动与导航欺骗攻击在闭环系统中的作用通道.

隐蔽攻击的定义如下:

定义1 如果在导航欺骗攻击 $\mathbf{a}$ 的作用下, 基于检测规则(26)的 χ^2 检测器漏报率渐进满足式(25), 即

$$\lim_{t \rightarrow \infty} \mathbb{P}\{J(t) > J_{th} \mid H_0\} = \beta, \quad (27)$$

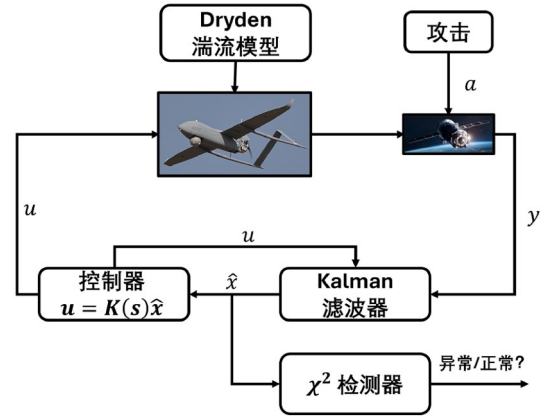


图1 (网络版彩图)基于GNSS导航的无人机纵向闭环控制结构及隐蔽导航欺骗攻击的注入位置

Figure 1 (Color online) GNSS-based attack injection for the drone.

则攻击 $\mathbf{a}$ 是隐蔽的.

考虑误差系统(19)和残差系统(20), 我们得到从 $\mathbf{a}$ 到 $\mathbf{r}$ 的传递函数矩阵具有如下实现:

$$\mathbf{G}_{ra}(s) = \begin{bmatrix} \mathbf{A} - \mathbf{LC} & -\mathbf{L} \\ \mathbf{C} & \mathbf{I} \end{bmatrix}. \quad (28)$$

因此, 我们定义如下的灵敏度和补灵敏度函数:

定义2 (从 $\mathbf{a}$ 到 $\mathbf{r}$ 的灵敏度函数与补灵敏度函数) 基于状态空间实现(28), 从攻击 $\mathbf{a}$ 到残差 $\mathbf{r}$ 的灵敏度函数为

$$\mathbf{P}_a(s) \triangleq \mathbf{G}_{ra}(s) = \mathbf{I} - \mathbf{C}(s\mathbf{I} - (\mathbf{A} - \mathbf{LC}))^{-1}\mathbf{L}, \quad (29)$$

相应的补灵敏度函数定义为

$$\mathbf{M}_a(s) \triangleq \mathbf{C}(s\mathbf{I} - (\mathbf{A} - \mathbf{LC}))^{-1}\mathbf{L}. \quad (30)$$

显然, 对任意的 $s \in \mathbb{C}$, 有

$$\mathbf{P}_a(s) + \mathbf{M}_a(s) = \mathbf{I}. \quad (31)$$

下面的定理将给出灵敏度函数 $\mathbf{P}_a$ 和补灵敏度函数 $\mathbf{M}_a$ 的插值约束.

定理1 ($\mathbf{P}_a$ 的差值约束) 记 $\mathbf{A}_{lon}$ 的不稳定特征值为 λ_k , $k = 1, \dots, n$, 对应的非零特征向量为 $\mathbf{x}_k$, 即 $\mathbf{A}_{lon}\mathbf{x}_k = \lambda_k\mathbf{x}_k$. 令 $\bar{\mathbf{x}}_k = [\mathbf{x}_k^T, 0]^T$ 以及 $\boldsymbol{\eta}_k = \mathbf{C}\bar{\mathbf{x}}_k = \mathbf{C}_{lon}\mathbf{x}_k$, 则灵敏度函数与补灵敏度函数在 $s = \lambda_k$ 处满足如下插值约束:

$$\mathbf{P}_a(\lambda_k)\boldsymbol{\eta}_k = 0, \quad \mathbf{M}_a(\lambda_k)\boldsymbol{\eta}_k = \boldsymbol{\eta}_k.$$

证明 令 $\mathbf{A}_L \triangleq \mathbf{A} - \mathbf{L}\mathbf{C}$. 由特征值条件可得

$$(\lambda_k \mathbf{I} - \mathbf{A}_L) \mathbf{x}_k = (\lambda_k \mathbf{I} - \mathbf{A}) \mathbf{x}_k + \mathbf{L}\mathbf{C}\mathbf{x}_k = \mathbf{L}\mathbf{C}\mathbf{x}_k,$$

从而可得 $(\lambda_k \mathbf{I} - \mathbf{A}_L)^{-1} \mathbf{L}\mathbf{C}\mathbf{x}_k = \mathbf{x}_k$. 对该式两边左同时乘 $\mathbf{C}$ 得到 $\mathbf{C}(\lambda_k \mathbf{I} - \mathbf{A}_L)^{-1} \mathbf{L}\mathbf{C}\mathbf{x}_k = \mathbf{C}\mathbf{x}_k$. 进而可得

$$\mathbf{P}_a(\lambda_k) \boldsymbol{\eta}_k = \mathbf{C}\mathbf{x}_k - \mathbf{C}(\lambda_k \mathbf{I} - \mathbf{A}_L)^{-1} \mathbf{L}\mathbf{C}\mathbf{x}_k = 0.$$

同理, 可得

$$\mathbf{M}_a(\lambda_k) \boldsymbol{\eta}_k = \mathbf{C}(\lambda_k \mathbf{I} - \mathbf{A}_L)^{-1} \mathbf{L}\mathbf{C}\mathbf{x}_k = \mathbf{C}\mathbf{x}_k = \boldsymbol{\eta}_k.$$

因此, 定理得证.

注释1 定理1表明原系统矩阵 $\mathbf{A}_{\text{lon}}$ 的所有特征值会在从 $\mathbf{a}$ 到 $\mathbf{r}$ 的灵敏度函数 $\mathbf{P}_a(s)$ 上诱导出一个传输零点; 当该特征值处于右半平面时, $\mathbf{P}_a(s)$ 必然在该点具有右半平面零点, 从而灵敏度函数在攻击-残差通道上呈现非最小相位特性. 这为后续隐蔽攻击设计与分析提供了状态空间层面的插值约束基础.

