DOI: 10.7641/CTA.2017.70053

新息序列驱动的无人机控制系统数据攻击检测

肖佳平[1,2†], 蒋建春[2,4], 佘春东[3]

(1. 北京航空航天大学 航空科学与工程学院, 北京 100191; 2. 中国科学院 软件研究所, 北京 100090;
3. 北京邮电大学 电子工程学院, 北京 100876; 4. 贺州学院 数据科学与信息安全联合实验室, 广西 贺州 542800)

摘要: 伴随物联网和自主系统的不断发展, 信息物理系统的网络安全备受关注. 无人机是一种典型的依靠通信和控制系统实现自主飞行的智能装置, 其安全性尤为突出. 本文针对无人机的状态估计算法, 考虑其传感器和控制指令受到数据攻击, 提出基于扩展卡尔曼滤波的新息序列状态估计检测方法. 首先建立无人机信息物理模型, 引入状态估计算法和数据攻击模型. 然后, 利用新息序列构造标量检测统计量用于数据攻击检测, 并针对飞行器机动造成的状态跳变引入负无穷范数, 用以降低数据攻击检测的误检率. 最后, 通过仿真实验验证所提出的检测方法能有效检测不同威胁模式下和状态下无人控制系统的数据攻击.

关键词: 无人机; 信息物理系统; 入侵检测; 网络安全

中图分类号: TP273 **文献标识码**: A

Data attack detection for an unmanned aerial vehicle control system using innovation sequences

XIAO Jia-ping[1,2†], JIANG Jian-chun[2,4], SHE Chun-dong[3]

(1. School of Aeronautic Science and Engineering, Beihang University, Beijing 100191, China;
2. Institute of Software, Chinese Academy of Sciences, Beijing 100090, China;
3. School of Electronic Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China;
4. Joint Laboratory of Data Science and Information Security, Hezhou University, Hezhou Guangxi 542800, China)

Abstract: With rapid advances in the fields of the Internet of things and autonomous systems, the network security of cyber-physical systems has attracted considerable attention. An unmanned aerial vehicle (UAV) is an intelligent device that relies on information communication and flight control systems to achieve autonomous flight. Consequently, its security is extremely important. This study proposes a new state estimation method that uses innovation sequences based on an extended Kalman filter for the detection of data attacks on a UAV. Our method can identify data attacks on tensors and control commands. First, a cyber-physical system model for a UAV is established, and the state estimation algorithm and data attack model are introduced. Then, a scalar detection statistic is constructed for data attack detection using innovation sequences, and the minus infinity norm method is introduced to reduce the false detection of data attacks while the aircraft is being maneuvered. Finally, simulation results show that the proposed detection method can effectively detect various threat patterns under a variety of circumstances for unmanned control systems.

Key words: unmanned aerial vehicle; cyber-physical system; intrusion detection; network security

1 引言(Introduction)

无人机是一种依赖地面通信和飞行控制系统实现自主飞行的智能信息物理系统, WiFi、GPS、蓝牙、红外线和ZigBee是无人机通信网络中经常使用的通讯方式, 而且很容易被攻击. 随着无人机广泛应用, 各种类型的无人机安全性问题[1−2]随之暴露. 例如, “大疆”无人机被曝光存在安全漏洞, 同时据CNN报导, 美国航空公司的航班客机也多次被黑客攻击. 无人系统的实时控制和通信能力使得其具备广泛应用能力, 同时也容易受到可能的数据攻击. 目前无人机面临的攻击和威胁主要集中在: 无线信号劫持与干扰、GPS欺骗、针对传感器网络的攻击、状态信息被其他控制端监测、实际物理状态和信息表述不一致、虚假无人机接入控制中心、报告虚假信息、无人机接受非授权

收稿日期: 2017−01−20; 录用日期: 2017−08−18.
†通信作者. E-mail: xjpmail@buaa.edu.cn; Tel.: +86 15652291691.
本文责任编委: 胡跃明.
国家自然科学基金项目(91438120), 广西壮族自治区教育厅符号计算与工程数据处理重点实验室开发课题(FH201504)资助.
Supported by National Natural Science Foundation of China (91438120) and Development Issue of Symbolic Computation and Engineering Data Processing Key Laboratory of Department of Education, Guangxi Zhuang Autonomous Region (FH201504).

