

深度置信网络在四旋翼无人机传感器攻击检测中的应用

石鹏程, 赵振根[†], 李庆龙

(南京航空航天大学 自动化学院, 江苏 南京 210016)

摘要: 为了实现四旋翼无人机的传感器攻击快速准确检测, 本文提出了一种基于状态估计和深度学习的攻击检测算法. 首先, 算法利用扩展卡尔曼滤波器(EKF)估计无人机状态, 并从传感器测量中提取特征信息. 接着, 采用滑动时序窗口构建检测信息, 并通过深度置信网络(DBN)建立检测信息与传感器状态(是否受攻击)之间的非线性映射关系. EKF简化了传感器状态检测信息的获取过程, 而DBN准确拟合了复杂的非线性关系, 从而显著提高了检测精度. 为增强状态估计的可靠性, 本文还设计了一种自适应EKF算法, 能够在检测到传感器攻击时动态调整测量噪声的协方差矩阵. 仿真结果表明, 所提出的EKF-DBN检测算法在准确率和检测效率上优于传统方法.

关键词: 扩展卡尔曼滤波器; 深度置信网络; 攻击检测; 四旋翼无人机; 自适应滤波

引用格式: 石鹏程, 赵振根, 李庆龙. 深度置信网络在四旋翼无人机传感器攻击检测中的应用. 控制理论与应用, 2026, 43(4): 774 – 782

DOI: 10.7641/CTA.2024.40199

Application of deep belief network in sensor attack detection for quadrotor UAVs

SHI Peng-cheng, ZHAO Zhen-gen[†], LI Qing-long

(College of Automation Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing Jiangsu 210016, China)

Abstract: To achieve fast and accurate detection of sensor attacks on quadrotor UAVs, this paper proposes an attack detection algorithm based on state estimation and deep learning. Firstly, the algorithm uses the extended Kalman filter (EKF) to estimate the UAV's state and extract feature information from sensor measurements. Then, a sliding temporal window is applied to construct detection information, and a deep belief network (DBN) is used to establish a nonlinear mapping between the detection information and the sensor state (whether under attack). EKF simplifies the acquisition of sensor state detection information, while DBN accurately fits the complex nonlinear relationship, significantly improving detection accuracy. Furthermore, an adaptive EKF algorithm is designed to dynamically adjust the measurement noise covariance matrix upon detecting a sensor attack, enhancing the reliability of state estimation. Simulation results show that the proposed EKF-DBN detection algorithm outperforms traditional methods in terms of accuracy and detection efficiency.

Key words: quadrotor UAV; extended Kalman filter; deep belief network; attack detection; adaptive filtering

Citation: SHI Pengcheng, ZHAO Zhengeng, LI Qinglong. Application of deep belief network in sensor attack detection for quadrotor UAVs. *Control Theory & Applications*, 2026, 43(4): 774 – 782

1 引言

随着技术的进步, 四旋翼无人机凭借其结构简单、机动性强等优势, 被广泛应用于农业、林业、安全等行业. 对于四旋翼无人机而言, 传感器采集的信息在其控制系统中至关重要, 其准确性和可靠性直接影响飞行安全^[1]. 无人机通常会配备有惯性导航系统(inertial

navigation system, INS) 和全球导航卫星系统(global navigation satellite system, GNSS), 为其提供确保飞行安全所必需的实时状态数据. 与INS不同, GNSS信号较弱且码结构公开, 因此更容易受到信号欺骗攻击, 存在严重的安全隐患^[2-4]. 若缺乏有效的检测机制, 攻击可能在未被察觉的情况下发生, 进而引发严

收稿日期: 2024-04-03; 录用日期: 2024-12-12.

[†]通信作者. E-mail: zhaozhengeng@nuaa.edu.cn; Tel.: +86 13101889700.

本文责任编辑: 左志强.

国家自然科学基金基础科学中心项目(62388101), 国家自然科学基金面上项目(62473195), 国家自然科学基金重点项目(62233009), 中国博士后科学基金面上项目(2021M701701), 中央高校基本科研业务费专项资金项目(NS2024017)资助.

Supported by the Basic Science Center Program of the National Natural Science Foundation of China (62388101), the National Natural Science Foundation of China General Program (62473195), the National Natural Science Foundation of China Key Program (62233009), the China Postdoctoral Science Foundation (2021M701701) and the Fundamental Research Funds for the Central Universities (NS2024017).

重后果^[5]. 因此, 无人机的传感器攻击检测是保障无人机安全的关键.

现有的无人机传感器攻击检测方法主要有两种, 即基于状态估计和基于学习. 基于状态估计的攻击检测方法通过状态观测器估计无人机的系统状态, 并验证状态估计与传感器测量值之间的差距是否超过预设阈值^[6-8], 以检测攻击. 文献[9]提出了一种基于扩展卡尔曼滤波器 (extended Kalman filter, EKF) 的新息序列检测方法, 用于检测传感器和控制指令是否受到虚假数据注入攻击. 然而, 这种方法的阈值选取依赖于先验知识, 而且容易受到系统噪声的干扰^[10].

基于学习的攻击检测方法在实际应用中较为广泛. 由于无人机传感器测量值具有明显的时间序列特性. 文献[11]提出了一种基于长短期记忆 (long short-term memory, LSTM) 神经网络的异常检测模型, 通过预测传感器数据并比较预测值与实际测量值的差异来检测攻击. 然而, 这类方法需要大量训练数据, 且由于四旋翼无人机的复杂性, 训练过程可能十分耗时. 因此, 通常将机器学习、强化学习等与状态估计及其他特征提取方法结合使用^[6]. 文献[12]研究了全球定位系统 (global positioning system, GPS) 和惯性测量单元 (inertial measurement unit, IMU) 在正常条件下的误差分布, 并基于此设计了一种支持向量机 (support vector machine, SVM) 的GPS攻击检测器.

综上所述, 基于状态估计和基于学习的检测方法均涉及特征提取和特征映射两个核心步骤. 特征提取是从系统输入输出数据中获取与传感器状态 (是否受攻击) 相关的信息; 特征映射则是构建这些特征与传感器状态相关的非线性映射关系. 本文提出了一种基于EKF和深度置信网络 (deep belief network, DBN) 的攻击检测算法. 该算法利用EKF估计无人机系统状态, 结合传感器测量值和滑动时序窗口构建检测信息, 再通过DBN拟合检测信息与传感器状态之间的非线性关系. 同时, 本文将攻击检测结果融入状态估计, 提出了一种自适应EKF算法, 通过调整测量噪声的协方差矩阵, 减少攻击传感器对EKF的影响.