上述结果从攻击-残差通道的角度揭示了无人机纵向动力学不稳定模态在隐蔽攻击形成中的结构性作用. 下面进一步分析该结构性特征在闭环输出通道中的影响, 以说明攻击信号在保持残差隐蔽的同时, 如何仍能对无人机纵向运动产生实质性作用. 考虑纵向线性化模型的状态空间(5)和测量方程(15), 我们具有如下的实现:

$$\mathbf{P}(s) = \begin{bmatrix} \mathbf{A}_{\text{lon}} & \mathbf{B}_{\text{lon}} \\ \mathbf{C} & \mathbf{0} \end{bmatrix}, \quad (32)$$

及其左右互质分解

$$\mathbf{P}(s) = \mathbf{N}_r(s) \mathbf{M}_r^{-1}(s) = \mathbf{M}_l^{-1}(s) \mathbf{N}_l(s), \quad (33)$$

其中 $\mathbf{N}_r, \mathbf{M}_r, \mathbf{N}_l, \mathbf{M}_l \in RH_\infty$, 并存在 $\mathbf{X}_r, \mathbf{Y}_r, \mathbf{X}_l, \mathbf{Y}_l \in RH_\infty$ 使得

$$\begin{bmatrix} \mathbf{X}_r & \mathbf{Y}_r \\ -\mathbf{N}_l & \mathbf{M}_l \end{bmatrix} \begin{bmatrix} \mathbf{M}_r & -\mathbf{Y}_l \\ \mathbf{M}_r & \mathbf{X}_l \end{bmatrix} = \begin{bmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{I} \end{bmatrix}. \quad (34)$$

对给定的 $\mathbf{P}(s)$, 选择任意使

$$\mathbf{A}_F := \mathbf{A}_{\text{lon}} + \mathbf{B}_{\text{lon}} \mathbf{F} \text{ 和 } \mathbf{A}_L := \mathbf{A}_{\text{lon}} + \mathbf{L}\mathbf{C}_{\text{lon}},$$

均为Hurwitz的反馈矩阵 $\mathbf{F}$ 与观测矩阵 $\mathbf{L}$. 则可构造一组规范右互素因式分解如下:

$$\begin{aligned} \mathbf{M}_r(s) &= \mathbf{I} + \mathbf{C}_{\text{lon}}(s\mathbf{I} - \mathbf{A}_F)^{-1} \mathbf{B}_{\text{lon}}, \\ \mathbf{N}_r(s) &= \mathbf{C}_{\text{lon}}(s\mathbf{I} - \mathbf{A}_F)^{-1} \mathbf{B}_{\text{lon}}, \end{aligned} \quad (35)$$

$$\begin{aligned} \mathbf{X}_r(s) &= \mathbf{I} + \mathbf{F}\mathbf{C}_{\text{lon}}(s\mathbf{I} - \mathbf{A}_L)^{-1} \mathbf{B}_{\text{lon}}, \\ \mathbf{Y}_r(s) &= \mathbf{F} + \mathbf{F}\mathbf{C}_{\text{lon}}(s\mathbf{I} - \mathbf{A}_L)^{-1} \mathbf{B}_{\text{lon}}. \end{aligned} \quad (36)$$

则可取一组与之对偶的左规范互素因子为

$$\begin{aligned} \mathbf{M}_l(s) &= \mathbf{I} + \mathbf{B}_{\text{lon}}(s\mathbf{I} - \mathbf{A}_L)^{-1} \mathbf{C}_{\text{lon}}, \\ \mathbf{N}_l(s) &= \mathbf{B}_{\text{lon}}(s\mathbf{I} - \mathbf{A}_L)^{-1} \mathbf{C}_{\text{lon}}, \end{aligned} \quad (37)$$

$$\begin{aligned} \mathbf{X}_l(s) &= \mathbf{I} + \mathbf{L}\mathbf{C}_{\text{lon}}(s\mathbf{I} - \mathbf{A}_F)^{-1} \mathbf{B}_{\text{lon}}, \\ \mathbf{Y}_l(s) &= \mathbf{L} + \mathbf{L}\mathbf{C}_{\text{lon}}(s\mathbf{I} - \mathbf{A}_F)^{-1} \mathbf{B}_{\text{lon}}. \end{aligned} \quad (38)$$

那么, 所有使 (P, K) 闭环内部稳定的线性时不变控制器可由自由稳定参数 $\mathbf{Q}(s) \in RH_\infty$ 参数化为

$$\begin{aligned} \mathbf{K}(s) &= -(\mathbf{X}_l(s) - \mathbf{Q}(s)\mathbf{N}_l(s))(\mathbf{Y}_r(s) + \mathbf{Q}(s)\mathbf{M}_l(s))^{-1} \\ &= -(\mathbf{X}_l(s) + \mathbf{Q}(s)\mathbf{N}_l(s))^{-1}(\mathbf{Q}(s)\mathbf{M}_l(s) + \mathbf{Y}_r(s)). \end{aligned} \quad (39)$$

Ding等人^[18]给出的Youla统一控制律为

$$\mathbf{u}_{\text{lon}} = \mathbf{F}\hat{\mathbf{x}}_{\text{lon}} - \mathbf{Q}(s)\mathbf{r}, \quad (40)$$

其中 $\hat{\mathbf{x}}_{\text{lon}}$ 是 $\mathbf{x}_{\text{lon}}$ 的估计, $\mathbf{F}$ 使 $(\mathbf{A}, \mathbf{B})$ 稳定, $\mathbf{Q}(s) \in RH_\infty$ 为Youla参数, $\mathbf{r}$ 在式(20)中给出. 将Youla参数化的控制器(40)带入纵向模型(5)得到

$$\begin{aligned} \dot{\mathbf{x}}_{\text{lon}} &= \mathbf{A}_{\text{lon}}\mathbf{x}_{\text{lon}} + \mathbf{B}_{\text{lon}}\mathbf{F}\hat{\mathbf{x}}_{\text{lon}} + \mathbf{B}_{\text{lon}}\mathbf{Q}\mathbf{r}, \\ \text{其观测器设计为} \\ \dot{\hat{\mathbf{x}}}_{\text{lon}} &= \mathbf{A}_{\text{lon}}\hat{\mathbf{x}}_{\text{lon}} + \mathbf{B}_{\text{lon}}\mathbf{F}\hat{\mathbf{x}}_{\text{lon}} + \mathbf{B}_{\text{lon}}\mathbf{Q}\mathbf{r} \\ &\quad + \mathbf{L}_{\text{lon}}(\tilde{\mathbf{y}} - \mathbf{C}\hat{\mathbf{x}}_{\text{lon}}) \\ &= (\mathbf{A}_{\text{lon}} - \mathbf{L}_{\text{lon}}\mathbf{C}_{\text{lon}})\hat{\mathbf{x}} + \mathbf{B}_{\text{lon}}\mathbf{F}\hat{\mathbf{x}} + \mathbf{B}_{\text{lon}}\mathbf{Q}\mathbf{r} \\ &\quad + \mathbf{L}_{\text{lon}}\mathbf{C}_{\text{lon}}\mathbf{x} + \mathbf{L}_{\text{lon}}\mathbf{a}. \end{aligned} \quad (41)$$

