计算机研究与发展
Journal of Computer Research and Development
DOI: 10.7544/issn1000-1239.202330451
60(10): 2291−2303, 2023

基于机器学习的无人机传感器攻击在线检测和恢复方法

孙　聪　曾荟铭　宋焕东　王运柏　张宗旭　马建峰
（西安电子科技大学网络与信息安全学院　西安　710071）
（suncong@xidian.edu.cn）

Machine Learning Based Runtime Detection and Recovery Method Against UAV Sensor Attacks

Sun Cong, Zeng Huiming, Song Huandong, Wang Yunbo, Zhang Zongxu, and Ma Jianfeng
（*School of Cyber Engineering*, *Xidian University*, *Xi'an* 710071）

Abstract　The sensor attacks towards the flight controller of unmanned aerial vehicle (UAV) induce the UAV to take false sensor signals or data and estimate fault system states, threatening the flight safety of UAVs. The state-of-the-art runtime sensor attack detection and recovery approaches have limited detection accuracy and lacked persistence on the recovery effect. The computational resource limit of the UAV hardware also impacts the accuracy of the detection model and the respective attack detection. We propose a runtime UAV sensor attack detection and recovery approach, called LDR, based on lightweight machine-learning models. We leverage the advantage of the machine-learning model's representation ability on nonlinear feedback control systems compared with the linear system models to build the machine-learning model for each UAV sensor and predict the system states corresponding to each sensor. We also propose a new attack detection algorithm to mitigate the short-time vibration of the prediction deviation to reduce the potential errors. We apply our approach to detect and recover the GPS sensor attacks and gyroscope attacks. The experimental results show that the performance overhead of our approach meets the flight controller's real-time requirements. Our approach is highly robust on normal flight tasks, and the prediction model is effective. The comparisons between our approach and related work demonstrate the effectiveness of our approach.

Key words　unmanned aerial vehicle (UAV); anomaly detection; sensor attack; machine learning; embedded software

摘　要　针对无人机（unmanned aerial vehicles, UAV）飞行控制系统的传感器注入攻击能够诱导无人机接受错误的传感器信号或数据，错误估计系统状态，从而威胁无人机的飞行安全. 当前针对无人机传感器注入攻击的在线检测和恢复方法存在检测精度不高、系统状态恢复缺乏持续性、控制模型精度及检测精度受无人机硬件算力限制的问题. 提出了一种基于轻量级机器学习模型的无人机传感器攻击在线检测和恢复方法（machine learning based runtime detection and recovery method against UAV sensor attacks, LDR），利用机器学习模型对非线性反馈控制系统的表征能力相比线性模型更强的特点，构建各传感器对应的预测模型，对不同传感器对应的无人机系统状态进行准确预测，结合提出的缓解预测误差短时振荡的攻击检测算法，对GPS传感器攻击和陀螺仪读数攻击进行有效的检测和系统状态恢复. 实验结果表明，所提方法的开销满足飞控系统的实时性要求，具有高可靠性和预测有效性，对典型攻击的在线检测和恢复效果相比现有工作更好.

收稿日期：2023-06-05；**修回日期**：2023-08-11
基金项目：国家自然科学基金项目（62272366）；陕西省重点研发计划项目（2023-YBGY-371）
This work was supported by the National Natural Science Foundation of China (62272366) and the Key Research and Development Program of Shaanxi Province (2023-YBGY-371).

关键词 无人机;异常检测;传感器攻击;机器学习;嵌入式软件

中图法分类号 TP309.1

无人机(unmanned aerial vehicle, UAV)的飞行依赖于传感器对环境的测量感知,以确定无人机所处的状态.准确地对系统状态做出估计是无人机系统可靠安全(safety)决策的前提[1],然而,无人机飞行控制系统的状态估计面临严重的传感器注入攻击威胁[2],攻击者通过干扰被感知的物理环境或者从物理上损害传感器等手段,误导无人机传感器接受恶意输入,估计出错误系统状态,从而使无人机控制器产生错误输出并导致飞行异常.与物理层拒绝功能的阻塞干扰(jamming)攻击[3]不同,传感器注入的目的是通过错误的信号或数据改变无人机传感器对环境的感知,以在控制系统层面改变无人机行为,故亦称为传感器欺骗.传感器注入攻击在诸多领域有着广泛应用,如针对植入式医疗设备的音频攻击[4]、对汽车防抱制动系统(antilock braking systems, ABS)的磁场注入[5]和对自动驾驶车辆的激光雷达数据欺骗[6]均说明此类攻击的有效性.

在传感器注入攻击检测和缓解方面,针对单一传感器数据特性(如GPS信号)的研究相对较多[7],而对不局限于特定数据/信号特性的通用传感器注入攻击缓解技术的研究则相对较少,一些现有方法还依赖于辅助传感器的正常工作[8]或要求增加特定硬件[9].特别地,如何基于无人系统的有限计算资源对传感器注入攻击进行准确地在线检测和缓解,仍是亟待解决的问题.在这方面,基于系统识别的攻击检测框架[10]和基于非线性物理不变量拟合的检测方案[11]通过在线检查所感知的物理状态是否与控制模型确定的预期状态一致来检测外部传感器攻击,检测效果因控制模型精度不同而存在差异.后续的恢复方法[12-13]对受攻击无人机的系统状态进行恢复,但由于无人机系统本身属于非线性系统,因此基于系统识别得到的线性模型恢复出的系统状态[12]的准确性有限,仅能提供无人机进入失效保护(failsafe)模式之前的短暂恢复,而基于机器学习的抗攻击前馈控制器[13]监控无人机的主控制器,在攻击下代替无人机主控制器恢复无人机,相比模型预测结果参与传感器融合的恢复机制[12]而言,这种前馈恢复机制缺乏稳定性和持续性.

本文的基本思想是利用机器学习模型对非线性系统的准确刻画能力,结合容忍预测误差短时振荡的攻击检测及恢复算法,在无人机飞行控制系统软件层面实现准确的传感器注入攻击检测和系统状态恢复.同时通过对轻量级机器学习模型的设计和选择,克服无人机计算资源对非线性系统模型的运行时开销的限制.具体地,本文提出的基于机器学习的无人机传感器攻击在线检测和恢复方法LDR建立了不同传感器相对应的轻量级机器学习预测模型,该模型可预测出对应传感器下一时刻的状态.飞控内嵌的LDR系统通过比对模型预测值和传感器测量值,准确检测并及时隔离受攻击的具体传感器,防止攻击者继续误导或破坏传感器,并使用机器学习模型的预测值替代传感器测量值参与无人机后续控制过程,使得无人机在受攻击后的一段时间内能够正常飞行.本文的主要贡献包括3个方面:

1) 提出的LDR利用轻量级机器学习预测模型对陀螺仪、加速度计、GPS、磁力计等多种传感器的注入攻击进行有效检测和传感器度量恢复.

2) 提出的LDR攻击检测及恢复算法利用误差超限计数阈值和恢复有效计数阈值容忍传感器模型预测误差振荡导致的误报,相比现有检测和恢复方法提升了传感器度量的恢复效果.

3) 在开源飞控系统ArduPilot 4.1.0上的实验说明了LDR在线检测和恢复的开销满足飞控系统运行时的要求,LDR系统在正常飞行下的误报满足飞行可靠性要求,LDR预测模型有效,LDR系统针对GPS传感器攻击和陀螺仪读数攻击的在线检测和恢复效果相比现有工作[12-13]更好.

1 相关工作

Nassi等人[14]将无人机系统所面临的攻击归纳为直接物理访问攻击(包括针对无人机固件的供应链攻击)、临近物理侧攻击(包括针对相机数据、陀螺仪/加速度计/罗盘等传感器数据、GPS信号的欺骗和抑制攻击)、无线信道攻击(包括网络边信道攻击、传统WiFi攻击).本文主要针对临近物理侧的传感器注入攻击进行检测和恢复,此类攻击利用的相关目标传感器包括GPS接收器、相机、加速度计、陀螺仪、磁力计等.

从控制模型理论分析和仿真的角度研究无人机系统错误数据注入攻击和检测的工作通常难以从系统安全的视角考虑具体控制系统软件和攻击在具体

系统上的可实现性，如将无人机抽象为线性非时变控制系统模型[15-16]，将隐蔽攻击序列（包括直接控制获取攻击和机载导航攻击[16]）均抽象为从理论上直接注入系统模型. 此外，还可以直接将传感器抽象为非线性系统并构建用于攻击检测的非线性模型结构[17].