2 系统建模与理论基础

2.1 四旋翼无人机建模

本文基于欧拉角的姿态表示方法, 建立了四旋翼无人机的非线性数学模型. ϕ , θ 和 ψ 分别表示机体坐标系相对于地理坐标系的滚转角、俯仰角和偏航角. 忽略空气阻力和陀螺仪效应后, 四旋翼无人机的非线性模型如式(1)所示^[6, 13-14]:

$$\begin{cases} \ddot{\mathbf{p}}^e = \mathbf{g}\mathbf{e}_3 - \frac{f}{m}\mathbf{R}_b^e\mathbf{e}_3, \\ \dot{\Theta} = \mathbf{W} \times \boldsymbol{\omega}^b, \\ \mathbf{J} \times \dot{\boldsymbol{\omega}}^b = -\boldsymbol{\omega}^b \times (\mathbf{J} \times \boldsymbol{\omega}^b) + \boldsymbol{\tau}, \end{cases} \quad (1)$$

其中: $\mathbf{p}^e = [p_x^e \ p_y^e \ p_z^e]^T$ 代表四旋翼无人机质心在地理坐标系下的位置, $\Theta = [\phi \ \theta \ \psi]^T$ 表示机体相对于地理坐标系的欧拉角, $\boldsymbol{\omega}^b = [\omega_x^b \ \omega_y^b \ \omega_z^b]^T$ 代表机体相对于机体坐标系的角速度, f 为螺旋桨总拉力, $\boldsymbol{\tau} = [\tau_x \ \tau_y \ \tau_z]^T$ 为螺旋桨在机体轴上产生的力矩, $\mathbf{e}_3 = [0 \ 0 \ 1]^T$ 表示地理坐标系下 $o_e z_e$ 轴的单位向量, \mathbf{g} 表示重力加速度. 姿态变化率和机体角速度之间的转换矩阵 \mathbf{W} 、转动惯量矩阵 \mathbf{J} 、机体坐标系到地理坐标系的旋转矩阵 \mathbf{R}_b^e 以及四旋翼无人机的非线性模型(1)的显示形式分别在附录中定义.

为了简化后续研究, 本文采用欧拉积分法对上式进行离散化, 时间间隔为 $T = 0.01$ s. 考虑到离散化的时间间隔较短, 因此假设在该时间间隔内系统的控制量保持不变. 上述非线性模型(1)可离散化为如式(2)所示:

$$\begin{cases} \mathbf{x}_{k+1} = \mathbf{F}(\mathbf{x}_k, \mathbf{u}_k) + \mathbf{w}_k, \\ \mathbf{y}_k = \mathbf{H}_k \mathbf{x}_k + \mathbf{v}_k, \end{cases} \quad (2)$$

其中: $\mathbf{u}_k = [f_k \ \tau_k^x \ \tau_k^y \ \tau_k^z]^T$ 表示四旋翼无人机的控制量; $\mathbf{x}_k = [\mathbf{p}_k \ \dot{\mathbf{p}}_k \ \Theta_k \ \boldsymbol{\omega}_k]$ 表示四旋翼无人机的状态量; $\mathbf{y}_k = [\mathbf{p}_k \ \dot{\mathbf{p}}_k \ \boldsymbol{\omega}_k]$ 为四旋翼无人机的传感器测量值; $\mathbf{F}(\cdot)$ 表示四旋翼无人机的非线性状态方程; \mathbf{H}_k 表示系统观测矩阵; 过程噪声 \mathbf{w}_k 和测量噪声 \mathbf{v}_k 是分别服从均值为零、协方差矩阵为 \mathbf{Q}_w 和 \mathbf{Q}_v 的正态分布, 两者相互独立. 过程噪声包括建模误差和外界扰动.

2.2 攻击建模

无人机的传感器攻击的目的主要为诱导无人机偏离正常位置, 从而捕获无人机^[15]. 本文针对攻击者能力差异, 分别设计了如下两种形式的攻击信号:

1) 随机信号

$$a_k^i = U(m, n), \quad (3)$$

其中: a_k^i 表示攻击信号 $\mathbf{a}_k \in \mathbb{R}^9$ 中第 i 个元素, $U(m, n)$ 表示服从区间 $[m, n]$ 的均匀分布的随机数.

2) 斜坡信号

$$a_k^i = b \times (k - \Gamma), \quad (4)$$

其中: b 为标量, Γ 表示无人机受到攻击的时刻.

结合上述攻击信号, 当四旋翼无人机传感器遭受虚假数据注入 (false data injection, FDI) 攻击时, 量测方程可以建模为如下形式:

$$\mathbf{y}_k = \begin{cases} \mathbf{H}_k \mathbf{x}_k + \mathbf{v}_k, & k < \Gamma, \\ \mathbf{H}_k \mathbf{x}_k + \mathbf{v}_k + \mathbf{G}\mathbf{a}_k, & k \geq \Gamma, \end{cases} \quad (5)$$

其中, $\mathbf{G} \in \mathbb{R}^{9 \times 9}$ 为攻击指示矩阵, 其对角线元素 λ_i 为 $\{0, 1\}$, 其他元素为0. 当 $\lambda_i = 1$ 时, 表示相应的测量信号遭受攻击; 否则, 表示该信号未受攻击. 本文仅考虑GNSS的欺骗攻击, 因此攻击矩阵 \mathbf{G} 中, $\lambda_4, \lambda_5, \dots$,

λ_9 均为0.

注1 无人机传感器故障和攻击都可能导致无人机的异常行为,并且均可建模为上述形式.然而,传感器攻击相比传感器故障具有更强的目的性和不可预测性,且后果更加严重.攻击者可以设计出随时间演化的攻击信号,在不触发传统 χ^2 检测的前提下实现对无人机传感器的攻击.因此,本文设计如攻击信号(4)对该情况进行说明.

注2 在实际实施中,攻击信号(3)–(4)要求攻击者能够获取无人机的具体位置并预测无人机在下一时刻的位置;然后,结合式(5)和攻击信号的特点生成虚假的位置信息,并设计相应的GNSS欺骗信号;最后,通过信号发射器广播,从而实现GNSS欺骗攻击^[15].与攻击信号(3)相比,攻击信号(4)要求攻击者能够获取准确的无人机位置并预测下一时刻的位置,以及更精细的控制GNSS欺骗信号,在不引起注意的前提下实现逐步诱骗无人机的目的.

为了验证传感器攻击对四旋翼无人机的影响,本文采用阶跃信号作为FDI攻击的攻击信号,进行如下仿真实验.如图1所示,黑色虚线表示无人机的期望轨迹,蓝色实线是未受攻击的飞行轨迹,红色实线是遭受FDI攻击后的飞行轨迹.假设无人机的实际位置为POS,传感器测量到的位置为 $POS^{(m)}$,期望位置为 $POS^{(d)}$.在正常情况下,传感器测量值 $POS^{(m)}$ 能够准确反映无人机的实际位置POS.然而,当GNSS受到幅值为 ε 的FDI攻击时,传感器的测量值将变为 $POS^{(m)} = POS + \varepsilon$.此时,控制器将根据测量值 $POS^{(m)}$ 进行控制,试图将无人机位置保持在期望值 $POS^{(d)}$,但实际上无人机的实际位置将变为 $POS^{(d)} - \varepsilon$.因此,传感器攻击可能导致无人机的实际位置偏离期望位置,从而引发无人机失控或被劫持.