验证的控制中心指令、无人机的信息处理能力下降、无人机接收处理外部恶意的数据, 导致飞行能力下降(例如能耗增加)[3]或飞行轨迹异常.

围绕无人机的攻击、状态估计和无人机安全保护问题, 国内外都开展相应的研究工作. Javaid等人[4] 对无人机系统建模并对其信息安全威胁进行了数据流层面的分析和评估, Hwang等人[5]通过构造隐秘的通信欺骗对无人机系统进行攻击, 这种攻击可以有效绕过常规的检测, 然后影响飞行安全, 文献[6]指出可利用网络安全方式例如信道加密[7]、DoS攻击防御[8]和入侵检测系统[9] 增强无人机通信网络安全. 对于无人机的通信数据攻击检测, 其核心则是基于传感器数据构建有效的状态估计方法. 状态估计用于空中交通管理的目标跟踪[10]、电力系统故障检测[11]和信息网络安全检测[12–13]. Tabuada等人[14] 提出了针对攻击状态下信息物理系统的安全性估计和控制方法. 目前, 已有的这些状态估计攻击检测方法主要针对稳态情况下的线性定常系统, 而实际的无人机系统则是复杂的非线性时变系统, 无人机的实时动态性能尤为重要, 传统的状态估计检测方法难以实时检测复杂机动条件下的数据攻击. 其面临的挑战, 一是非线性时变混合系统的状态估计需要构建比较精确的系统模型, 二是难以对存在不同尺度随机跳变的系统进行较为精确的状态估计, 即使Liu等人[15]对随机混合系统提出一般状态估计方法, 飞行机动中的状态跳变与传感器数据攻击共存也使得数据攻击检测存在较大难度.

针对上述挑战问题, 本文考虑无人机飞行过程的非线性和时变特征, 采用新息序列驱动估计检测方法, 该方法考虑滑动窗口内估计残差序列的统计特性, 用于优化估计状态. 在本文中, 一是提出了基于新息序列驱动的状态估计方法, 二是建立机动状态下的传感器动态数据攻击检测方法. 该方法基于扩展卡尔曼滤波对无人机的姿态进行状态估计, 利用传感器的新息序列, 对姿态估计进行修正. 当传感器数据遭遇攻击, 根据窗口内状态估计残差统计特征设置警报. 机动状态下考虑估计状态的时间快慢尺度特性[16], 对窗口内估计残差取范数, 实现飞行机动与传感器数据攻击的状态估计分离, 从而利用飞行机动跳变影响较慢的估计状态检测数据攻击.

本文其余组成是: 第2部分针对四旋翼无人机建立非线性信息物理系统模型, 采用扩展卡尔曼滤波对飞行器姿态进行状态估计, 并构建不同的通信数据攻击模型; 第3部分提出基于新息序列驱动的动态数据攻击检测机制; 第4部分给出飞行器处于不同飞行模式下的数据攻击检测仿真验证结果; 第5部分给出分析和结论.

2 无人机信息物理模型(Unmanned aerial vehicle cyber physical model)

针对无人机的姿态估计, 不失一般性, 考虑其为离散时间的非线性时变系统:

$$\begin{cases} x_{k+1} = f(x_k, u_k, w_k), \\ y_k = h(x_k, u_k, v_k), \end{cases} k \in \mathbb{N}, \tag{1}$$

式中: $x_k \in \mathbb{R}^n$为状态量, $y_k \in \mathbb{R}^m$为量测量, u_k表示输入量, 过程噪声w_k和量测噪声v_k为相互独立的随机变量且满足均值为零的正态分布.