而从系统安全的视角，典型 GPS 欺骗攻击[18-19]能够引入位置、导航和时间计算方面的错误，导致无人机偏离预定轨迹. 通过分析无人机飞控软件的 GPS 失效保护模式，能够给出针对不同类型无人机实施有效 GPS 欺骗的攻击策略[20]. 无人机的微机电系统（micro-electromechanical systems, MEMS）陀螺仪可在声音频段共振，这种声学干扰引起陀螺仪性能衰减，利用这种性能衰减在飞控软件中的传播可导致无人机坠毁[21]，类似的攻击还被应用在 MEMS 加速度计上[22]. 利用光线对光流传感器的输入进行欺骗攻击，能够控制无人机在定点悬停模式下的侧向速度[23]. 现有的攻击方案还考虑了无人机具备扩展卡尔曼滤波（extended Kalman filter, EKF）或控制不变量[10]等基于先验不变量的异常检测机制，如当前已实现的错误数据注入、人为延迟、飞行模式切换攻击[2]能够推断检测阈值并据此构造隐蔽的传感器攻击. 针对 ArduPilot 飞控系统的数据融合实施的错误数据注入能够绕过 EKF 异常检测机制操作磁力计读数，在无人机无法接收地面站或 GPS 信号时导致无人机偏航[24].

已有针对传感器攻击提出的多种防御方案[2,18-19,21-22,24]，然而这些方案或仅针对特定传感器，或对控制系统硬件和算力有很高要求. 在惯性测量单元（inertial measurement unit, IMU）受攻击产生故障时，现有容错方案[8]使用其余传感器估计的位置和航向信息来恢复受损的姿态状态，使无人机在没有 IMU 读数的情况下稳定飞行一定时长. 对 Lucas-Kanade 光流传感方法的传感器输入欺骗攻击（包括图像欺骗和激光欺骗等），随机采样一致性（random sample consensus, RANSAC）算法能够合成缓解攻击的传感器输出[23]. DeepSIM[25]通过比较本机航拍照片和预存卫星图片进行位置验证，实现了一种高成本、高鲁棒性的 GPS 欺骗检测. BlueBox[9]的跨层安全架构利用外部独立的软硬件计算单元进行异常检测和恢复，硬件冗余使得 BlueBox 具有相对于传统模型更强的恢复能力. 基于单分类器的入侵检测方法[26]利用多种单分类器（包括单类支持向量机、自动编码器和局部离群因子算法）进行异常检测，检测的精度较差，且未实现系统状态恢复.

对硬件算力的限制和对安全机制的通用性要求促使了面向多种传感器攻击的飞控内嵌的通用运行时检测和恢复机制的发展. 使用系统识别方法能够生成反映无人机物理特性、控制算法和外部物理定律的控制不变量模型[10]，控制不变量模型在运行时利用其前序预测结果与无人机当前目标状态预测出对传感器的当前期望值，若时间窗口内无人机传感器的测量值和期望值的差异大于阈值，则检测出外部攻击异常. 后续提出的系统恢复方案[12]利用这种控制不变量模型的物理状态预测值，为每个传感器设计一个软件传感器，软件传感器预测传感器测量值并替换潜在被攻击的实际传感器测量值，该方案对传感器测量值的恢复持续时间较短且对个别传感器类型的恢复效果有限. SAVIOR[11]使用非线性物理不变量拟合的无人机系统模型相比控制不变量线性模型更准确，但该方法尚不支持攻击恢复. PID-Piper[13]基于长短期记忆（long short term memory, LSTM）实现了一种抗攻击的前馈控制器，将 LSTM 模型控制器以 C++代码形式嵌入飞控，深度模型在线根据控制器输出的偏移量大小决定是否接管 PID 控制器，尽管无法判断传感器是否存在异常（即不存在一般意义的检测机制），PID-Piper 仍能够根据控制误差启动恢复，该方案的实际恢复稳定性和持续性不及文献 [12] 的攻击恢复方案. LDR 能够对计算资源受限的无人机及其开源飞控系统进行有效的在线攻击检测和恢复，达到优于文献 [12−13] 的检测和恢复效果. 方案特点对比如表 1 所示.

Table 1 Comparison on the Characteristics of Primary Attack Mitigation Schemes

表 1 主要攻击缓解方案特点对比

方案类型	模型类型		
	线性模型	非线性模型	机器学习模型
检测+恢复	SW-Sensor[12]		LDR（本文）
恢复			PID-Piper[13]
检测	控制不变量[10]	SAVIOR[11]	

2 LDR 检测和恢复方案设计

本节介绍 LDR 的具体方案. 方案保护的典型传感器包括 GPS、陀螺仪、加速度计和磁力计.

2.1 总体框架

考虑到 EKF 的传感器噪声矫正效果不利于攻击检测且传感器融合过程不利于攻击影响的隔离，LDR 选择在传感器测量值进入 EKF 传感器融合过程

之前插入 LDR 传感器预测模块及相应的恢复开关机制,插入预测模块的无人机飞控系统整体运行架构如图 1 所示. 由于不同传感器的测量值以一定的顺序接入 EKF 传感器融合过程,因此图 1 中虚线内部分实际上在传感器融合过程中存在多个实例,每个实例对应于 1 个传感器,其中的 LDR 传感器预测模块对不同的传感器使用不同的预测模型(具体见 2.2 节).

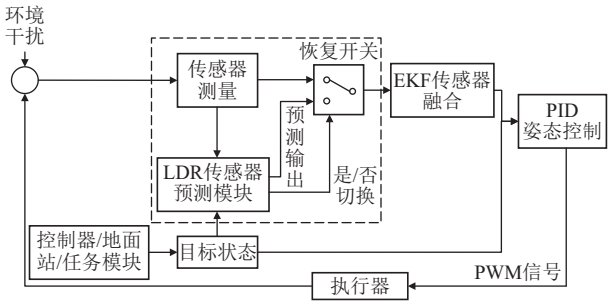


Fig. 1 Architecture of LDR embedded in UAV flight controller system

图 1 无人机飞控系统中内嵌的 LDR 系统架构

原始飞控系统的多个传感器的测量值在融合后会与系统目标状态一起输入控制器. 引入 LDR 传感器预测模块后,该模块依据目标状态实时运行,并使用检测算法(具体见 2.3 节)检测各传感器状态是否受到攻击,当检测到传感器攻击时,开启恢复开关,隔离被攻击的传感器;同时进入恢复状态,用 LDR 传感器预测模块对传感器读数的预测值替代被攻击传感器的测量值用于 EKF 传感器融合. 未被攻击的传感器则继续工作. 如受攻击传感器的测量值与对应的 LDR 传感器预测模块输出的累积误差在特定时间窗口内小于特定恢复阈值,则认为攻击已停止,关闭恢复开关,无人机继续使用正常的传感器测量值进行飞行控制.

LDR 传感器预测模块的内部构造如图 2 所示. 其中,机器学习模型将前一时刻该机器学习模型的预测值和无人机系统的目标状态值作为输入,迭代输出当前时刻的预测值. 由于每个机器学习模型对应于一个特定的无人机状态变量(具体见 2.2 节),而状态变量可能不能与真实传感器测量值直接比较(如表 2 中加速度计传感器预测模型预测的速度矢量不能与测量出的加速度直接比较),因此对于机器学习模型的预测输出,先通过适当转换处理,生成当前时刻 LDR 传感器预测模块对传感器的预测输出;对于无需转换处理的模型预测输出,直接作为传感器预测输出使用. 在攻击检测时(见 2.3 节),将传感器预测输出与真实传感器测量值进行比对. 当 1 个检测窗口时间内,传感器测量值与对应的传感器预测输出的累积误差多次超过相应的误差阈值(不同传感器误差阈值不同),则检测到攻击存在,触发恢复开关开启信号,由传感器的预测输出代替测量值参与后续传感器的融合和控制流程.

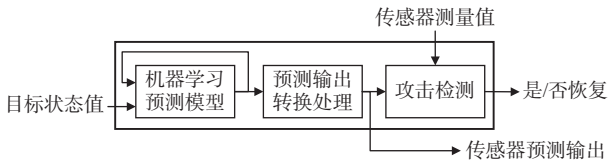


Fig. 2 LDR sensor prediction module

图 2 LDR 传感器预测模块

Table 2 Sensor's Prediction Model and Corresponding System State Variables and Prediction Output

表 2 传感器预测模型和对应的系统状态变量及预测输出

传感器	无人机状态变量	目标状态值	预测输出转换	传感器预测输出
陀螺仪	角速度矢量 $\{\omega_x, \omega_y, \omega_z\}$	目标角速度矢量		角速度矢量
加速度计	速度矢量 $\{v_x, v_y, v_z\}$	目标速度矢量	速度→加速度	加速度矢量
GPS	位置矢量 $\{p_x, p_y, p_z\}$	目标位置矢量		位置矢量
磁力计	偏航角ψ	目标偏航角		偏航角

2.2 预测模型构建

由于本文的目标是构建可内嵌于飞控的在线检测和恢复机制,因此对机器学习模型有严格的效率要求. 本文使用简单神经网络模型(包括单层感知机和多层感知机)训练各个传感器所需的预测模型,解决无人机传感器输出的时间序列预测问题.