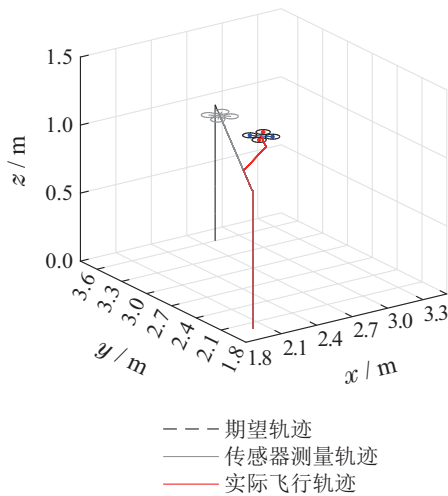


图1 注入攻击影响

Fig. 1 Effect of injection attack

2.3 扩展卡尔曼滤波器

本研究采用扩展卡尔曼滤波器(EKF)来估计四旋翼无人机的内部状态,核心是通过忽略高阶项对非线性

函数进行线性化.状态转移方程的线性化形式 Φ_k 可通过下式计算:

$$\Phi_k = \frac{\partial \mathbf{F}(\mathbf{x}, \mathbf{u}_k)}{\partial \mathbf{x}} \Big|_{\mathbf{x}=\hat{\mathbf{x}}_{k|k}}. \quad (6)$$

扩展卡尔曼状态估计分为预测阶段和更新阶段,具体步骤如下:

1) 预测阶段:基于上一时刻的最优状态估计,预测下一时刻的状态和协方差矩阵:

$$\begin{cases} \hat{\mathbf{x}}_{k|k-1} = \mathbf{F}(\hat{\mathbf{x}}_{k-1|k-1}, \mathbf{u}_{k-1}), \\ \mathbf{P}_{k|k-1} = \Phi_{k-1} \mathbf{P}_{k-1|k-1} \Phi_{k-1}^T + \mathbf{Q}_w, \\ \mathbf{r}_k = \mathbf{y}_k - \mathbf{H}_k \hat{\mathbf{x}}_{k|k-1}. \end{cases} \quad (7)$$

2) 计算卡尔曼增益:卡尔曼增益的计算是扩展卡尔曼滤波中的核心步骤之一,

$$\mathbf{K}_k = \mathbf{P}_{k|k-1} \mathbf{H}_k^T (\mathbf{H}_k \mathbf{P}_{k|k-1} \mathbf{H}_k^T + \mathbf{Q}_v)^{-1}. \quad (8)$$

3) 更新阶段:利用预测信息和实际观测值,修正状态估计和协方差矩阵,

$$\begin{cases} \hat{\mathbf{x}}_{k|k} = \hat{\mathbf{x}}_{k|k-1} + \mathbf{K}_k \mathbf{r}_k, \\ \mathbf{P}_{k|k} = (\mathbf{I}_n - \mathbf{K}_k \mathbf{H}_k^T) \mathbf{P}_{k|k-1}. \end{cases} \quad (9)$$

2.4 自适应扩展卡尔曼滤波器

当传感器受到FDI攻击时,EKF的结果将会偏离实际.因此在无人机受传感器攻击的情况下,本文采用自适应EKF进行状态估计.当检测到传感器受到攻击后,自适应EKF将重新计算测量噪声的协方差矩阵,具体公式如下:

$$\mathbf{S}_k = \left(\sum_{j=1}^N \nu_j \mathbf{r}_{k-j} \mathbf{r}_{k-j}^T - \mathbf{H}_k \mathbf{P}_{k|k-1} \mathbf{H}_k^T \right) \mathbf{Q}_v^{-1}, \quad (10)$$

其中: $\nu_j \in \mathbb{R}^{9 \times 9}$ 表示随机加权矩阵; N 表示滑动时序窗口的大小; \mathbf{S}_k 表示缩放矩阵,用来提高自适应EKF的鲁棒性.

为了保证测量噪声协方差的有效性和正确性,将需要首先修改 \mathbf{S}_k ,并相应调整卡尔曼增益 \mathbf{K}_k ,

$$\begin{cases} \hat{\mathbf{S}}_k = \text{diag}\{\hat{s}_1, \dots, \hat{s}_9\}, \\ \hat{s}_i = \max(1, S_{ii}), \quad i = 1, 2, \dots, 9, \\ \mathbf{K}_k = \mathbf{P}_{k|k-1} \mathbf{H}_k^T (\mathbf{H}_k \mathbf{P}_{k|k-1} \mathbf{H}_k^T + \hat{\mathbf{S}}_k \mathbf{Q}_v)^{-1}, \end{cases} \quad (11)$$

其中, S_{ii} 表示缩放矩阵 \mathbf{S}_k 第*i*个对角线元素.

2.5 深度置信网络

深度置信网络(DBN)是一种多层神经网络,既可以进行非监督学习,也可以进行监督学习;是通过堆叠多个受限玻尔兹曼机(restricted Boltzmann machine, RBM)来构建的,具体结构如图2所示.每个RBM由一个可见层和一个隐层组成,这两层之间的神经元是双向全连接的.RBM的主要功能是通过输入数据集来学习数据的概率分布,具体的数学推导可以参考文

献[16].

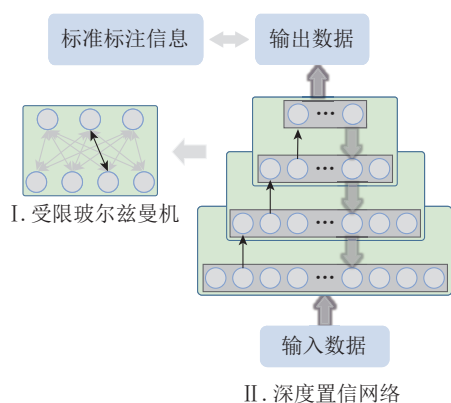


图2 深度置信网络

Fig. 2 Deep belief network (DBN)

由于DBN是由多个RBM组成,因此训练DBN的实质就是对各个RBM进行训练. Hinton等^[17]在2002年提出的对比散度(contrastive divergence, CD)算法大大简化了RBM的训练过程. 在本文的应用中,为了实现最终目标,本文在预训练后的DBN上添加了一个分类层. 然后,通过反向传播(back propagation, BP)算法,将误差信息从DBN的顶层传播到底层,从而对整个网络进行微调,实现全局优化. 训练过程可以分为两个主要阶段:

1) 预训练阶段: 逐层训练DBN中的每个RBM, 利用CD算法对每个RBM进行训练, 以获取数据的特征表示;

2) 微调阶段: 在预训练完成后, 为了实现最终目标, 在DBN的顶层添加一个分类层(通常是一个具有sigmoid激活函数的全连接层). 接下来, 使用监督学习的反向传播算法对整个网络进行微调, 从而实现对整个网络的全局优化.

通过这两个阶段的训练, 可以确保DBN在获取数据特征的同时, 也能够有效地进行分类, 从而提升模型的整体性能.