令闭环状态

$$\mathbf{z} := \begin{bmatrix} \mathbf{x}_{\text{lon}} \\ \hat{\mathbf{x}}_{\text{lon}} \end{bmatrix}, \quad \tilde{\mathbf{y}} = \mathbf{C}_{\text{lon}}\mathbf{x}_{\text{lon}} = [\mathbf{C}_{\text{lon}} \quad \mathbf{0}]\mathbf{z},$$

则闭环系统可写为

$$\dot{\mathbf{z}} = \mathbf{A}_{\text{cl}}\mathbf{z} + \mathbf{B}_{\text{Q}}\mathbf{r} + \mathbf{B}_{\text{a}}\mathbf{a}, \quad \tilde{\mathbf{y}} = \mathbf{C}_{\text{y}}\mathbf{z},$$

其中

$$\begin{aligned} \mathbf{A}_{\text{cl}} &:= \begin{bmatrix} \mathbf{A}_{\text{lon}} & \mathbf{B}_{\text{lon}}\mathbf{F} \\ \mathbf{L}_{\text{lon}}\mathbf{C}_{\text{lon}} & \mathbf{A}_{\text{lon}} - \mathbf{L}_{\text{lon}}\mathbf{C}_{\text{lon}} \end{bmatrix}, \quad \mathbf{B}_{\text{Q}} := \begin{bmatrix} \mathbf{B}_{\text{lon}}\mathbf{Q} \\ \mathbf{B}_{\text{lon}}\mathbf{Q} \end{bmatrix}, \\ \mathbf{B}_{\text{a}} &:= \begin{bmatrix} \mathbf{0} \\ \mathbf{L}_{\text{lon}} \end{bmatrix}, \quad \mathbf{C}_{\text{y}} := [\mathbf{C}_{\text{lon}} \quad \mathbf{0}]. \end{aligned}$$

因此, 在文献[19]给出的标准单位负反馈结构下从输

出端叠加信号 $\mathbf{a}$ 到输出 $\mathbf{y}$ 的传递函数为补输出灵敏度函数, 可以表示为

$$\mathbf{G}_{ay}(s) = -\mathbf{T}_o(s) = \mathbf{C}_y(s\mathbf{I} - \mathbf{A}_{cl})^{-1}(\mathbf{B}_a + \mathbf{B}_Q\mathbf{P}_a).$$

下面的定理给出该灵敏度函数 $\mathbf{T}_o(s)$ 的插值约束.

定理2 ($\mathbf{T}_o$ 插值约束) 假设 $\mathbf{A}_{lon}$ 存在不稳定特征对 $(\lambda_k, \mathbf{x}_k)$, 满足 $\mathbf{A}_{lon}\mathbf{x}_k = \lambda_k\mathbf{x}_k$, 令 $\boldsymbol{\eta}_k = \mathbf{C}_{lon}\mathbf{x}_k$, 则输出补灵敏度函数 $\mathbf{T}_o(s)$ 在点 $(\lambda_k, \boldsymbol{\eta}_k)$ 上满足

$$\mathbf{T}_o(\lambda_k)\boldsymbol{\eta}_k = \boldsymbol{\eta}_k.$$

证明 由于 $\mathbf{F}$ 和 $\mathbf{L}$ 分别使 $(\mathbf{A}_{lon}, \mathbf{B}_{lon})$ 与 $(\mathbf{A}_{lon}, \mathbf{C}_{lon})$ 可稳定和可检测, 分离原理保证 $\mathbf{A}_{cl}$ Hurwitz, 因此, $\lambda_k\mathbf{I} - \mathbf{A}_{cl}$ 在所有右半平面 λ_k 处均可逆. 定义向量

$$\mathbf{z}_k := \begin{bmatrix} \mathbf{x}_k \\ 0 \end{bmatrix}.$$

利用 $(\lambda_k\mathbf{I} - \mathbf{A}_{lon})\mathbf{x}_k = 0$ 及 $\mathbf{L}_{lon}\mathbf{C}_{lon}\mathbf{x}_k = \mathbf{L}_{lon}\boldsymbol{\eta}_k$, 可直接计算

$$(\lambda_k\mathbf{I} - \mathbf{A}_{cl})\mathbf{z}_k = \begin{bmatrix} (\lambda_k\mathbf{I} - \mathbf{A}_{lon})\mathbf{x}_k \\ \mathbf{L}_{lon}\mathbf{C}_{lon}\mathbf{x}_k \end{bmatrix} = \begin{bmatrix} \mathbf{0} \\ \mathbf{L}_{lon}\boldsymbol{\eta}_k \end{bmatrix} = \mathbf{B}_a\boldsymbol{\eta}_k.$$

由于 $(\lambda_k\mathbf{I} - \mathbf{A}_{cl})$ 可逆, 可得 $\mathbf{z}_k = (\lambda_k\mathbf{I} - \mathbf{A}_{cl})^{-1}\mathbf{B}_a\boldsymbol{\eta}_k$. 对上式左乘 $\mathbf{C}_y$ 得

$$\mathbf{C}_y(\lambda_k\mathbf{I} - \mathbf{A}_{cl})^{-1}\mathbf{B}_a\boldsymbol{\eta}_k = \mathbf{C}_{lon}\mathbf{x}_k = \boldsymbol{\eta}_k.$$

另外, 基于定理1, $\mathbf{P}_a(\lambda_k)\boldsymbol{\eta}_k = 0$, 那么可得

$$\mathbf{T}_o(\lambda_k)\boldsymbol{\eta}_k = -\mathbf{C}_y(\lambda_k\mathbf{I} - \mathbf{A}_{cl})^{-1}(\mathbf{B}_a + \mathbf{B}_Q\mathbf{P}_a)\boldsymbol{\eta}_k = \boldsymbol{\eta}_k.$$

定理得证.