本文针对四旋翼无人机的 10 个状态变量分别构建机器学习预测模型,陀螺仪、加速度计、GPS、磁力计分别使用这些模型进行预测. 状态变量与使用该变量的传感器的对应关系如表 2 所示. 在状态变量集合$\{p_x, p_y, p_z, \psi, \omega_x, \omega_y, \omega_z, v_x, v_y, v_z\}$中,每一种状态变量在任一时刻的目标状态值都能够在无人机飞行时从 PID 姿态控制器获取. 特别是飞控系统中无法直接获得加速度的目标状态值,因而,LDR 加速度计预测模块对无人机加速度的预测需要先使用机器学习模型预测速度,再将每一时刻的预测速度矢量在线转换处理为预测加速度矢量,用于与加速度计的测量值进行比较. 而对于磁力计,飞控系统亦无法获得磁力矢量的目标状态值,因而 LDR 磁力计预测模块使用机器学习模型预测偏航角(yaw),记作ψ. 但与 LDR 加速度计预测模块的预测输出转换(从速度预

测值转换为加速度预测值)不同, LDR 磁力计预测模块直接使用预测出的偏航角执行攻击检测. 磁场测量值向偏航角测量值的转换基于公式[27]:

$$\psi = \arctan\left(-\frac{m_y\cdot\cos\phi - m_z\cdot\sin\phi}{m_x\cdot\cos\theta + m_y\cdot\sin\theta\cdot\sin\phi + m_z\cdot\sin\theta\cdot\cos\phi}\right),$$

其中, m_x、m_y、m_z分别为机体坐标系沿x、y、z轴的磁场测量值, ϕ和θ分别为翻滚角(roll)和俯仰角(pitch)的测量值. 对于磁力计受攻击情况下的恢复, 由于无人机磁力计度量的作用是矫正姿态四元数, LDR 直接将预测得到的偏航角引入 EKF 传感器融合过程以实现对姿态的矫正, 而不再将预测偏航角转化为磁力计读数的预测值.

模型的训练过程使用无人机正常飞行过程中的目标状态值和测量值数据进行. 具体地, 使用状态变量当前时刻的测量值和无人机目标状态值作为输入特征, 使用状态变量下一时刻的测量值作为输出特征, 以使模型学习到正常飞行时状态变量测量值的时序特征. 对于不同机器学习预测模型, 需要收集不同的状态变量测量值和目标状态值的时间序列数据, 作为预测模型训练所使用的输入特征和输出特征. 因此, 我们在无人机正常(仿真)飞行过程中收集状态变量测量值和目标状态值的时间序列数据, 然后应用具体机器学习预测模型的训练过程(使用的神经网络结构见 3.1 节). 特别地, 为训练 LDR 加速度计预测模块所使用的速度预测模型, 需要获得速度测量值的时间序列, 本文从控制器内部直接获取速度测量值序列用于预测模型的训练. 为训练 LDR 磁力计预测模块所使用的偏航角预测模型, 将磁力矢量的测量值序列转化为偏航角测量值序列, 用于预测模型训练.

本文的机器学习模型与飞控系统中的 EKF 都是基于前一时刻估计量进行下一时刻状态估计, 但飞控系统的 EKF 实现需要 IMU 传感器的测量值方可执行状态估计, 而本文机器学习模型在完成初始状态设置后即可独立运行, 无需传感器提供输入. 当特定传感器不可用时, 本文机器学习模型可作为替换, 维持 EKF 的正常运行.

2.3 检测及恢复算法

图 1 所示 LDR 传感器预测模块及恢复开关的运行时功能可由算法 1 描述. 算法 1 在传感器的每个采样周期上的输出是由本文 LDR 检测和恢复机制处理后的传感器读数的参考值, 该值在攻击未检出时即为传感器的真实测量值, 而在攻击检出时改为使用恢复机制提供的预测模型输出值. 算法接受当前时刻的传感器目标状态值、传感器测量值以及上一时刻机器学习预测模型的预测值作为输入, 首先获得机器学习预测模型当前时刻的预测值, 并转换为 LDR 传感器预测模块在当前时刻对传感器的预测输出 $pred_i$. $WinTH$ 表示检测窗口阈值, 即检测窗口包含的时间片数量. 如果当前时刻是一个检查点(新检测窗口开始), 重置当前检测窗口内的时间片计数i、误差计数$errCnt$、测量值与预测值的累积误差 $errSum$, 并判断恢复模式是否已启动($recovSig$是否为 true). 若未启动, 则使用当前传感器测量值$sens_i$重置预测输出 $pred_0$, 这样在下一轮可以校准预测模型的输出. 此后, 计算预测输出与传感器测量值的均方误差并计入累积误差 $errSum$ 中, 进而得出当前检测窗内的平均累计误差err. 设计误差阈值 $ErrTH$ 和误差超限计数阈值 $ErrCntTH$, 当检查到平均累计误差err连续大于设定的误差阈值 $ErrTH$ 的次数超过 $ErrCntTH$ 次时, 认为无人机受到了传感器攻击, 开启恢复模式并发出受到传感器攻击的警报. 在恢复模式下($recovSig$为 true), 实际传感器的测量值$sens_i$被替换为传感器的预测输出 $pred_i$. 设计恢复阈值 $RecovTH$ 和恢复有效计数阈值 $RecovCntTH$, 当累积误差连续小于设定的恢复阈值 $RecovTH$ 的次数超过 $RecovCntTH$ 次时, 则认为攻击已结束, 关闭恢复模式, 无人机将继续使用真实传感器的值.

算法 1. 攻击检测及恢复算法

输入: 当前时刻i的传感器目标状态tgt_i, 传感器测量值$sens_i$, 上一时刻机器学习预测模型的预测值$pred_{i-1}$;

输出: 每一个传感器采样周期传感器读数的参考值$sens_i$.

① $recovSig \leftarrow$ false, $errCnt \leftarrow 0$, $errSum \leftarrow 0$, $recovCnt \leftarrow 0$, $i \leftarrow 0$; /*初始化*/

② procedure DetectRecovery($tgt_i, sens_i, pred_{i-1}$); /*获取并处理预测结果*/

③ $raw_i \leftarrow prediction(pred_{i-1}, tgt_i)$;

④ $pred_i \leftarrow convert(raw_i)$;

⑤ if $i \geqslant WinTH$ then

⑥ if !$recovSig$ then

⑦ $pred_0 \leftarrow sens_i$;

⑧ end if

⑨ $tgt_0 \leftarrow tgt_i$, $sens_0 \leftarrow sens_i$;

⑩ $errCnt \leftarrow 0$, $errSum \leftarrow 0$;

⑪ $i \leftarrow 0$;

⑫ end if

⑬ $errSum \leftarrow errSum + (pred_i - sens_i)^2$

⑭ $err \leftarrow errSum/i$;

⑮ if $err > ErrTH$ then /*判断恢复是否启动*/

⑯ $errCnt++$;

⑰ end if

⑱ if $errCnt > ErrCntTH$ then

⑲ $recovSig \leftarrow$ true;

⑳ $recovCnt \leftarrow 0$;

㉑ $attackAlert()$; /*攻击报警*/

㉒ end if

㉓ if $recovSig$ then

㉔ $sens_i \leftarrow pred_i$; /*执行恢复操作*/

㉕ if $errSum < RecovTH$ then

㉖ $recovCnt++$;

㉗ end if

㉘ if $recovCnt > RecovCntTH$ then

㉙ $recovSig \leftarrow$ false; /*恢复关闭*/

㉚ end if

㉛ end if

㉜ $i++$;

㉝ end procedure.

特别地, 算法 1 的启动需要初始预测值 $pred_{-1}$参与; 在现实中, 使用无人机未受攻击的状态下的一个特定时刻传感器测量值作为初始 $pred_{-1}$. 算法 1 的复杂度在单个时间片内由行③④的预测过程和转换过程决定, 转换过程相比预测过程更为简单. 除这 2 个过程外, 其余部分复杂度为$O(1)$. 因此, 在实现中选择高效的机器学习预测模型尤为重要(见第 3.1 节). 相比于文献 [12−13] 的算法, 算法①由于引入了误差超限计数阈值 $ErrCntTH$ 和恢复有效计数阈值 $RecovCntTH$, 使得算法①能够更好地应对急转等预测振荡情况, 防止由于短时的预测误差振荡所导致的误报, 第 3.2 节攻击恢复效果实验显示本文 LDR 攻击检测和恢复方法在恢复持续时间上有优势.