2.6 问题描述

本文着眼于无人机系统中传感器的安全性, 旨在开发一种基于EKF和DBN的攻击检测算法, 以准确地识别无人机传感器的FDI攻击. 本研究重点关注特征提取、特征映射和攻击检测模型的构建, 旨在解决以下几个关键问题:

- 1) 如何有效地从传感器数据中提取关键特征?
- 2) 如何构建能够准确区分正常和异常模式的攻击检测模型?
- 3) 提出的方法的检测性能表现如何?

本研究将采用EKF和DBN解决特征提取和特征映射的问题, 并基于此设计攻击检测器以实现攻击的准确检测. 同时, 本文设计一个离线训练算法用于训

练攻击检测器, 以及一个在线攻击检测算法用于评价检测算法的性能. 此外, 本文还探讨了如何将攻击检测结果反馈到EKF设计中, 提高系统在复杂环境下的可靠性.

3 攻击检测器设计

本研究将攻击检测器的设计过程分为两个主要环节: 特征提取和特征映射. 为应对这一挑战, 本文提出了一种结合EKF和DBN的无人机传感器攻击检测算法. 在该算法中, EKF负责从传感器数据中提取关键特征, 而DBN则用于处理这些特征的映射关系, 以实现有效的攻击检测. 该攻击检测算法的设计流程如图3所示. 为了提高系统在攻击条件下的可靠性, 本文将攻击检测结果融合到状态估计中, 提出了一种自适应EKF算法.

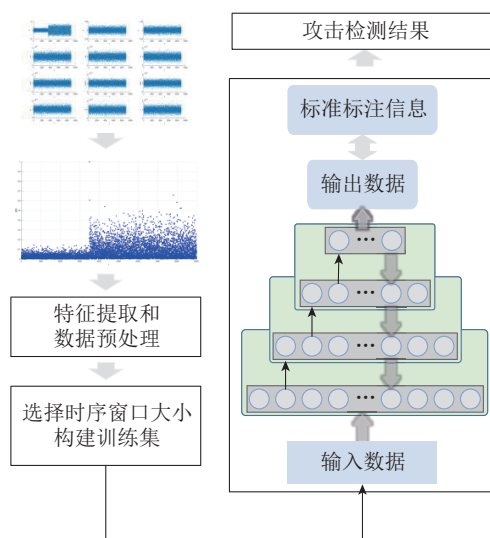


图3 攻击检测器设计流程图

Fig. 3 Attack detector design flow chart

3.1 特征提取

本文利用EKF获取四旋翼无人机系统状态的估计值, 并将其与传感器的测量值进行比较. 在正常情况下, EKF的估计值 $\hat{x}_{k|k-1}$ 应该与传感器的测量值 y_k 是相似的. 换言之, 当这两者之间存在显著差异时, 就可以推断无人机受到了攻击.

在数学上, 衡量数据相似度的方法通常分为基于距离和基于相似度系数的算法. 然而, 基于相似度系数的方法无法有效衡量每一维数据的差异^[18]. 而相较于其他距离度量方法, 欧几里得距离对低维数据的敏感性更强, 且能够直观地计算传感器测量值与状态估计之间的偏差^[19]. 因此, 本文采用欧几里得距离作为衡量 $H_k \hat{x}_{k|k-1}$ 与 y_k 之间差异的指标,

$$\eta_k = \mathbf{r}_k^T \mathbf{r}_k, \quad (12)$$

其中: \mathbf{r}_k 表示EKF的估计误差; η_k 表示 $\hat{x}_{k|k-1}$ 与 y_k 之间的欧几里得距离.

斜坡信号可以在不引起 η_k 变化的前提下对系统的观测结果造成巨大损失. 因此本文引入滑动时序窗口对 \mathbf{r}_k 各个维度的特征信息进行处理, 获取可用于攻击信号为斜坡信号的FDI攻击检测的特征信息,

$$\bar{\mathbf{r}}_k = \sum_{i=k-W+1}^k \mathbf{r}_i, \quad (13)$$

其中: W 表示滑动时序窗口的大小; $\bar{\mathbf{r}}_k \in \mathbb{R}^9$ 表示在滑动时序窗口 W 内估计误差 \mathbf{r}_k 的累计和.

由于攻击信号(3)–(4)对无人机系统产生的影响不同, 本文结合滑动时序窗口对两种攻击信号分别设计了相应的传感器的攻击检测信息, 分别表示为式(14)和式(15), 即

$$\mathbf{o}_\eta = [\eta_{k-M+1} \cdots \eta_{k-1} \eta_k], \quad (14)$$

$$\mathbf{o}_r = [\bar{\mathbf{r}}_{k-N+1}^{px} \cdots \bar{\mathbf{r}}_k^{px} \bar{\mathbf{r}}_{k-N+1}^{py} \cdots \bar{\mathbf{r}}_k^{py} \bar{\mathbf{r}}_{k-N+1}^{pz} \cdots \bar{\mathbf{r}}_k^{pz}], \quad (15)$$

其中: M 和 N 表示对应的滑动时序窗口的大小; $\mathbf{o}_\eta \in \mathbb{R}^M$ 表示攻击信号(3)的攻击检测信息, $\mathbf{o}_r \in \mathbb{R}^{3N}$ 表示攻击信号(4)的攻击检测信息.

滑动时序窗口的选择对攻击检测器性能至关重要. 较大的窗口包含更多数据, 有助于提高检测准确性, 但会增加计算成本; 较小的窗口则数据量较少, 可能降低检测准确性. 因此, 实际应用中需根据无人机系统的具体情况和性能要求, 合理选择窗口大小, 以平衡准确性和计算效率.

3.2 特征映射

特征映射是利用DBN强大的数据特征提取能力, 构建检测信息与传感器状态之间的非线性映射关系. 为此, 本文提出了一种基于DBN的传感器攻击检测算法. 首先, 逐层预训练RBM初始化DBN的权重; 然后, 通过监督学习微调DBN的网络参数, 使其更好地适应传感器攻击检测任务. 同时, 本文提出了一种在线检测算法以评估DBN攻击检测器的检测性能. 当检测器检测到攻击并做出响应后, 系统将重新启动新一轮在线检测.

基于此, 本文总结了如算法1(见表1)和算法2(见表2)所示的离线训练算法和在线检测算法. 算法1用来训练四旋翼无人机传感器攻击检测器; 算法2是用来评价设计好的DBN攻击检测器的检测性能. 在算法1中: \mathcal{D} 表示训练迭代次数, \mathcal{N} 表示训练样本数据集中的个数, \mathcal{L} 表示RBM的层数. 在算法2中: output 表示DBN攻击检测器的输出值, T 表示攻击检测器检测到攻击的时刻.