注释2 进一步刻画了上述结构性特征在闭环输出通道中的影响. 该定理表明, 尽管攻击信号在残差通道中被抑制, 但在输出补灵敏度函数中, 不稳定特征值对应的方向却满足严格的插值约束, 使得攻击信号能够在输出通道中完整激发相应的不稳定模态. 这一结果揭示了攻击“隐蔽性”与“破坏性”并存的内在机理: 攻击信号一方面无法通过基于残差能量的 χ^2 检测器被察觉, 另一方面却能够沿无人机纵向不稳定模态持续驱动飞行状态偏离参考轨迹. 在本文中, 正是基于该定理结论选择攻击注入方向并构造攻击信号的时间演化形式, 从而保证所设计导航欺骗攻击在理论上具有严格的隐蔽性, 同时对纵向飞行安全造成实质性影响.

考虑将攻击信号直接加在导航测量噪声通道, 设计的攻击信号如下:

$$\mathbf{a}_k(t) := e^{\lambda_k t} \boldsymbol{\eta}_k, \quad t \geq 0. \quad (42)$$

其中 $(\lambda_k, \mathbf{x}_k)$ 是 $\mathbf{A}_{lon}$ 的不稳定特征对, $(\lambda_k, \mathbf{x}_k)$ 满足

$$\mathbf{A}_{lon}\mathbf{x}_k = \lambda_k\mathbf{x}_k, \quad \boldsymbol{\eta}_k := \mathbf{C}_{lon}\mathbf{x}_k \neq 0.$$

我们可得到如下的定理.

定理3 (隐蔽导航欺骗攻击) 令被控对象与观测器的初始条件为

$$\mathbf{x}(0) = 0, \quad \hat{\mathbf{x}}(0) = 0.$$

则攻击 $\mathbf{a}_k$ 是定义1意义下的隐蔽导航欺骗攻击, 即满足式(27). 更进一步,

$$\mathbf{y}_{lon}(t) = -\mathbf{a}_k(t) + \mathbf{y}_s(t), \quad \lim_{t \rightarrow \infty} \mathbf{y}_s(t) = 0. \quad (43)$$

证明 证明过程分为两步: 首先给出残差与输出在确定性部分的渐近性质, 然后在此基础上讨论 χ^2 统计量的分布.

首先忽略噪声项 $\mathbf{n}, \mathbf{m}$ 考虑残差系统

$$\mathbf{e}(t) = (\mathbf{A} - \mathbf{LC})\mathbf{e}(t) - \mathbf{L}\mathbf{a}_k(t), \quad \mathbf{r}_n(t) = \mathbf{C}\mathbf{e}(t) + \mathbf{a}_k(t),$$

并将攻击信号(42). 取特解 $\mathbf{e}_p(t) = -\mathbf{x}_k e^{\lambda_k t}$, 再配合齐次解 $\mathbf{e}_h(t) = e^{(\mathbf{A} - \mathbf{LC})t} \mathbf{x}_k$, 可得到

$$\mathbf{e}(t) = e^{(\mathbf{A} - \mathbf{LC})t} \mathbf{x}_k - \mathbf{x}_k e^{\lambda_k t},$$

从而残差为

$$\mathbf{r}(t) = \mathbf{C}\mathbf{e}(t) + \mathbf{a}_k(t) = \mathbf{C}e^{(\mathbf{A} - \mathbf{LC})t} \mathbf{x}_k.$$

由于 $\mathbf{A} - \mathbf{LC}$ Hurwitz, 以及其像 $\mathbf{C}e^{(\mathbf{A} - \mathbf{LC})t} \mathbf{x}_k$ 均指数收敛到0. 令

$$\mathbf{r}(t) = \mathbf{r}_a(t) + \mathbf{r}_n(t),$$

其中 $\mathbf{r}_n(t)$ 由零均值高斯噪声经线性时不变系统生成, 因此对每个 t , $\mathbf{r}_n(t)$ 服从零均值高斯分布, 且

$$\mathbb{E}[\mathbf{r}_n(t)\mathbf{r}_n^T(t)] = \mathbf{S} = \mathbf{C}\mathbf{P}\mathbf{C}^T + \mathbf{R},$$

即 $\mathbf{r}_n(t) \sim \mathcal{N}(0, \mathbf{S})$. 由此可得检验统计量 $J(t) = \mathbf{r}^T(t)\mathbf{S}^{-1}\mathbf{r}(t)$ 满足

$$J(t) \sim \chi_p^2.$$

因此, 对任意给定显著性水平 β 与对应阈值 $J_{th} = \chi_p^2(1 - \beta)$,

当 $t \rightarrow \infty$, 有

$$\mathbb{P}\{\chi_p^2 > J_{th}\} = \beta.$$

这恰与正常工况 H_0 下的误报概率一致. 换言之, 在攻击 $\mathbf{a}_k$ 存在的情况下, 检测器 χ^2 在渐近意义上无法区分“有攻击”与“无攻击”两种情形, 其漏报率满足定义1中给出的条件, 故 $\mathbf{a}_k$ 为隐蔽导航欺骗攻击.

对输出通道, 攻击信号的拉普拉斯变换为

$$\mathbf{A}_k(s) = \frac{\boldsymbol{\eta}_k}{s - \lambda_k}.$$

由闭环结构可知, 从 $\mathbf{a}$ 到输出 $\mathbf{y}$ 的传递函数为 $\mathbf{G}_{ay}(s) = -\mathbf{T}_o(s)$, 因此

$$\mathbf{Y}(s) = \mathbf{G}_{ay}(s)\mathbf{A}_k(s) = -\mathbf{T}_o(s)\frac{\boldsymbol{\eta}_k}{s - \lambda_k}.$$

利用输出补灵敏度函数 $\mathbf{T}_o(s)$ 的插值约束 $\mathbf{T}_o(\lambda_k)\boldsymbol{\eta}_k = \boldsymbol{\eta}_k$ (参见前述定理), 可在 $s = \lambda_k$ 处将向量函数 $\mathbf{T}_o(s)\boldsymbol{\eta}_k$ 展开为

$$\mathbf{T}_o(s)\boldsymbol{\eta}_k = \boldsymbol{\eta}_k + (s - \lambda_k)\boldsymbol{\psi}_k(s),$$