3 实现与评价

3.1 LDR 方案实现

1) 机器学习模型结构及训练

本文使用无人机执行 20 次飞行任务的日志, 在 Keras 框架下训练本文的机器学习预测模型. 飞行任务为无人机在多个随机的位点进行起飞、降落、转弯等机动操作. 数据采样频率为 400 Hz 时, 所有任务的数据量约为 70 万条, 每一条数据包括所有传感器所需收集的信息. 训练数据以覆盖无人机在各种飞行模式和典型环境下的姿态特征为核心要求. 在训练集与测试集数据量比例为 7∶3 下, 对于表 2 中每个无人机状态变量所对应的机器学习模型, 单个模型从模型的训练到模型的测试完成 1 次所需时间平均仅约 30 s. 由于模型训练所需资源较少, 因而本文使用一个自动化程序来遍历搜索不同的模型参数的组合, 模型参数包括每层神经元数量、神经网络层数、批次大小(batch size)等. 在每一个参数组合下自动训练、测试机器学习模型, 从而找到适合不同传感器的神经网络结构. 最终得到的每个无人机状态变量对应的机器学习预测模型结构如表 3 所示, 所有模型均使用 Adam 优化器, 损失函数选择均方差(mean square error, MSE)损失, 激活函数选择 ReLU.

Table 3 UAV State Variables and Corresponding Structures of Machine Learning Prediction Models

表 3 无人机状态变量和对应的机器学习预测模型结构

状态变量		神经网络层数	每层神经元个数			1 次训练样本数
			第一层	第二层	第三层	
角速度	ω_x	2	2	1		1 024
	ω_y	2	2	1		1 024
	ω_z	2	4	1		128
速度	v_x	2	2	1		256
	v_y	2	2	1		256
	v_z	3	4	2	1	256
位置	p_x	2	2	1		256
	p_y	2	4	1		256
	p_z	2	2	1		512
偏航角	ψ	3	2	2	1	256

2) 加速度预测的去噪

为检测加速度计攻击和恢复加速度状态而引入的预测输出“速度→加速度”转换(见表 2), 要求将每一时刻的预测速度矢量$v(t)$在线转换处理为预测加速度矢量$a(t)$, 转换方式是求解采样时间间隔内的平均加速度, 即$a(t) = \Delta v^t_{t-\Delta t}/\Delta t$. 计算得到的加速度会包含大量高频噪声, 从而使其在与真实传感器测量值直接比较时会有大量的错误警报. 本文使用一阶低通数字滤波器[28]对预测输出转换得到的加速度进行过滤, 衰减高频频率使得最后得到的加速度变化更加平滑. 具体地, 滤波后加速度的输出值Y定义为

$$Y(t) = \alpha a(t) + (1-\alpha)Y(t-1),$$

$$\alpha = \mathrm{T_s}/\left(T_s + \frac{1}{2\pi f_c}\right),$$

其中，a为通过加速度公式直接计算的加速度，f_c为低通滤波器的截止频率，T_s为采样周期.

3）系统参数选择

算法 1 所述攻击检测与恢复算法的有效运行依赖于合适的检测窗口阈值 *WinTH*、误差阈值 *ErrTH*、恢复阈值 *RecovTH*、误差超限计数阈值 *ErrCntTH* 和恢复有效计数阈值 *RecovCntTH*. 在飞控运行过程中，相对于传感器测量值的实际变化，模型预测的变化趋势可能存在超前或滞后. 因此，本文采用动态时间规整算法[29]，从正常飞行数据集中计算出最大时间位移，计算模型预测值序列和测量值数据序列的最佳对齐方式，并将该时间位移的长度作为检测窗口阈值 *WinTH*. 确认了检测窗口阈值 *WinTH* 后，可从检测窗口观察到预测模型输出与真实传感器测量值之间的最大误差，从而计算出误差阈值 *ErrTH*. 误差阈值 *ErrTH* 应尽可能小，以规避漏报，同时要略大于所有正常飞行数据中观测到的最大均方误差 *MaxError*，从而容忍突然的风力增加等外部因素引起的一些意外误差，减少误报的可能性. 由于攻击者对无人机传感器发起攻击引起的外部误差远大于外部因素引起的暂时性误差，并且攻击者无法生成与无人机飞行时目标状态紧密相关的恶意信号序列，本文进一步设置恢复阈值 *RecovTH*，且有 $MaxError < RecovTH \leqslant ErrTH$. 当传感器真实值与预测输出的差值在一个检测窗口内多次处于恢复阈值之下时，可认为攻击已停止. 在获得检查窗口阈值 *WinTH* 和误差阈值 *ErrTH* 后，通过实验观测在实际飞行时，1 个检测窗口时间内有可能的真实传感器检测值与预测模型输出的差值超过误差阈值 *ErrTH* 的次数，将误差超限计数阈值 *ErrCntTH* 设置为大于这个次数值. 在获得检查窗口阈值 *WinTH* 和恢复阈值 *RecovTH* 后，通过实验观测从传感器注入攻击停止时起，1 个检测窗口时间内有可能的真实传感器检测值与预测模型输出的差值超过恢复阈值的次数，将恢复有效计数阈值 *RecovCntTH* 设置为大于这个次数值.

4）模型加载与插入位置

由于本文实验所使用的 ArduPilot 由 C++编写，因此本文使用的基于 C++的开源机器学习实现框架 frugally-deep[30] 运行适用于飞控性能约束的机器学习预测模型. frugally-deep 能快速、高效运行深度神经网络，可以加载 Keras 训练好的预测模型，并提供了轻量级的推理和预测功能；可以在资源受限的环境中使用，保证模型在无人机上运行时预测效率不影响正常飞行，达到预期的在线检测和恢复效果.

将每个传感器上的攻击检测和恢复算法实现为具体函数模块，将传感器对应的 LDR 预测和恢复模块插入该传感器测量的对应函数中. 其中，将 GPS 对应的位置矢量预测和恢复模块插入函数 *NavEKF2_core*::*readGpsData*()中；将磁力计对应的偏航角预测和恢复模块插入函数 *NavEKF2_core*::*SelectMagFusion*()中；将陀螺仪对应的角速度矢量预测和恢复模块、加速度计对应的加速度矢量预测和恢复模块均插入函数 *NavEKF2_core*::*readIMUData*()中.

3.2 实验评估

本节首先介绍评估 LDR 系统的实验设置，然后评估 LDR 系统的运行效率、正常飞行下可靠性、预测模型的有效性对 2 种公开攻击（GPS 传感器攻击和陀螺仪读数攻击）的恢复效果及优势.

1）实验设置与攻击设置

本文使用 2 个四旋翼无人机系统评估实现的 LDR 系统. 其中，ArduPilot Mega SITL 为软件在环仿真环境，真实无人机则使用雷迅 V5+作为飞控硬件. 表 4 列出了本文所使用的无人机的控制软件版本及各类传感器数量. 仿真环境的主机配置为 Intel Core™i5-11 400@2.60 GHz CPU, 6 GB RAM. 真实飞控硬件配置包括 ARM Cortex-M7 处理器（时钟频率 216 MHz），512 KB RAM，以及 2 MB 用以存储飞控二进制文件的闪存. 表 5 列出了真实无人机传感器的具体配置，无人机与地面站通信频率为 840~845 MHz，数据传输速率为 345 Kbps.

由于真实传感器攻击需要特殊攻击设备，难以在实验环境下直接实施，因而本文沿用当前主流的攻击模拟方式[12-13]，使用软件实现的攻击模块模拟了传感器受到攻击的效果，并将攻击模块直接插入飞控代码中. 具体地，在各类型传感器代码中添加一段恶意攻击代码，该段攻击代码在无人机运行时可以修改传感器的测量值，以模仿传感器实际受到攻击时的传感器读数效果. 为使得传感器攻击能受控生

Table 4 UAV Types and Number of Sensors for Evaluations

表 4 评估用无人机类型及传感器数量

飞控硬件	控制软件	传感器数量			
		GPS	陀螺仪	加速度计	磁力计
ArduPilot Mega SITL	ArduCopter 4.1.0	1	2	2	1
雷迅 V5+	ArduCopter 4.1.0	1	3	3	1

Table 5 Sensor Configuration of Real UAV

表 5 真实无人机的传感器配置

传感器	型号	传感器数量
GPS	Neo V2	1
IMU（每单元含 1 个加速度计和 1 个陀螺仪）	ICM20602	1
	ICM20689	1
	BMI055	1
磁力计	IST8310	1

效, 使用 MAVLink 命令从地面站远程开启和关闭攻击. 本文所设置的攻击来自文献 [12−13], 攻击包括: GPS 传感器攻击, 可以让无人机偏离原定航线; 陀螺仪读数攻击, 会使得无人机坠毁.