为了评估所提出算法的检测性能, 本文定义了攻击检测的虚警率和漏报率. 虚警率 P_{FAR} 表示在正常情况下, 攻击检测器错误地将传感器系统识别为受攻击的概率. 漏报率 P_{MAR} 表示在攻击发生后的允许时间

内, 攻击检测器仍然没有识别出攻击的概率. 这两个指标的计算公式如下:

$$\begin{cases} P_{\text{FAR}} = \frac{\mathcal{T}_{T < \Gamma}}{\mathcal{T}_{T < \Gamma} + \mathcal{T}_{\Gamma \leq T \leq \Gamma+t} + \mathcal{T}_{T > \Gamma+t}}, \\ P_{\text{MAR}} = \frac{\mathcal{T}_{T > \Gamma+t}}{\mathcal{T}_{T < \Gamma} + \mathcal{T}_{\Gamma \leq T \leq \Gamma+t} + \mathcal{T}_{T > \Gamma+t}}, \end{cases} \quad (16)$$

其中: T 表示攻击检测宣布检测出攻击的时间; Γ 表示攻击者发起攻击的时间; t 表示检测出攻击的最大允许时间; $\mathcal{T}_{T < \Gamma}$, $\mathcal{T}_{\Gamma \leq T \leq \Gamma+t}$ 和 $\mathcal{T}_{T > \Gamma+t}$ 表示检测系统检测到攻击的时间 T 满足对应的条件的实验的次数.

表1 算法1: 离线训练算法

Table 1 Algorithm 1: The offline training algorithm

输入:	预处理好的训练数据集、真实标签集
1	初始化DBN网络, RBM层数 \mathcal{L} 、迭代次数 \mathcal{D}
2	For $l=1:\mathcal{L}$
3	For epoch=1: \mathcal{D}
4	使用对比散度算法更新RBM权值
5	End For
6	End For
7	For epoch=1: \mathcal{D}
8	DBN进行前向传播, 得到输出值 output
9	计算 output 与对应标签值的误差
10	误差反向传播, 微调DBN的权值
11	End For
输出:	训练好的DBN攻击检测器

表2 算法2: 在线攻击检测

Table 2 Algorithm 2: The online attack detection

输入:	训练好的DBN攻击检测器以及对应攻击信号
1	While $\text{output} == 1$ Do
2	收集四旋翼无人机的测量值 \mathbf{y}_k
3	采用式(7)计算 \mathbf{r}_k
4	分别采用式(12)–(13)提取特征信息
5	设计对应攻击检测信息 \mathbf{o}_η 或 \mathbf{o}_r
6	获取DBN攻击检测器输出 output
7	$k = k + 1$
8	End While
输出:	遭受传感器受攻击的时刻: $T = k$

3.3 攻击检测与自适应EKF的结合

持续攻击会对EKF的结果造成显著影响. 为了提高系统在持续攻击下的可靠性, 本文提出了一种将攻击检测结果与自适应EKF相结合的自适应状态估计算法. 该算法的具体步骤如表3所示, 其中: k_{end} 表示仿真终止时间, output 表示DBN攻击检测器的输出结果.

3.4 数据集生成

为了验证所提出的攻击检测算法, 本文采用MATLAB编写四旋翼无人机仿真模型, 并采用PID控制器

对无人机定点飞行控制的仿真方法生成了一些无人机正常飞行以及受攻击后飞行的数据。

表3 自适应状态估计算法

Table 3 Algorithm3: The adaptive state estimation algorithm

输入:	训练好的DBN攻击检测器
1	For $k=1:k_{\text{end}}$
2	采用式(7)计算 r_k
3	分别采用式(12)–(13)提取特征信息
4	构建攻击检测信号 o_η 和 o_r
5	计算DBN攻击检测器的输出output
6	If output == 1
7	采用式(10)–(11)计算 K_k
8	Else
9	采用式(8)计算 K_k
10	End If
11	采用式(9)更新状态估计
12	$k = k + 1$
13	End For

无人机的仿真飞行时间为80 s, 时间间隔为0.01 s, FDI攻击发生的时间为40 s, 攻击矩阵为 $G = \text{diag}\{1, 0, 0, 0, 0, 0, 0, 0\}$. 四旋翼无人机的相关参数和仿真平台的参数在附录部分给出. 本文采用不同FDI攻击信号分别进行仿真飞行获取无人机数据集, 然后获取EKF的状态估计 $\hat{x}_{k|k-1}$ 与传感器的测量值 y_k 之间的估计误差 r_k . 并定义滑动时序窗口 $W = 25$, 采用式(12)–(13)计算特征信息 η_k 和 \bar{r}_k , 并构建数据集. 为了提高后续神经网络训练过程的效率和准确性, 需要对攻击检测信息进行归一化处理, 得到如表4所示的攻击数据集.

表4 传感器攻击数据集

Table 4 The sensor attack dataset

名称	攻击信号	特征信息	对应检测信息
数据集1	$a_k = U(0.1, 0.2)$	η_k	$o_\eta \in \mathbb{R}^M$
数据集2	$a_k = 0.1 \times (k - \Gamma)$	\bar{r}_k	$o_r \in \mathbb{R}^{3N}$

4 攻击检测器性能分析

4.1 滑动时序窗口对检测性能的影响

增加RBM层数可增强DBN的学习能力, 但过多的层数可能导致训练不稳定. 基于仿真实验结果, 本文确定最优配置为四层RBM. 此外, 本文选择了滑动时序窗口大小为18, 21, 24, 27, 并设计了如表5所示的DBN攻击检测器, 以探讨窗口大小对攻击检测算法的影响.

4.1.1 计算复杂度分析

滑动时序窗口的大小对DBN攻击检测算法的计算复杂度具有显著影响, 随着窗口大小的增加, 模型所需的计算开销也会增加.

表5 DBN结构

Table 5 The structure of DBN

检测器名称	数据集	滑动时序窗口	四层RBM配置	输出层维度
DBN1	数据集1	$M = 18$	18 72 36 36 18	1
DBN2	数据集1	$M = 21$	21 84 42 42 21	1
DBN3	数据集1	$M = 24$	24 96 48 48 24	1
DBN4	数据集1	$M = 27$	27 108 54 54 27	1
DBN5	数据集2	$N = 18$	54 216 108 108 54	1
DBN6	数据集2	$N = 21$	63 252 126 126 63	1
DBN7	数据集2	$N = 24$	72 288 144 144 72	1
DBN8	数据集2	$N = 27$	81 324 162 162 81	1

为量化这种影响, 本文采用DBN攻击检测器在特定数据集上, 经过若干次迭代所需的训练时间和DBN攻击检测器对单个检测信息进行前向传播所需的检测时间作为评估算法计算复杂度和实时性的指标^[20]. 本文将DBN攻击检测器预训练阶段的迭代次数设置为2000次, 参数微调阶段的迭代次数设置为2500次. 表6展示了在附录中描述的硬件平台上, DBN攻击检测器的训练时间和检测时间.