其中 $\boldsymbol{\psi}_k(s)$ 在 $s = \lambda_k$ 的邻域内解析且有界. 代入 $\mathbf{Y}(s)$ 得

$$\mathbf{Y}(s) = -\frac{\boldsymbol{\eta}_k}{s - \lambda_k} - \boldsymbol{\psi}_k(s).$$

对其作拉普拉斯逆变换, 可得时间域响应

$$\mathbf{y}(t) = -\mathbf{e}^{\lambda_k t}\boldsymbol{\eta}_k + \mathbf{y}_s(t) = -\mathbf{a}_k(t) + \mathbf{y}_s(t),$$

其中 $\mathbf{y}_s(t)$ 是稳定有理矩阵 $\boldsymbol{\psi}_k(s)$ 的逆变换所对应的响应, 仅包含左半平面的稳定模态, 因此 $\mathbf{y}_s(t) \rightarrow 0$, 得到式(43).

综上所述, 攻击信号(42)同时满足残差渐近为零与 χ^2 统计量分布渐近不变两点意义上的隐蔽性, 定理得证.

5 仿真与验证

仿真中采用的系统参数来源于 Aerosonde 固定翼无人机的纵向动力学模型, 该模型在低空飞行条件下具有典型的纵向不稳定特征, 能够真实反映实际无人机在导航与控制系统中的动态行为. 本节给出基于 Aerosonde 无人机以及 Dryden 阵风模型的仿真结果, 验证

所提出的导航欺骗攻击的隐蔽性. Aerosonde 无人机及 Dryden 阵风模型的参数如表2所示.

基于增广纵向-阵风耦合模型(5)与测量方程(15), 本节首先给出用于数值仿真的 Kalman 滤波器与 χ^2 检测器参数配置. 在增广系统中 $\mathbf{x} \in \mathbb{R}^8$ 为增广状态, $\mathbf{u}_{lon} \in \mathbb{R}^2$ 为升降舵与油门输入, $\mathbf{y} = [u, h]^T$ 为纵向速度与高度量测, $\mathbf{n}(t) \sim \mathcal{N}(0, \mathbf{Q})$ 、 $\mathbf{m}(t) \sim \mathcal{N}(0, \mathbf{R})$ 为相互独立的过程噪声与测量噪声. 为了体现低空小型无人机环境下的典型噪声水平, 仿真中选取

$$\mathbf{Q} = \text{diag}\{10^{-4}, 10^{-4}, 10^{-4}, 10^{-5}, 10^{-5}, 10^{-4}, 10^{-4}, 10^{-4}\},$$

$$\mathbf{R} = \text{diag}\{(0.5 \text{ m/s})^2, (1.0 \text{ m})^2\},$$

即假设纵向速度量测标准差约为 0.5 m/s, 高度量测标准差约为 1 m. 需要说明的是, 仿真中所采用的过程噪声协方差矩阵 $\mathbf{Q}$ 用于刻画无人机纵向动力学中未建模的气动扰动、阵风影响及参数不确定性, 其量级选取参考了低空飞行条件下常见扰动水平, 并保证在无攻击工况下 Kalman 滤波器能够实现稳定、合理的状态估计. 量测噪声协方差矩阵 $\mathbf{R}$ 则用于描述无人机常用传感器的测量噪声特性, 其中速度与高度通道的噪声方差量级与工程中典型的空速计和高度测量传感器精度相一致. 上述噪声参数的选取旨在构建具有代表性的工程噪声环境, 而非针对特定型号传感器进行精细标定.

在此配置下, 由连续时间代数 Riccati 方程(18)可求得稳态协方差矩阵 $\mathbf{P}$, 进而得到 $\mathbf{L}$ 和 Kalman 滤波器. 在无攻击且仅存在高斯噪声时, 残差 $\mathbf{r}$ 满足零均值高斯分布, 其协方差收敛到 $\mathbf{S}$, 满足零均值高斯分布, 其协方差收敛到 $\mathbf{S}$, 据此构造标准化残差能量 $J(t)$, 其在稳态近似服从自由度 $p = 2$ 的 χ^2 分布, 即 $J(t) \sim \chi_2^2$. 仿真中取显著性水平 $\beta = 0.01$, 则检测阈值为

$$J_{th} = \chi_2^2(0.99) \approx 9.21.$$

当 $J(t) > J_{th}$ 时判断系统存在异常, 否则认为系统处于正常工作状态.

5.1 本文设计攻击仿真分析

接下来, 按照式(42)构造隐蔽导航欺骗攻击. 首先对 $\mathbf{A}_{lon}$ 求解特征值问题, 得到其右半平面的不稳定特

表 2 Aerosonde无人机及Dryden阵风模型所用参数

Table 2 Parameters of Aerosonde and Dryden model

参数	数值(含单位)	物理含义
m	13.5 kg	无人机质量
J_y	1.135 kg m ²	绕机体 y 轴的俯仰转动惯量
S	0.55 m ²	机翼参考面积
c	0.18994 m	平均气动弦长
ρ	1.2682 kg/m ³	大气密度(低空)
V_a^*	30 m/s	配平空速
g	9.81 m/s ²	重力加速度
C_{L0}	0.28	升力系数零攻角截距
C_{D0}	0.03	阻力系数零升力截距
C_{m0}	-0.38	俯仰力矩系数零攻角截距
$C_{L\alpha}$	3.45	升力系数对攻角的导数(升力刚度)
$C_{D\alpha}$	0.30	阻力系数对攻角的导数
$C_{m\alpha}$	-0.38	俯仰力矩系数对攻角的导数(静稳定性)
C_{mq}	-3.6	俯仰力矩系数对俯仰角速度的导数(阻尼导数)
$C_{L\delta_e}$	0.3476	升力系数对升降舵偏角的导数
$C_{m\delta_e}$	-0.5	俯仰力矩系数对升降舵偏角的导数
L_u	200 m	水平阵风尺度长度(Dryden模型)
L_w	50 m	垂直阵风尺度长度(Dryden模型)
σ_u	1.5 m/s	水平阵风速度标准差
σ_w	1.0 m/s	垂直阵风速度标准差