2) LDR 检测与恢复开销

本节比较添加 LDR 系统之前和之后的飞控主循环的每一次迭代运行时间, 以评估时间开销, 所有时间开销在仿真环境下测得. 具体地, 首先测量原始飞控软件运行 1 次主循环的时间开销; 然后以此为基准, 依次插入每个传感器对应的 LDR 检测和恢复模块, 包括运行代码所依赖的库; 随后分别测量主循环运行 1 次的时间开销; 最后, 将所有的传感器对应的 LDR 检测和恢复模块同时插入测量总时间开销.

图 3 为同一飞行任务上, 飞控系统在未插入任何传感器的 LDR 检测和恢复机制时(图 3(a))、插入单一类型传感器的 LDR 检测和恢复模块时(图 3(b)~(e)), 以及插入全部传感器的 LDR 检测和恢复模块时(图 3(f)), 其主控制循环的时间开销比较. 纵轴为每次主循环运行的时间开销. 在 ArduCopter 中, 原始飞控软件的系统循环执行频率为 400 Hz, 调度程序在每个执行周期(2.5 ms)内执行 1 次控制功能, 并使用执行周期内的剩余时间调度辅助任务. 由于飞控软件对不同传感器的采样频率不同(如对磁力计的采样频率常为 100 Hz), 不同的 LDR 检测和恢复模块也需分别运行在相应频率上, 而陀螺仪和加速度计的运行频率高(400 Hz), 因而导致对应的 LDR 模块的时间开销最高. 经实验测量, 原始飞控软件运行 1 次主循环的平均时间开销为 0.026 ms, 向所有传感器插入 LDR 系统后的飞控软件运行 1 次主循环的平均时间开销为 0.180 ms. 虽然主循环平均时间开销有明显增长, 但由于主循环平均时间开销相比执行周期(2.5 ms)仍仅占较小比例, 且峰值时间开销也在 2.5 ms 以内, 因而添加 LDR 系统后, 所有控制功能及辅助任务均能在执行周期内完成, 因此添加 LDR 系统导致的时间开销增长可接受, 不影响无人机正常飞行操作.

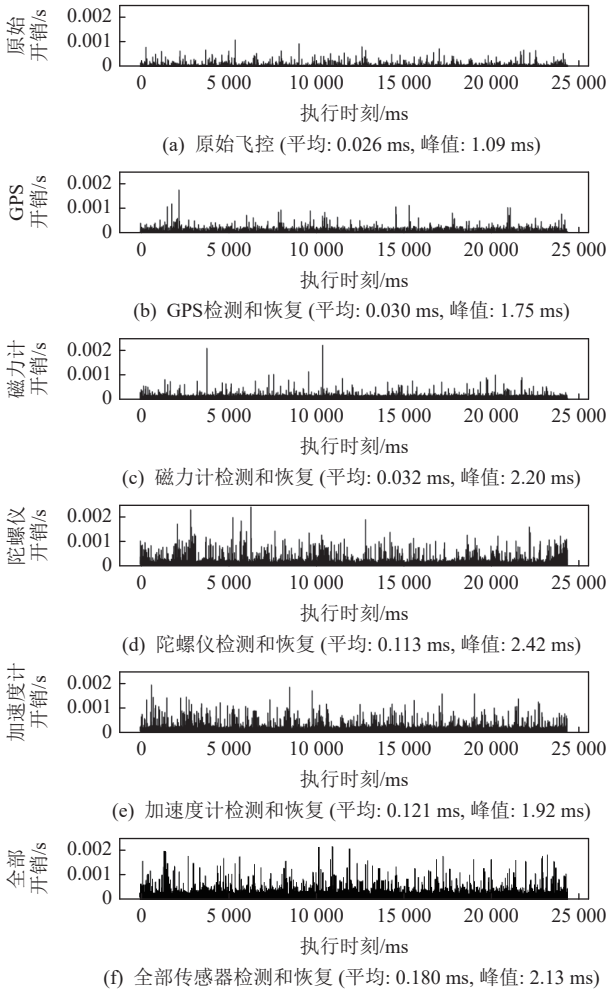


Fig. 3 Runtime cost of the main control loop before and after LDR module is inserted into the flight controller system

图 3 飞控系统在插入 LDR 模块前后的主控制循环的运行时间开销比较

本文还比较了添加 LDR 系统前后 ArduCopter 进程运行时的内存消耗峰值, 以评估空间开销. 在仿真环境下, 通过记录 20 次飞行任务过程中测量的内存消耗峰值, 发现添加 LDR 系统后, 内存消耗仅增长 7.25%, 可见 LDR 的检测和恢复机制对飞控运行时的内存消耗影响非常小.

由于本文方案和 PID-Piper 均使用神经网络模型进行预测, 且模型运算是方案的主要开销, 因此我们从浮点运算数(floating-point operand, FLOP)指标出发, 比较这 2 种方案的机器学习模型计算开销. FLOP 的大小取决于模型结构内部的连接数量. 每条连接均需执行一次加法运算和一次乘法运算, 因此, 模型的浮点运算数是连接数量的倍增. PID-Piper 仅为计算 3 个姿态角, 即翻滚角、俯仰角和偏航角, 就部署了 3 个结构相同的神经网络模型. 这些模型的层数和神

经元数量均多于本文使用的模型，其总浮点运算数达到约 50 000. 相比之下，本文模型不仅层数更少，涵盖的状态数量更多，且所有模型的浮点运算数总和仅有 120，远低于 PID-Piper 的计算开销. 由于计算时延与网络层数和浮点运算数正相关，因此，本文模型相比 PID-Piper 的机器学习模型是更轻量级的，具有更低的计算开销和时延.

3）正常飞行下的可靠性和预测有效性

本文测试了在没有攻击的情况下实际飞行时 LDR 的运行情况，以说明 LDR 检测和恢复机制在没有攻击下的可靠性. 本文随机选择了 10 个飞行任务，与机器学习模型训练用任务不同，用于检验可靠性的任务动作包括起飞、降落、转弯等，飞行模式设置为 auto 模式，每个任务时间为 3 min，所有任务的总时间为 30 min. 测试结果发现，这 10 个任务中有 2 个任务激活了 LDR 检测和恢复系统，这 2 个任务均激活了陀螺仪传感器 LDR 检测和恢复机制，即出现了检测误报. LDR 检测和恢复功能激活后，使得任务失败的次数为 0，在 2 次出现误报的任务中，无人机飞行平稳后 LDR 系统的警报都能自动关闭.

进一步地，在仿真环境下验证无人机在一个随机的测试飞行任务过程中，无人机 LDR 预测的传感器读数与真实传感器的测量值的吻合程度，以说明 LDR 的机器学习模型预测的有效性. 如图 4 所示，模型的预测结果与真实传感器的测量结果基本吻合，磁力计对应的偏航角的预测值与真实测量值的抖动是计数方式上产生的 0°与 359°之间的微小偏航角变化，在物理上不存在无人机偏航角的大幅度变化.

4）LDR 对公开攻击的检测和恢复效果

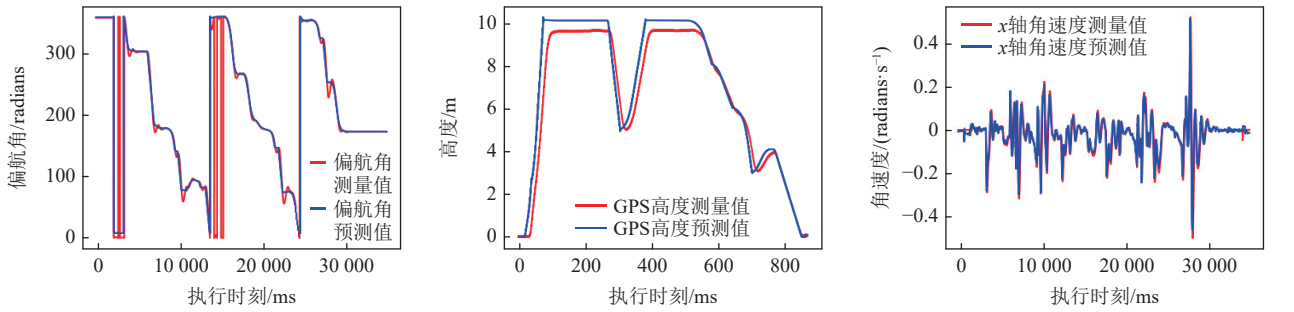
为了测试 LDR 在检测公开攻击和从公开攻击中恢复飞控状态的有效性，本文首先在仿真环境下针对陀螺仪和 GPS 分别发起攻击，测量了在攻击发起后 LDR 对攻击的检测用时（time to detection, TTD）和恢复效果；然后在真实无人机上测试 LDR 系统对 GPS 攻击的恢复效果. 检测用时的计算方法为：

$$TTD = t_{\text{detect}} - t_{\text{attack}},$$

其中，t_{detect}为 LDR 系统首次报告检测出攻击的时刻，t_{attack}为攻击实际发起的时刻.