表6 攻击检测器的计算复杂度

Table 6 The computation complexity of the attack detector

名称	训练时间/s	检测时间/ms
DBN1	2 024.9	1.60×10^{-2}
DBN2	2 095.3	1.62×10^{-2}
DBN3	2 350.1	1.64×10^{-2}
DBN4	2 677.9	1.71×10^{-2}
DBN5	4 604.7	2.82×10^{-2}
DBN6	5 434.5	2.97×10^{-2}
DBN7	6 318.7	3.22×10^{-2}
DBN8	7 221.9	3.42×10^{-2}

4.1.2 检测性能分析

本节通过仿真实验研究了滑动时序窗口大小对攻击检测性能的影响. DBN攻击检测器的预训练阶段迭代次数设为2000次, 参数微调阶段迭代次数设为2500次. 采用算法2评估无人机攻击检测器, 总实验次数为5000次. 为了评估DBN检测器能否在攻击对系统造成严重影响前发现攻击, 将随机信号的最大允许检测时间设为0.15 s, 斜坡信号的最大允许检测时间设为0.25 s. 根据在线检测的仿真结果和性能指标, 得出了检测结果, 如图4–5所示.

检测结果表明, DBN攻击检测器的性能会随着滑动时序窗口大小的变化而显著变化. 对于随机信号, 虚警率随着窗口 M 增大而降低, 而漏报率则上升. 这是因为当无人机受攻击时, 在 $k > \Gamma$ 时, 检测信息中

的异常特征数据比例会随着窗口 M 增大而减小,导致DBN检测器难以在规定时间内检测到攻击,从而增加漏报率.相反,当无人机处于正常状态时,窗口 M 增大使得检测器对噪声引起的异常值不敏感,从而降低虚警率.对于斜坡信号,随着窗口 N 增大,检测准确率和漏报率均有所降低.窗口增大会增加攻击检测信息的有效数据,从而提高检测效果.

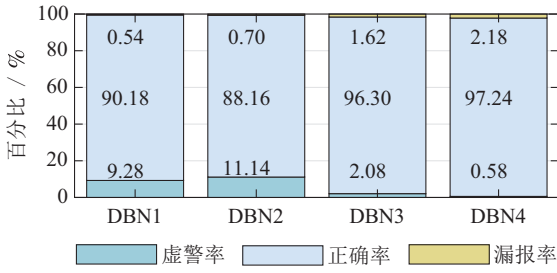


图4 检测结果($a_k^i = U(0.1, 0.2)$)

Fig. 4 The detection result ($a_k^i = U(0.1, 0.2)$)

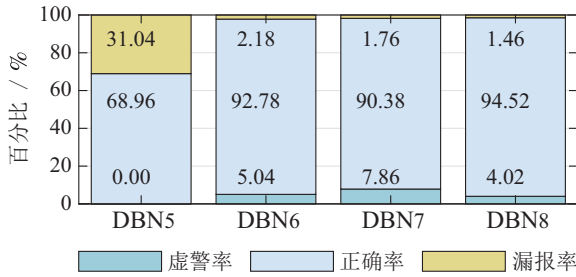


图5 检测结果($a_k^i = 0.1 \times (k - \Gamma)$)

Fig. 5 The detection result ($a_k^i = 0.1 \times (k - \Gamma)$)

从不同滑动时序窗口下对DBN攻击检测器复杂度和性能的分析可见,增大窗口大小有助于提高检测准确性,但同时也增加了训练和检测时间.基于对不同窗口配置下DBN检测器计算复杂度和性能的分析,本文最终选择滑动时序窗口大小为27来构建DBN攻击检测器.

4.2 检测性能对比分析

为了验证DBN在攻击检测中的优势,本文将其与 l_2 范数攻击检测算法^[8],文献[9]所提出的新息序列检测算法 (innovation sequence detection, ISD) 以及基于DNN网络的攻击检测算法^[21]进行对比.采用文献[22]所提出的智能算法,在置信度为99%以及虚警率为0.5%的条件下将 l_2 范数攻击检测算法的阈值设置为0.0021;将ISD的阈值设置为14.35;DNN网络结构为最优状态.

针对攻击信号(3)和攻击信号(4),4种攻击检测方法的检测结果分别如下图6-7所示.从图6-7中不难看出,基于 l_2 范数的攻击检测算法和ISD算法无法有效检测出攻击信号(3)和攻击信号(4).特别是针对攻击信号(4),两种方法的检测准确率均低于5%.而DNN

攻击检测算法和本文提出的攻击检测算法相对于前面两种检测算法来说有较大的提升,但针对两种攻击信号本文所提出的攻击检测方法均优于DNN网络,而且本文提出的攻击检测算法的漏报率更低,这样可以及时检测出传感器攻击并执行应对方法,不至于出现更严重的后果.因此,本文所提出的DBN攻击检测算法更有优势.

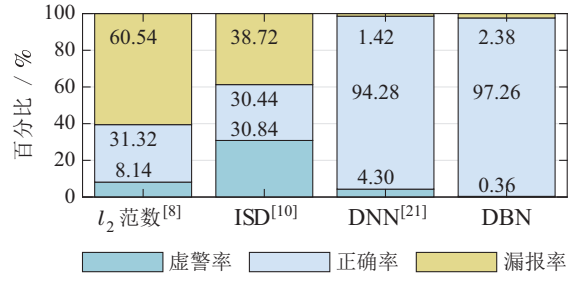


图6 对比分析($a_k^i = U(0.1, 0.2)$)

Fig. 6 Contrast analysis ($a_k^i = U(0.1, 0.2)$)

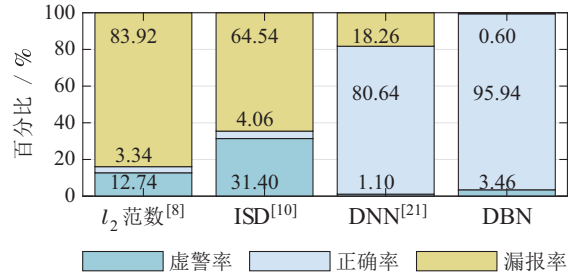


图7 对比分析($a_k^i = 0.1 \times (k - \Gamma)$)

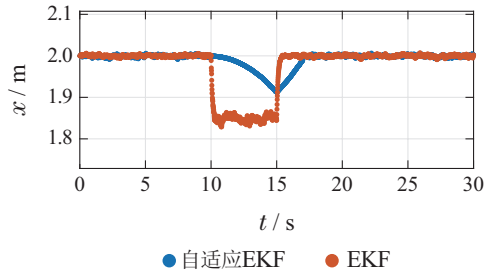
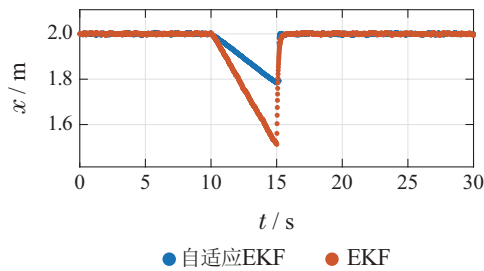
Fig. 7 Contrast analysis ($a_k^i = 0.1 \times (k - \Gamma)$)

4.3 基于检测的自适应EKF性能分析

本节将通过仿真实验验证本文提出的自适应状态估计算法的性能.假设FDI攻击在无人机飞行的第10~15s发生,分别比较EKF和自适应EKF的状态估计效果.