征对 $(\lambda_k, \mathbf{x}_k)$, 即 $\mathbf{A}_{\text{lon}}\mathbf{x}_k = \lambda_k\mathbf{x}_k, \Re(\lambda_k) > 0$. 数值计算表明, $\mathbf{A}_{\text{lon}}$ 在右半平面存在一对实特征值, 记其中正实部较大的为 $\lambda_k \approx 1.94$. 该特征值对应于纵向不稳定模态(类似于缓慢发散的长周期模态). 取相应的特征向量 $\mathbf{x}_k$, 并令

$$\boldsymbol{\eta}_k = \mathbf{C}_{\text{lon}}\mathbf{x}_k \neq 0,$$

即 $\boldsymbol{\eta}_k$ 直接给出了在该不稳定模态下纵向速度与高度输出的方向. 因此, 按照定理3, 将攻击信号设计为

$$\mathbf{a}_k(t) = \alpha_0 e^{\lambda_k t} \boldsymbol{\eta}_k, \quad t \geq 0, \quad (44)$$

其中 $\alpha_0 > 0$ 为攻击幅值系数, 用于调节攻击强度. 攻击通过GNSS通道叠加在纵向速度和高度量测上, 仿真中选取 $\alpha_0 = 0.05$, 保证攻击在初始阶段幅值较小, 不会

在短时间内引起明显的突变, 从而更符合渐进隐蔽攻击的物理场景.

为系统评估 χ^2 检测器在隐蔽攻击下的性能, 设计如下两组对比工况. 工况1(正常工况): 系统在纵向恒定高度与空速配平点附近飞行, 输入 $\mathbf{u}_{\text{lon}}(t)$ 按照Youla参数化的 $\mathbf{K}$ 给出, 存在风扰动与导航噪声, 但无攻击信号, 即 $\mathbf{a}(t) \equiv 0$; 工况2(隐蔽攻击工况): 在 $t = t_a$ 时刻起(例如 $t_a = 50$ s), 攻击者开始向GNSS测量注入攻击信号 $\mathbf{a}_k(t)$, 其形式如(44)所示, 其余条件与工况1完全相同.

图2给出了工况1和2下 χ^2 检测统计量 $J(t)$ 的时间演化曲线以及检测阈值 J_{th} . 可以观察到, 在正常工况下 $J(t)$ 在阈值附近随机波动, 偶尔出现越阈, 但总体越

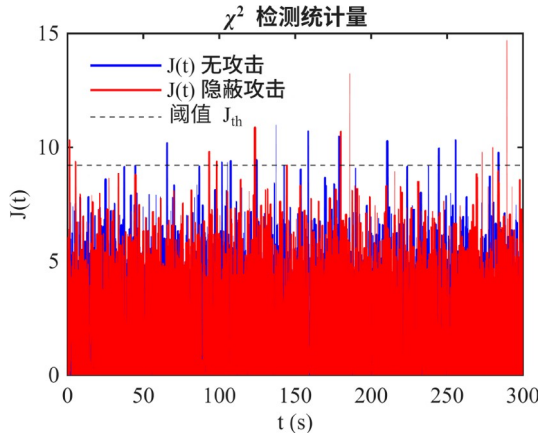


图2 (网络版彩图)工况1和2下 χ^2 检测统计量 $J(t)$ 与阈值 J_{th} 比较

Figure 2 (Color online) Comparison of the χ^2 test statistic $J(t)$ and the threshold J_{th} under operating conditions 1 and 2.

阈概率与显著性水平 $\beta = 0.01$ 相一致, 验证了Kalman滤波器与 χ^2 检测器参数整定的合理性. 在隐蔽攻击工况下, 攻击开始前($t < t_a$)的曲线与正常工况几乎完全重合; 攻击启动后, 由于定理3所示的插值约束, 从攻击到残差的灵敏度函数 $\mathbf{P}_a(s)$ 在 $s = \lambda_k$ 处具有右半平面零点, 残差的确定性分量 $\mathbf{r}_a(t)$ 迅速衰减, $J(t)$ 的统计特性保持与无攻击工况近似相同. 数值仿真结果表明, 在整段仿真区间内, 工况2的越阈次数与工况1几乎一致, 其经验越阈概率与理论值 β 之间差异很小, 这说明所设计的攻击在 χ^2 检测器意义下是隐蔽的.

图3和4给出了两种工况下飞机状态的响应曲线. 从图中可以看出, 在正常工况下, 纵向速度和高度均稳定跟踪配平参考值, 仅在阵风作用下产生小幅波动; 而在隐蔽攻击工况中, 攻击启动后, $u(t)$ 与 $h(t)$ 沿着不稳定模态方向逐渐偏离配平点, 表现为高度缓慢但持续地发散. 尤其是在仿真末端, $h(t)$ 已经出现数十米量级的高度偏差, 但此时 $J(t)$ 仍然大部分时间保持在阈值以下, 检测器未能及时发出告警.

为进一步量化攻击对纵向飞行安全性的影响, 图5展示了攻击下高度误差的演化. 可以看到, 在攻击存在时, 高度误差大致以 $e^{\lambda_k t}$ 的速度增长, 与理论推导中 $\mathbf{y}(t) \approx -\mathbf{a}_k(t)$ 的结论一致, 这说明攻击信号成功将不稳定模态从残差通道“隐藏”到输出通道, 使得 χ^2 检测器无法察觉, 而无人机纵向轨迹却在攻击者预期方向

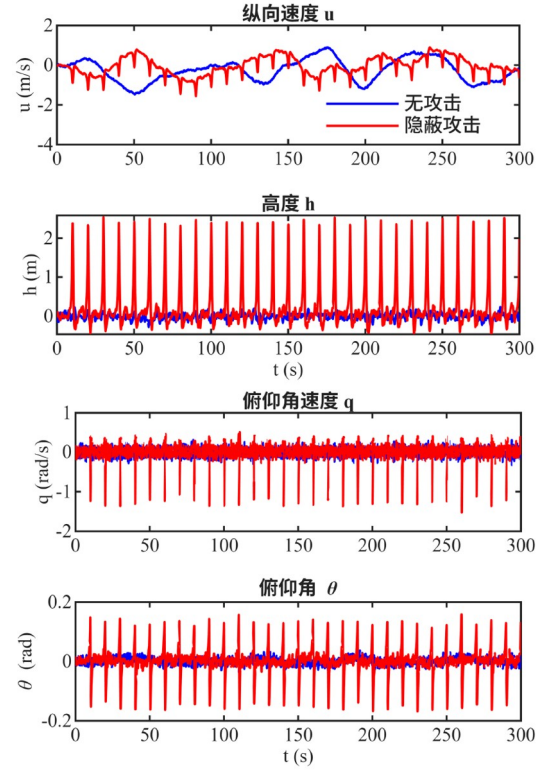


图3 (网络版彩图)俯仰角速度、俯仰角、纵向速度、高度正常工况与隐蔽攻击工况下的响应比较

Figure 3 (Color online) Comparison of pitch rate, pitch angle, longitudinal velocity, and altitude responses under normal and stealthy-attack conditions.