本文 GPS 攻击实验通过对 GPS 测量的位置信息注入偏差来达到攻击的目的，攻击在无人机飞行途中发起，通过攻击代码缓慢地对 GPS 注入攻击偏移，无人机的降落点将会偏离计划航点约 55 m. 针对这一攻击，LDR 系统的平均检测用时为 0.88 ms. 图 5（a）三维图给出了无人机在未受攻击情况下的行进路线、无人机从特定点开始受到持续 GPS 攻击的行进路线，以及 LDR 系统生效的无人机在受 GPS 攻击后的行进路线. 相应地，图 5（b）为无人机 GPS 传感器在未受攻击、受攻击、受攻击且 LDR 系统生效这 3 种情况下，位置信息测量值的 y 轴变化差异；图 5（c）为受攻击、受攻击且 LDR 系统生效 2 种情况下，GPS 传感器测量值（或 LDR 对 GPS 的预测值）相比未受攻击时的 GPS 测量值的偏移量比较.

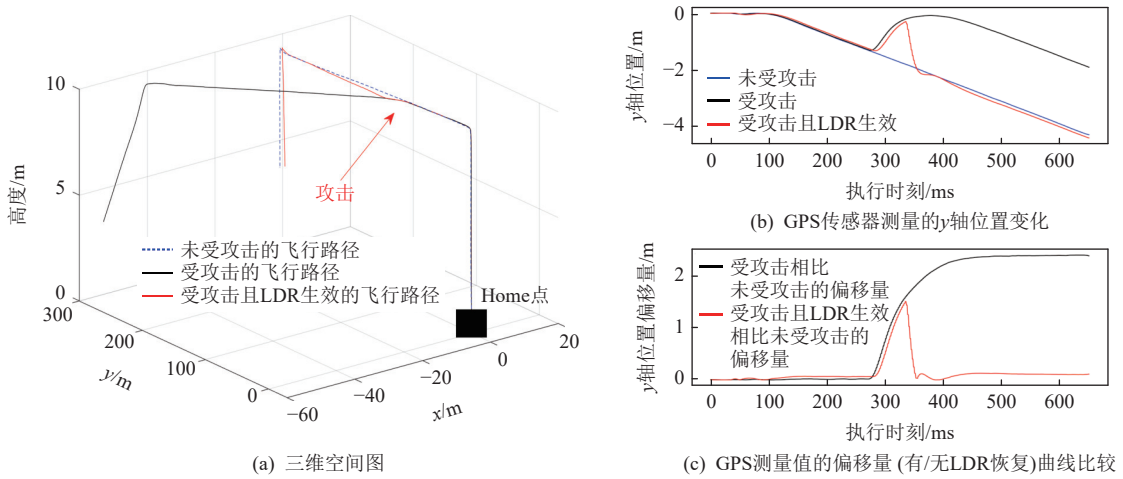
本文陀螺仪读数攻击实验在无人机飞行途中对无人机的陀螺仪读数进行注入. 图 6（a）三维图给出了无人机在未受攻击情况下的行进路线、无人机从特定点开始受到陀螺仪读数攻击的行进路线，以及 LDR 系统生效的无人机在受到陀螺仪读数攻击后的行进路线. 针对这一攻击，LDR 系统的平均检测用时为 1.24 ms. 可见在 LDR 系统未生效的情况下，无人机受到攻击后很快坠毁；而在 LDR 系统的恢复下，无人机还可正常运行约 5.1 s，此时长即为有效恢复持续时间. 尽管 LDR 系统成功阻止了传感器攻击，防止了无人机立即坠毁，但由于预测误差的原因，LDR 系统无法永久或长期替换物理传感器，因此需要在有效恢复持续时间内使用其他控制信道接管无人机. 图 6（b）为无人机姿态翻滚角变化曲线，可见攻击注



(a) 偏航角Ψ的真实传感器测量值与模型预测值的吻合程度　(b) GPS高度p_z的真实传感器测量值与模型预测值的吻合程度　(c) 陀螺仪角速度ω_x的真实传感器测量值与模型预测值的吻合程度

Fig. 4　Effectiveness of model prediction of machine learning in LDR system

图 4　LDR 系统的机器学习模型预测的有效性



(a) 三维空间图 (b) GPS传感器测量的y轴位置变化 (c) GPS测量值的偏移量 (有/无LDR恢复)曲线比较

Fig. 5 Recovery effect of LDR system under GPS sensor attack

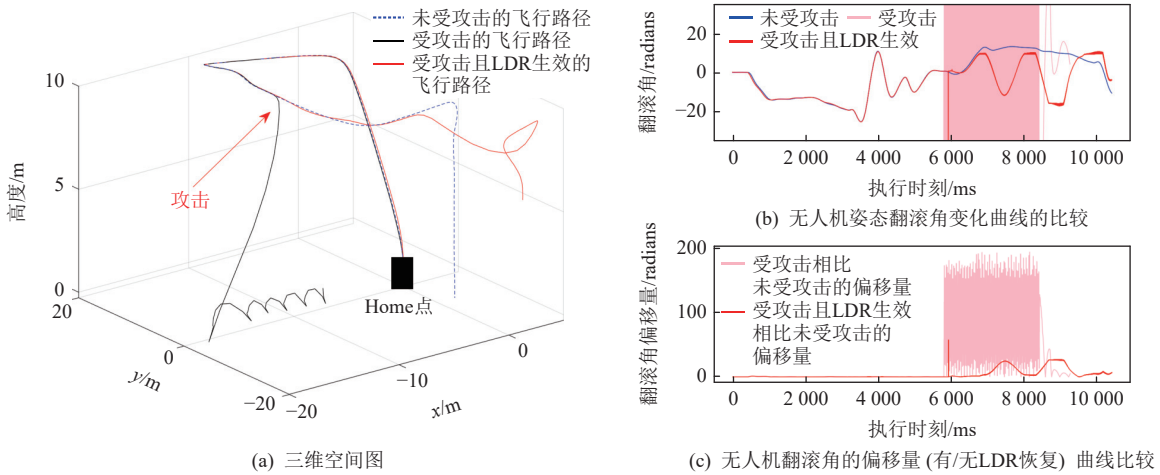
图 5 LDR 系统在 GPS 传感器攻击下的恢复效果

入会使无人机翻滚角发生高频变化, 从而导致无人机坠毁, 而 LDR 系统生效的无人机的翻滚角变化相比无攻击情况下的无人机翻滚角相差不大. 图 6(c)为受攻击、受攻击且 LDR 系统生效 2 种情况下无人机翻滚角相比未受攻击时的翻滚角的偏移量曲线比较, 可见引入 LDR 系统使得翻滚角偏移量显著减小.

本文在真实无人机上测试 LDR 的恢复效果. 虽然 LDR 恢复机制能在陀螺仪读数攻击下延缓无人机失控, 但使用地面站对攻击生效后的无人机进行控制接管仍存在一定概率失败, 因此在真实无人机上本文仅进行 GPS 传感器攻击的注入. 本文设计一个距离为 13.51 m 的直线折返飞行任务, 即无攻击情况下无人机起飞后沿该路线折返 2 次后回到起飞位置. 我们在无人机第 1 次开始折返时, 给无人机注入(0.05~0.15)m/20 ms 的 GPS 传感器攻击, 测得无人机完成飞行任务时距离起飞点的距离为 4.37 m. 在同样的攻击下, 在起飞后第 1 次开始折返时开启 LDR 系统, 无人机完成飞行任务时距离起飞点的距离为 0.89 m. 实验说明 LDR 检测系统在实际无人机飞行任务上有效.