如图8和图9分别展示了系统在受到攻击信号(3)和(4)时,自适应EKF和EKF对系统状态的估计表现.结果表明,自适应EKF在两种攻击信号下的估计偏差均小于EKF.然而,攻击结束后,针对攻击信号(3),系统的估计偏差仍然会持续一段时间,而在攻击信号(4)则不会出现这种情况.

这是因为在攻击结束后,针对攻击信号(3)的检测器未能正确识别传感器状态(是否受攻击),导致系统仍然采用自适应EKF降低传感器测量值的权重,进而导致系统状态估计的不准确.而导致这种现象的主要原因是针对两种攻击信号的检测机制不同:针对攻击信号(3)的检测信号(14)由 η_k 构成,仅考虑了估计误差 r_k 的数值大小而不考虑其方向性(正负号);而针对攻击信号(4)的检测信号(15)则由 \bar{r}_k 构成,考虑了估计误差 r_k 数值大小和方向性.

图8 EKF和自适应EKF性能对比($a_k^i = U(0.1, 0.2)$)Fig. 8 Performance comparison between EKF and adaptive EKF ($a_k^i = U(0.1, 0.2)$)图9 EKF和自适应EKF性能对比($a_k^i = 0.1 \times (k - \Gamma)$)Fig. 9 Performance comparison between EKF and adaptive EKF ($a_k^i = 0.1 \times (k - \Gamma)$)

5 结论

本文提出了一种基于EKF-DBN的四旋翼无人机传感器攻击检测器。首先, 算法结合EKF和滑动时序窗口构建检测信息, 然后, 利用DBN构建传感器攻击检测器。为降低持续FDI攻击对系统的影响, 本文将攻击检测框架与自适应EKF结合, 设计了自适应状态估计算法, 以提高系统的鲁棒性。在分析DBN攻击检测器计算复杂度的基础上, 本文通过仿真探讨了滑动时序窗口大小对检测效果的影响, 构建了最优的DBN攻击检测器, 并与其他检测器进行了对比。实验结果表明, DBN攻击检测器的准确率优于其他算法。然而, 本研究存在两点局限性: 一是未在实际无人机系统中部署所提算法; 二是未深入探讨如何应对攻击者可能对系统造成的重大影响。未来工作将重点解决这些问题, 以增强系统的适应性和鲁棒性, 提升其在实际应用中的可靠性。

参考文献:

[1] HE D J, CHAN S, GUIZANI M. Communication security of unmanned aerial vehicles. *IEEE Wireless Communications*, 2017, 24(4): 134 – 139.

[2] SCHMIDT E, GATSI S N, AKOPIAN D. A GPS spoofing detection and classification correlator-based technique using the LASSO. *IEEE Transactions on Aerospace and Electronic Systems*, 2020, 56(6): 4224 – 4237.

[3] GYO Y, WU M P, TANG K H, et al. Covert spoofing algorithm of UAV based on GPS/INS-integrated navigation. *IEEE Transactions on Vehicular Technology*, 2019, 68(7): 6557 – 6564.

[4] ZHI Y Y, FU Z J, SUN X M, et al. Security and privacy issues of uav: A survey. *Mobile Networks and Applications*, 2020, 25(1): 95 – 101.

[5] HUMPHREYS T E, LEDVINA B M, PSIAKI M L, et al. Assessing the spoofing threat: development of a portable GPS civilian spoofer. *International Technical Meeting of the Satellite Division of the Institute of Navigation*. Savannah: ION, 2008, 9: 2314 – 2325.

[6] XIAO J P, FEROSKHAN M. Cyber attack detection and isolation for a quadrotor UAV with modified sliding innovation sequences. *IEEE Transactions on Vehicular Technology*, 2022, 71(7): 7202 – 7214.

[7] ZHUANG Kangxi, SUN Ziwen. Establishing a detection model for denial of service attacks in industrial cyber physical systems. *Control Theory & Applications*, 2020, 37(3): 629 – 638. (庄康熙, 孙子文. 针对工业信息物理系统中的拒绝服务攻击建立检测模型. *控制理论与应用*, 2020, 37(3): 629 – 638.)

[8] ELSISI M, ALTIUS M, SU S F, et al. Robust Kalman filter for position estimation of automated guided vehicles under cyberattacks. *IEEE Transactions on Instrumentation and Measurement*, 2023, 72: 1 – 12.

[9] XIAO Jiaping, JIANG Jianchun, SHE Chungong. Data attack detection for an unmanned aerial vehicle control system using innovation sequences. *Control Theory & Applications*, 2017, 34(12): 1575 – 1582. (肖佳平, 蒋建春, 余春东. 新息序列驱动的无人机控制系统数据攻击检测. *控制理论与应用*, 2017, 34(12): 1575 – 1582.)

[10] GIRALDO J, URBINA D, CARDENAS A, et al. A survey of physics-based attack detection in cyber-physical systems. *ACM Computing Surveys*, 2019, 51(4): 1 – 36.

[11] LI Chen, WANG Buhong, TIAN Jiwei. Anomaly detection method for UAV sensor data based on LSTM-OCSVM. *Journal of Chinese Computer Systems*, 2021, 42(4): 700 – 705. (李晨, 王布宏, 田继伟. 基于LSTM-OCSVM的无人机传感器数据异常检测. *小型微型计算机系统*, 2021, 42(4): 700 – 705.)

[12] PANICE G, LUONGO S, GIGANTE G, et al. A SVM-based detection approach for GPS spoofing attacks to UAV. *The 23rd International Conference on Automation and Computing (ICAC)*. Huddersfield: IEEE, 2017, 7: 1 – 11.

[13] MAHONY R, KUMAR V, CORKE P. Multirotor aerial vehicles: modeling, estimation and control of quadrotor. *IEEE Robotics & Automation Magazine*, 2012, 19(3): 20 – 32.

[14] YAO Qianqian, QI Guoyuan. Model compensation optimal control for quadrotor UAV system. *Control Theory & Applications*, 2024, 41(11): 2061 – 2070. (姚倩倩, 齐国元. 四旋翼无人机系统模型补偿最优控制. *控制理论与应用*, 2024, 41(11): 2061 – 2070.)

[15] GUO Yan, TANG Kanghua, ZHANG Lu. GNSS navigation spoofing method of UAV based on point-by-point offset. *Advanced Engineering Sciences*, 2023, 55(2): 275 – 284. (郭妍, 唐康华, 张鹭. 面向无人机的逐点偏移式卫星导航欺骗干扰方法. *工程科学与技术*, 2023, 55(2): 275 – 284.)

[16] FISCHER A, IGEL C. Training restricted Boltzmann machines: An introduction. *Pattern Recognit*, 2014, 47(1): 25 – 39.