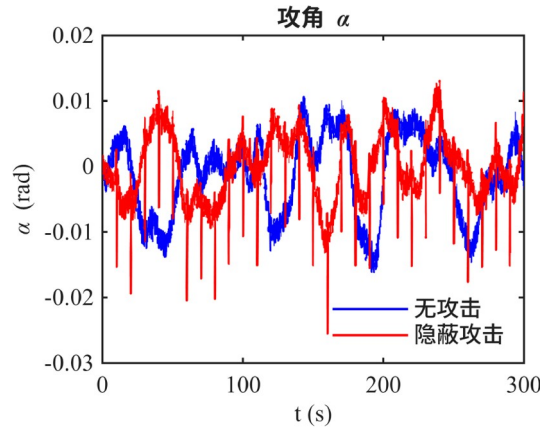


图4 (网络版彩图)攻角在正常工况与隐蔽攻击工况下的响应比较

Figure 4 (Color online) Comparison of attack angle responses under normal and stealthy-attack conditions.

上发生明显偏移.

综上所述, 仿真结果从两个方面验证了本文理论

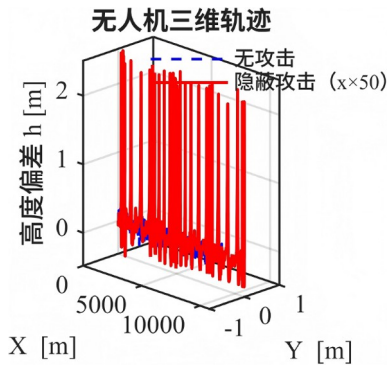


图 5 (网络版彩图)无人机位置在两种工况下的演化

Figure 5 (Color online) Time response of the UAV position under the two operating conditions.

分析的正确性:一方面,基于右半平面特征值和非最小相位零点构造的攻击信号 $\mathbf{a}_k(t)$ 使得 χ^2 检测统计量的稳态分布在有无攻击时保持近似不变,满足定义1中对隐蔽性的统计定义;另一方面,该攻击在纵向速度与高度通道上诱导了沿不稳定模态的显著轨迹偏移,说明即使在传统导航监视与异常检测机制未触发告警的情况下,无人机仍可能被逐步引导至危险飞行状态,凸显了基于系统结构脆弱性的隐蔽导航欺骗攻击的严重危害性。

5.2 重放攻击对比仿真分析

需要指出的是,本文的定理从系统结构层面揭示了隐蔽导航欺骗攻击得以成立的关键条件,即攻击信号必须能够沿无人机纵向动力学中的不稳定模态作用于闭环输出,同时在估计-检测结构中抑制残差响应。该结论意味着,并非所有导航欺骗攻击在同一检测框架下均具有隐蔽性,其隐蔽性高度依赖于攻击与系统动力学及观测结构之间的耦合关系。为进一步验证上述理论分析,并与典型攻击方式形成对照,本文补充考虑了一类重放攻击^[20]的对比仿真实验。该攻击在攻击窗口内将当前量测替换为历史纪录的量测数据,未针对无人机纵向不稳定模态及观测器结构进行专门设计。为保证对比的公平性,仿真中保持与本文主实验完全一致的无人机纵向动力学模型、控制器结构、Kalman 滤波器参数、过程噪声与量测噪声协方差以及 χ^2 检测阈值,并采用相同的噪声实现序列,仅改变攻击注入方式。

仿真结果如图6所示,在重放攻击作用下,回放量

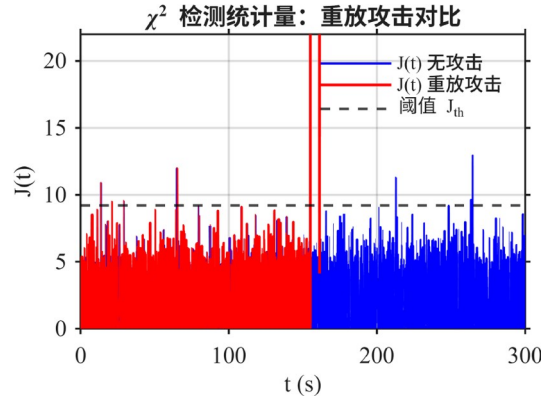


图 6 (网络版彩图)重放攻击下 χ^2 检测统计量 $J(t)$ 与阈值 J_{th} 比较

Figure 6 (Color online) Comparison of the χ^2 test statistic $J(t)$ and the threshold J_{th} under replay attack.

测与当前系统真实状态之间逐渐失配,残差信号显著增大,导致 χ^2 检测统计量 $J(t)$ 频繁超过阈值,其中超阈值样本占比达到48.32%。该结果表明,重放攻击在本文所采用的Kalman滤波器- χ^2 检测框架下无法满足前述定理所揭示的隐蔽性结构条件,因此不具备隐蔽性。相比之下,本文所提出的攻击正是基于上述定理所刻画的结构条件进行构造,能够在抑制残差响应的同时沿纵向不稳定模态持续驱动飞行状态偏离参考轨迹。

6 结论与讨论

本文针对无人机导航系统面临的欺骗攻击隐蔽性问题,从控制系统理论的角度出发,系统性地研究并设计了一种基于系统结构脆弱性的隐蔽导航欺骗攻击方法。通过分析无人机纵向动力学模型中存在的右半平面极点及其在Kalman滤波器中所诱导的非最小相位零点,本文提出了攻击信号的构造方法,确保其在通过 χ^2 异常检测器时具有统计意义上的隐蔽性。理论分析表明,所设计的攻击信号能够在不触发检测器报警的前提下,逐步引导无人机偏离预设飞行轨迹。特别地,本文利用灵敏度函数与补灵敏度函数在右半平面极点处的插值约束,严格证明了攻击信号在残差通道中的渐近衰减特性,从而保证了其在 χ^2 检测器下的隐蔽性。基于Aerosonde固定翼无人机的高保真仿真实验进一步验证了理论分析的正确性。仿真结果表明,在攻击作用下,无人机的纵向速度与高度均沿不稳定模态