5) LDR 与其他传感器攻击恢复方案的比较

以下对比 LDR 与其他无人机传感器攻击在线恢复方案, 包括软件传感器 SW-Sensor[12]、PID-Piper[13]的恢复效果差异. 由于文献 [10−11] 仅支持检测而不支持对传感器测量值和无人机状态的恢复, 因此本文不与文献 [10−11] 比较. 由于文献 [12] 未开源实现, 本文尽最大努力使用 Matlab 的系统识别工具对该方案进行了复现, 并使用训练数据推导出模型, 使用测试数据验证其模型的准确性. PID-Piper 提供了在 ArduCopter 3.7.0 上的开源实现, 本文使用该公开版本



(a) 三维空间图 (b) 无人机姿态翻滚角变化曲线的比较 (c) 无人机翻滚角的偏移量 (有/无LDR恢复) 曲线比较

Fig. 6 Recovery effect of LDR system under gyroscope reading attack

图 6 LDR 系统在陀螺仪读数攻击下的恢复效果

进行对比试验，进行相同的攻击实现、攻击测试并记录下相同的传感器数值变化.

实验结果显示，SW-Sensor[12]、PID-Piper[13]和LDR都能够对GPS传感器攻击和陀螺仪读数攻击做出响应. 在对受攻击的无人机进行恢复方面，图7为GPS攻击下3种恢复方案的效果对比. 受GPS攻击且无恢复机制的无人机的GPS传感器测量值相比未受攻击时的偏移量随时间逐渐增加. 对于LDR、SW-Sensor、PID-Piper，偏移量增大后逐渐减小. GPS的预测值相比未受攻击时的偏移量更大，说明受攻击后的无人机偏离预定轨迹的幅度越大. 可见，LDR相比SW-Sensor的恢复(偏移量趋向0)更迅速，无人机受到攻击后偏离幅度更小. 而PID-Piper的实际恢复效果较差，无法阻止无人机的持续性偏离.

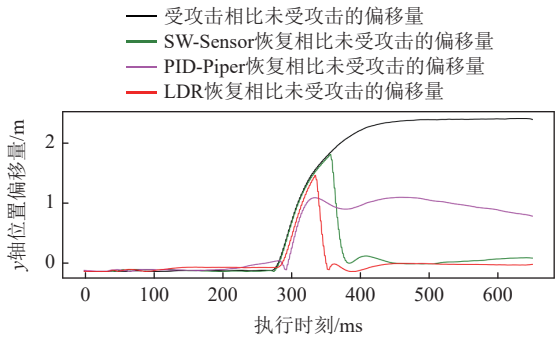


Fig. 7 GPS sensor attack recovery effect comparison between LDR and related research work

图7 LDR与相关研究工作的GPS传感器攻击恢复效果比较

图8为陀螺仪读数攻击下，3种恢复方案在无人机姿态翻滚角指标上的恢复效果对比. 图8(a)(b)给出了LDR预测得到的翻滚角与未受攻击状态下的翻滚角相比的偏差绝对值曲线. 图8(a)给出了SW-Sensor预测得到的翻滚角与未受攻击状态下的翻滚角相比的偏差绝对值曲线. 图8(b)给出了PID-Piper预测得到的翻滚角与未受攻击状态下的翻滚角相比的偏差绝对值曲线. 翻滚角的偏差绝对值越大，代表无人机受到攻击后机体摆动幅度越大. 由图8结合图6(c)结果可见，SW-Sensor和PID-Piper在无人机受到陀螺仪读数攻击后翻滚角偏差和振荡非常大，与没有应用任何恢复机制时的偏差相比(见图6(c))，机体摆动幅度减小不明显. 而LDR系统检测到陀螺仪读数攻击后，翻滚角保持了一段时间的平稳，且相比SW-Sensor和PID-Piper的翻滚角偏差有显著减小，表明在受到攻击后LDR仍能有效恢复陀螺仪读数，使无人机保持一段时间较为平稳地飞行.

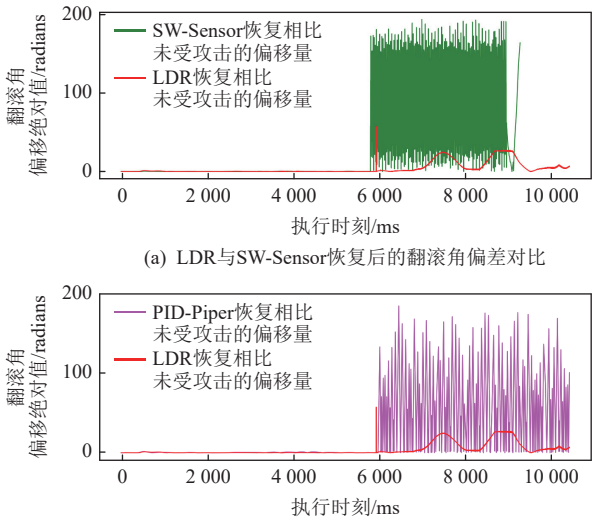


Fig. 8 Gyroscope reading attack recovery effect comparison between LDR and related research work

图8 LDR与相关研究工作的陀螺仪读数攻击恢复效果比较

4 讨 论

本文主要考虑针对传感器实施的攻击，由于本文检测和恢复机制皆依赖于模型预测结果，攻击者可能会尝试通过操纵模型决策或模型输入输出的方式来绕过本文方案. 然而，决策和数据皆位于飞控软件内部. 攻击者要达成意图，需要借助软件层面(如控制流劫持)或网络层面的攻击手段. 这些攻击手段的攻击面正交于本文所关注的传感器攻击，因而超出了本文的研究范畴. 此外，本文可以借助已有的软件安全机制应对这些安全威胁. 如将飞控系统部分实现为可信执行环境中的可信应用[31]，以阻止攻击者操纵飞控的数据流和控制流，从而确保模型决策和预测结果的可靠性.

此外，无人机在实际运行中可能会因部件磨损、使用环境改变等因素导致系统行为改变，致使模型不再准确可靠. 对此，可以定期在安全受控环境下对无人机进行飞行测试，收集飞行日志进行分析，并按需更新模型以适应新的系统行为模式. 由于本文模型训练时间短、训练开销小，仅需通用PC机即可完成，因此更新模型不会引入难以承担的时间开销和算力开销.

飞控系统本身的基于EKF的传感器融合机制能够提供一定程度的抗干扰能力，使无人机的传感器测量值在无人机机体正常抖动、噪声等扰动下正常

飞行. 这些噪声和干扰也确实会一定程度上影响本文机器学习模型的训练和检测, 本文使用的缓解方法是通过实施真实无人机上的硬件手段(减震板等降噪措施)和软件手段(如滤波)减轻其影响.

更低的攻击频率和更小的攻击幅度可能会对本文的检测和恢复产生影响, 使得本文的检测算法需要使用更紧的阈值, 收紧阈值也可能导致潜在的漏报产生, 我们虽然证明了本文提出的检测及恢复算法在2种典型公开攻击下的有效性, 但针对隐蔽攻击的检测和恢复效果仍有待进一步验证.

5 结 论

本文提出了一种基于机器学习的无人机传感器攻击在线检测和恢复方案 LDR. 证明了针对2类典型的传感器注入攻击, 由机器学习模型的非线性系统表征能力、所提出的检测和恢复算法对短时预测振荡导致的误报的缓解能力, 以及轻量级机器学习模型的有限运行时开销所带来的检测恢复效果, 达到了相比现有在线传感器攻击检测和恢复方案更好的检测和恢复效果. 未来的工作包括3个方面: 1)将本文方案应用于其他的开源无人机飞控系统, 如 PX4; 2)将本文方案应用于更多的传感器注入攻击形式, 特别是一些攻击注入量较小的隐蔽攻击, 并讨论不同机器学习模型和检测算法的检测敏感程度差异; 3)尝试引入其他非线性控制模型用于无人机系统状态恢复.

作者贡献声明: 孙聪提出了论文核心思想并撰写论文; 曾荟铭设计检测算法、实现论文软件并进行主要实验; 宋焕东实施部分对比试验; 王运柏实现部分对比方案; 张宗旭协助部分软件功能实现; 马建峰提出指导意见并修改论文.