[17] HINTON G E. Training products of experts by minimizing contrastive divergence. *Neural Computation*, 2002, 14(8): 1771 – 1800.

[18] XU R, WUNSCHII D. Survey of clustering algorithms. *IEEE Transactions on Neural Networks*, 2005, 16(3): 645 – 678.

[19] MANANDHAR K, CAO X J, HU F, et al. Detection of faults and attacks including false data injection attack in smart grid using Kalman filter. *IEEE Transactions on Control of Network Systems*, 2014, 1(4): 370 – 379.

[20] FREIRE P, SRIVALLAPANONNDH S, SPINNLER B, et al. Computational complexity optimization of neural network-based equalizers in digital signal processing: A comprehensive approach. *Journal of Lightwave Technology*, 2024, 42(12): 4177 – 4199.

[21] DEVAN P, KHARE N. An efficient XGBoost-DNN-based classification model for network intrusion detection system. *Neural Computing and Applications*, 2020, 32(16): 12499 – 12514.

- [22] LIU R J, LI L L, YANG Y. Performance residual based fault detection for feedback control systems. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 2021, 68(10): 3291 – 3295.

附录

四旋翼无人机的数学模型将在附录中给出. 为了表述简单, 分别将 $\sin(\cdot)$ 和 $\cos(\cdot)$ 定义为 $s(\cdot)$ 和 $c(\cdot)$. 机体坐标系到地理坐标系的旋转矩阵 \mathbf{R}_b^e 表示为如下形式:

$$\mathbf{R}_b^e = \begin{bmatrix} c\theta c\psi & c\psi s\theta s\phi - s\psi c\phi & c\psi s\theta c\phi + s\psi s\phi \\ c\theta s\psi & s\psi s\theta s\phi + c\psi c\phi & s\psi s\theta c\phi - c\psi s\phi \\ -s\theta & s\phi c\theta & c\phi c\theta \end{bmatrix}. \quad (\text{A1})$$

四旋翼无人机的姿态变化率和机体角速度之间的转换矩阵 \mathbf{W} 定义为如下形式:

$$\mathbf{W} = \begin{bmatrix} 1 & s\phi s\theta k\theta & c\phi s\theta k\theta \\ 0 & c\phi & -s\phi \\ 0 & s\phi k\theta & c\phi k\theta \end{bmatrix}. \quad (\text{A2})$$

转动惯量矩阵 \mathbf{J} 可以表示为

$$\mathbf{J} = \begin{bmatrix} I_{xx} & 0 & 0 \\ 0 & I_{yy} & 0 \\ 0 & 0 & I_{zz} \end{bmatrix}, \quad (\text{A3})$$

其中, I_{xx} , I_{yy} , I_{zz} 分别表示四旋翼无人机绕 x , y , z 轴的转动惯量.

为了简化后续研究, 本文采用欧拉积分法对上式进行离散化, 离散的时间间隔为 $T = 0.01$ s. 考虑到离散化采用的时间间隔较短, 因此假设在该时间间隔内控制器输入的控制量不变. 非线性连续方程(1)可离散化为如下形式:

$$\begin{aligned} p_{k+1}^x &= p_k^x + \frac{T}{2}(p_{k+1}^{\dot{x}} + p_k^{\dot{x}}) + w_{px}, \\ p_{k+1}^y &= p_k^y + \frac{T}{2}(p_{k+1}^{\dot{y}} + p_k^{\dot{y}}) + w_{py}, \\ p_{k+1}^z &= p_k^z + \frac{T}{2}(p_{k+1}^{\dot{z}} + p_k^{\dot{z}}) + w_{pz}, \\ p_{k+1}^{\dot{x}} &= p_k^{\dot{x}} + \frac{Tf_k}{m}(s\theta_k c\phi_k c\psi_k + s\phi_k s\psi_k) + w_{vx}, \\ p_{k+1}^{\dot{y}} &= p_k^{\dot{y}} + \frac{Tf_k}{m}(s\theta_k c\phi_k s\psi_k - s\phi_k c\psi_k) + w_{vy}, \\ p_{k+1}^{\dot{z}} &= p_k^{\dot{z}} + T(g - \frac{f_k}{m}c\theta_k c\phi_k) + w_{vz}, \end{aligned}$$

$$\begin{aligned} \phi_{k+1} &= \phi_k + T(\omega_x^b + \frac{\omega_y^b s\phi s\theta}{c\theta} + \frac{\omega_z^b c\phi s\theta}{c\theta}) + w_\phi, \\ \theta_{k+1} &= \theta_k + T(\omega_y^b c\phi - \omega_z^b s\phi) + w_\theta, \\ \psi_{k+1} &= \psi_k + T(\frac{\omega_y^b s\phi}{c\theta} + \frac{\omega_z^b c\phi}{c\theta}) + w_\psi, \\ \omega_{k+1}^x &= \omega_k^x + T(\frac{I_y - I_z}{I_x} \omega_k^y \omega_k^z + \frac{1}{I_x} \tau_x) + w_{\omega_x}, \\ \omega_{k+1}^y &= \omega_k^y + T(\frac{I_z - I_x}{I_y} \omega_k^x \omega_k^z + \frac{1}{I_y} \tau_y) + w_{\omega_y}, \\ \omega_{k+1}^z &= \omega_k^z + T(\frac{I_x - I_y}{I_z} \omega_k^y \omega_k^x + \frac{1}{I_z} \tau_z) + w_{\omega_z}, \quad (\text{A4}) \end{aligned}$$

其中: 下标 k 表示在 k 时刻的值; w 表示系统的过程噪声, 它的下标分别表示对应通道.

本文以四旋翼无人机仿真飞行验证设计的攻击检测器算法的可行性和有效性. 本次仿真采用的计算机配置为一块集成了Intel(R) UHD Graphics 730集成图形处理器的12th Generation Intel Core i5-12400处理器. 无人机飞行过程仿真、数据处理、神经网络训练以及在线攻击检测过程均在MATLAB 2021a上进行. 四旋翼无人机的参数如表A1所示. 当飞行时间大于预定的攻击时间后, 按照式(5)实施FDI攻击, 获取攻击检测器所需数据.

表 A1 四旋翼无人机参数
Table A1 Quadrotor parameters

项目	符号	单位	数值
机体质量	m	kg	1.2
旋翼中心到机体中心的距离	l	m	0.154
绕 x 轴转动惯量	I_{xx}	kg·m ²	0.008 64
绕 y 轴转动惯量	I_{yy}	kg·m ²	0.008 64
绕 z 轴转动惯量	I_{zz}	kg·m ²	0.062 0

作者简介:

石鹏程 硕士研究生, 研究方向为无人机安全, E-mail: spc0506@nuaa.edu.cn;

赵振根 副教授, 硕士生导师, 研究方向为信息物理系统安全与无人机智能控制, E-mail: zhaozhengen@nuaa.edu.cn;

李庆龙 硕士研究生, 研究方向为无人机安全, E-mail: liqinglong@nuaa.edu.cn.