方向逐渐发散, 而 χ^2 检测统计量仍保持在正常范围内, 未出现显著异常报警。这一结果不仅证实了所提攻击

策略的隐蔽性与有效性, 也揭示了现有基于残差的异常检测机制在面对结构性安全威胁时的局限性。

参考文献

- 1 Huang X. The small-drone revolution is coming—scientists need to ensure it will be safe. *Nature*, 2025, 637: 29–30
- 2 Chen M, Ma H X, Yong K N, et al. Safety flight control of UAV: A survey (in Chinese). *Robot*, 2023, 45: 345–366 [陈谋, 马浩翔, 雍可南, 等. 无人机安全飞行控制综述. *机器人*, 2023, 45: 345–366]
- 3 Pan Q, Guo Y, Lyu Y, et al. Autonomous safety and security of UAV systems: Definition, modeling, and gradation. *Sci Sin-Inf*, 2023, 53: 1608–1628
- 4 Kerns A J, Shepard D P, Bhatti J A, et al. Unmanned aircraft capture and control via GPS spoofing. *J Field Robotics*, 2014, 31: 617–636
- 5 Tippenhauer N O, Pöpper C, Rasmussen K B, et al. On the requirements for successful GPS spoofing attacks. In: *Proceedings of the 18th ACM Conference on Computer and Communications Security*. New York: ACM, 2011. 75–86
- 6 Broumandan A, Jafarnia-Jahromi A, Lachapelle G. Spoofing detection, classification and cancelation (SDCC) receiver architecture for a moving GNSS receiver. *GPS Solut*, 2015, 19: 475–487
- 7 Jafarnia-Jahromi A, Broumandan A, Nielsen J, et al. GPS vulnerability to spoofing threats and a review of antispoofing techniques. *Int J Navig Obs*, 2012, 2012: 1–16
- 8 Khanafseh S, Roshan N, Langel S, et al. GPS spoofing detection using raim with ins coupling. In: *Proceedings of 2014 IEEE/ION Position, Location and Navigation Symposium-PLANS 2014*. Piscataway: IEEE, 2014. 1232–1239
- 9 Zeng K C, Shu Y, Liu S, et al. A practical GPS location spoofing attack in road navigation scenario. In: *Proceedings of the 18th International Workshop on Mobile Computing Systems and Applications*. New York: ACM, 2017. 85–90
- 10 Horton E, Ranganathan P. Development of a GPS spoofing apparatus to attack a DJI Matrice 100 Quadcopter. *J Glob Position Syst*, 2018, 16: 9
- 11 Su J, He J, Cheng P, et al. A stealthy GPS spoofing strategy for manipulating the trajectory of an unmanned aerial vehicle. *IFAC-PapersOnLine*, 2016, 49: 291–296
- 12 Shi M, Mu J Y, Chen S X. Bias analysis of GPS/INS integrated navigation under GPS deception (in Chinese). *Electron Opt Control*, 2016, 23: 16–20 [史密, 牟京燕, 陈树新, 等. GPS诱骗下GPS/INS组合导航偏差分析. *电光与控制*, 2016, 23: 16–20]
- 13 Sandberg H. *Safety, Security and Privacy for Cyber-Physical Systems*. Cham: Springer, 2021. 61–78
- 14 Khazraei A, Meng H, Pajic M. Black-box stealthy GPS attacks on unmanned aerial vehicles. In: *Proceedings of 2024 IEEE 63rd Conference on Decision and Control (CDC)*. Piscataway: IEEE, 2024. 2857–2862
- 15 Zhang K, Keliris C, Parisini T, et al. Stealthy integrity attacks for a class of nonlinear cyber-physical systems. *IEEE Trans Automat Contr*, 2021, 67: 6723–6730
- 16 Hu L, Wang Z, Han Q L, et al. State estimation under false data injection attacks: Security analysis and system protection. *Automatica*, 2018, 87: 176–183
- 17 Guo Z, Shi D, Johansson K H, et al. Optimal linear cyber-attack on remote state estimation. *IEEE Trans Control Netw Syst*, 2016, 4: 4–13
- 18 Ding S X, Li L, Zhao D, et al. Application of the unified control and detection framework to detecting stealthy integrity cyber-attacks on feedback control systems. *Automatica*, 2022, 142: 110352
- 19 Zhou K, Doyle J, Glover K. *Robust and optimal control*. New York: Prentice Hall, 1996
- 20 Mo Y, Sinopoli B. Secure control against replay attacks. In: *Proceedings of 2009 47th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*. Piscataway: IEEE, 2009. 911–918

Stealthy navigation spoofing attack for unmanned aerial vehicles

ZHANG KangKang¹, JIANG Bin¹, ZHOU Qi², WANG Biao¹, ZHANG GenHan¹ & HUANG Jie²

¹ *Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China*

² *AVIC Xi'an Flight Automatic Control Research Institute, Xi'an 710076, China*

This paper investigates the stealthiness of navigation spoofing attacks against unmanned aerial vehicles (UAVs). The analysis builds on fundamental control-theoretic principles, including the cancellation between system right-half-plane (RHP) poles and the nonminimum-phase zeros of its observer, as well as the intrinsic blocking effect of nonminimum-phase zeros on exponentially divergent signals. Considering the inherent instability of the UAV longitudinal dynamics and the commonly used Kalman-filter-based χ^2 anomaly detector, we design the attack injection direction and the time-varying structure of the attack signal according to the nonminimum-phase zeros induced by the RHP poles of the longitudinal motion model. Rigorous theoretical analysis shows that the constructed attack is perfectly stealthy with respect to the χ^2 detector, while simultaneously driving the UAV's longitudinal motion to deviate severely from its nominal trajectory. Finally, simulation results based on an Aerosonde UAV validate the stealthiness and effectiveness of the proposed navigation spoofing strategy.

navigation spoofing attack, stealthy attack, unmanned aerial vehicles

doi: [10.1360/SST-2025-0363](https://doi.org/10.1360/SST-2025-0363)