参 考 文 献

[1] Wang Jinyong, Huang Zhiqiu, Yang Deyan, et al. Spatio-clock synchronous constraint guided safe reinforcement learning for autonomous driving[J]. Journal of Computer Research and Development, 2021, 58(12): 2585−2603 (in Chinese)
(王金永, 黄志球, 杨德艳, 等. 面向无人驾驶时空同步约束制导的安全强化学习[J]. 计算机研究与发展, 2021, 58(12): 2585−2603)

[2] Dash P, Karimibiuki M, Pattabiraman K. Out of control: Stealthy attacks against robotic vehicles protected by control-based techniques [C] //Proc of the 35th Annual Computer Security Applications Conf. New York: ACM, 2019: 660−672

[3] Lu Xiaozhen, Jie Jingfang, Lin Zihan, et al. Reinforcement learning based energy efficient robot relay for unmanned aerial vehicles against smart jamming[J]. Science China Information Sciences, 2022, 65(1): 112304

[4] Kune D F, Backes J, Clark S S, et al. Ghost talk: mitigating EMI signal injection attacks against analog sensors [C] //Proc of IEEE Symp on Security and Privacy. Piscataway, NJ: IEEE, 2013: 145−159

[5] Shoukry Y, Martin P, Tabuada P, et al. Non-invasive spoofing attacks for anti-lock braking systems [C] //Proc of 15th Int Workshop on Cryptographic Hardware and Embedded Systems. Berlin: Springer, 2013: 55−72

[6] Cao Yulong, Xiao Chaowei, Cyr B, et al. Adversarial sensor attack on lidar-based perception in autonomous driving [C] //Proc of the 2019 ACM SIGSAC Conf on Computer and Communications Security. New York: ACM, 2019: 2267−2281

[7] Schmidt D, Radke K, Camtepe S, et al. A survey and analysis of the GNSS spoofing threat and countermeasures[J]. ACM Computing Surveys, 2016, 48(4): 1−31

[8] Tu Zhan, Fei Fan, Eagon M, et al. Flight recovery of MAVs with compromised IMU [C] //Proc of IEEE/RSJ Int Conf on Intelligent Robots and Systems. Piscataway, NJ: IEEE, 2019: 3638−3644

[9] Fei Fan, Tu Zhan, Yu Ruikun, et al. Cross-layer retrofitting of UAVs against cyber-physical attacks [C] //Proc of IEEE Int Conf on Robotics and Automation. Piscataway, NJ: IEEE, 2018: 550−557

[10] Choi H, Lee W C, Aafer Y, et al. Detecting attacks against robotic vehicles: A control invariant approach [C] //Proc of the 2018 ACM SIGSAC Conf on Comupter and Communications Security. New York: ACM, 2018: 801−816

[11] Quinonez R, Giraldo J, Salazar L E, et al. SAVIOR: Securing autonomous vehicles with robust physical invariants[C] // Proc of the 29th USENIX Security Symp. Berkeley, CA: USENIX Association, 2020: 895−912

[12] Choi H, Kate S, Aafer Y, et al. Software-based realtime recovery from sensor attacks on robotic vehicles [C] //Proc of the 23rd Int Symp on Research in Attacks, Intrusions and Defenses. Berkeley, CA: USENIX Association, 2020: 349−364

[13] Dash P, Li Guanpeng, Chen Zitao, et al. PID-Piper: Recovering robotic vehicles from physical attacks [C] //Proc of the 51st Annual IEEE/IFIP Int Conf on Dependable Systems and Networks. Piscataway, NJ: IEEE, 2021: 26−38

[14] Nassi B, Bitton R, Masuoka R, et al. SoK: Security and privacy in the age of commercial drones [C] //Proc of IEEE Symp on Security and Privacy. Piscataway, NJ: IEEE, 2021: 1434−1451

[15] Kwon C, Liu Weiyi, Hwang I. Analysis and design of stealthy cyber attacks on unmanned aerial systems[J]. Journal of Aerospace Information Systems, 2014, 11(8): 525−539

[16] Kwon C, Yantek S, Hwang I. Real-time safety assessment of unmanned aircraft systems against stealthy cyber attacks[J]. Journal of Aerospace Information Systems, 2016, 13(1): 27−45

[17] Aboutalebi P, Abbaspour A, Forouzannezhad P, et al. A novel sensor fault detection in an unmanned quadrotor based on adaptive neural observer[J]. Journal of Intelligent and Robotic Systems, 2018, 90: 473−484

[18] Chen Wenxin, Dong Yingfei, Duan Zhenhai, Accurately redirecting a malicious drone [C] //Proc of 19th Annual Consumer Communications and Networking Conf. Piscataway, NJ: IEEE, 2022: 827−834

[19] 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

[20] Noh J, Kwon Y, Son Y, et al. Tractor beam: Safe-hijacking of consumer drones with adaptive GPS spoofing [J]. ACM Transactions on Privacy and Security, 2019, 22(2): 12: 1−12: 26

[21] Son Y, Shin H, Kim D, et al. Rocking drones with intentional sound noise on gyroscopic sensors [C] //Proc of the 24th USENIX Security Symp. Berkeley, CA: USENIX Association, 2015: 881−896

[22] Trippel T, Weisse O, Xu Wenyuan, et al. WALNUT: Waging doubt on the integrity of MEMS accelerometers with acoustic injection attacks [C] //Proc of IEEE European Symp on Security and Privacy. Piscataway, NJ: IEEE, 2017: 3−18

[23] Davidson D, Wu Hao, Jellinek R, et al. Controlling UAVs with sensor input spoofing attacks [C] //Proc of the 10th USENIX Workshop on Offensive Technologies. Berkeley, CA: USENIX Association, 2016: 1−11

[24] Chen Wenxin, Duan Zhenhai, Dong Yingfei. False data injection on EKF-based navigation control [C] //Proc of the Int Conf on Unmanned Aircraft Systems. Piscataway, NJ: IEEE, 2017: 1608−1617

[25] Xue Nian, Niu Liang, Hong Xianbin, et al. DeepSIM: GPS spoofing detection on UAVs using satellite imagery matching [C] // Proc of the 36th Annual Computer Security Applications Conf. New York: ACM, 2020: 304−319

[26] Whelan J, Sangarapillai T, Minawi O, et al. Novelty-based intrusion detection of sensor attacks on unmanned aerial vehicles [C] //Proc of the 16th ACM Symp on QoS and Security for Wireless and Mobile Networks. New York: ACM, 2020: 23−28

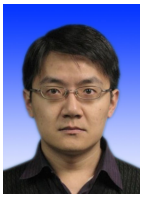
[27] Henderson D M. Euler angles, Quaternions, and transformation matrices for space shuttle analysis[R]. NASA STI Repository. 1977 [2023-05-23]. https://ntrs.nasa.gov/citations/19770019231

[28] Oppenheim A V, Willsky A S, Nawab S H. Signals and Systems [M]. Upper Saddle River, NJ: Prentice Hall, 1997

[29] Sakoe H, Chiba S. Dynamic programming algorithm optimization for spoken word recognition[J]. IEEE Transactions on Acoustics, Speech, and Signal Processing, 1978, 26(1): 43−49

[30] Tobias Hermann. frugally-deep [EB/OL]. [2023-05-23]. https://github.com/Dobiasd/frugally-deep

[31] Wang Jinwen, Li Ao, Li Haoran, et al. RT-TEE: Real-time system availability for cyber-physical systems using ARM TrustZone [C] // Proc of IEEE Symp on Security and Privacy. Piscataway, NJ: IEEE, 2022: 352−369

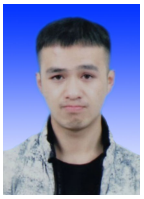


Sun Cong, born in 1982. PhD, professor, PhD supervisor. Member of CCF. His main research interests include software security, program analysis, and unmanned system security.

孙　聪, 1982 年生. 博士, 教授, 博士生导师. CCF 会员. 主要研究方向为软件安全、程序分析、无人系统安全.

Zeng Huiming, born in 1997. Master, engineer. His main research interest includes unmanned system security.

曾荟铭, 1997 年生. 硕士, 工程师. 主要研究方向为无人系统安全.



Song Huandong, born in 1997. Master, engineer. His main research interest includes unmanned system security.

宋焕东, 1997 年生, 硕士, 工程师. 主要研究方向为无人系统安全.

Wang Yunbo, born in 1995. PhD candidate. His main research interests include UAV security, embedded system, and machine learning.

王运柏, 1995 年生. 博士研究生. 主要研究方向为无人机安全、嵌入式系统和机器学习.

Zhang Zongxu, born in 2001. Master candidate. His main research interest includes unmanned system security.

张宗旭, 2001 年生. 硕士研究生. 主要研究方向为无人系统安全.

Ma Jianfeng, born in 1963. PhD, professor, PhD supervisor. CCF fellow. His main research interests include information security, cryptography, and network security.

马建峰, 1963 年生. 博士, 教授, 博士生导师. CCF 会士. 主要研究方向为信息安全、密码学、网络安全.