过程噪声包含未建模动态或者扰动输入, 分布p满足以下概率密度函数:

$$\begin{cases} p(w) \sim \aleph(0, Q),\ Q = \mathrm{diag}\{\sigma_{w1}^2, \sigma_{w2}^2, \cdots\}, \\ p(v) \sim \aleph(0, R),\ R = \mathrm{diag}\{\sigma_{v1}^2, \sigma_{v2}^2, \cdots\}, \end{cases} \tag{2}$$

式中σ^2表示对应噪声分布的方差.

2.1 基于扩展卡尔曼滤波的状态估计 (The state estimation based on extended Kalman filtering)

扩展卡尔曼滤波(extended Kalman filtering, EKF)将系统方程沿每步的先验估计$\hat{x}_k$进行线性化, 然后将系统视为线性系统处理. 计算系统方程关于状态量x_k和噪声量w_k, v_k的偏微分方程得到Jacobian矩阵:

$$A_{\mathrm{lin},k} = (\frac{\partial f(x_k, u_k, w_k)}{\partial x_k})^{\mathrm{T}}|_{\hat{x}_k^-}, \tag{3a}$$

$$W_{\mathrm{lin},k} = (\frac{\partial f(x_k, u_k, w_k)}{\partial w_k})^{\mathrm{T}}|_{\hat{x}_k^-}, \tag{3b}$$

$$H_{\mathrm{lin},k} = (\frac{\partial h(x_k, u_k, v_k)}{\partial x_k})^{\mathrm{T}}|_{\hat{x}_k^-}, \tag{3c}$$

$$V_{\mathrm{lin},k} = (\frac{\partial h(x_k, u_k, v_k)}{\partial v_k})^{\mathrm{T}}|_{\hat{x}_k^-}, \tag{3d}$$

式中竖线下变量表示在此时刻状态下的偏导.

EKF计算过程如下:

1) 初值选择. 选取初始状态估计值$\hat{x}_k^0$和状态误差协方差矩阵初始值P_k^0;

2) 先验预测. 预计状态变量和状态误差协方差矩阵:

$$\hat{x}_{k+1}^- = f(\hat{x}_k, u_k, 0), \tag{4}$$

$$P_{k+1}^- = A_{\mathrm{lin},k} P_k A_{\mathrm{lin},k}^{\mathrm{T}} + W_{\mathrm{lin},k} Q_k W_{\mathrm{lin},k}. \tag{5}$$

3) 后验修正.

首先, 计算卡尔曼增益

$$K_k = P_k^- H_{\mathrm{lin},k}^{\mathrm{T}} (H_{\mathrm{lin},k} P_k^- H_{\mathrm{lin},k}^{\mathrm{T}} + V_{\mathrm{lin},k} R_k V_{\mathrm{lin},k})^{-1}. \tag{6}$$

然后, 根据量测值更新估计状态

$$\hat{x}_k = \hat{x}_k^- + K_k(y_k - h(\hat{x}_k^-, u_k, 0)). \tag{7}$$

最后, 更新状态误差协方差矩阵

$$P_k = (I - K_k H_{\mathrm{lin},k}) P_k^{-}. \tag{8}$$

按照以上流程循环进行状态估计, 直至稳定收敛.

选取状态量和观测量如下:

$$x = \begin{bmatrix} q_0 \\ q_1 \\ q_2 \\ q_3 \end{bmatrix},\ y = \begin{bmatrix} a_{\mathrm{x}} \\ a_{\mathrm{y}} \\ a_{\mathrm{z}} \\ \psi_{\mathrm{m}} \end{bmatrix}, \tag{9}$$

式中: q_i 表示姿态解算的四元数值, $a_{\mathrm{x}}, a_{\mathrm{y}}, a_{\mathrm{z}}$ 表示MEMS中加速度计的测量值, ψ_{m}表示通过三轴磁阻传感器解算得到的航向角. 估计状态方程如式(10)所示:

$$\dot{x} = \frac{1}{2}\begin{bmatrix} 0 & -\omega_{\mathrm{x}} & -\omega_{\mathrm{y}} & -\omega_{\mathrm{z}} \\ \omega_{\mathrm{x}} & 0 & \omega_{\mathrm{z}} & -\omega_{\mathrm{y}} \\ \omega_{\mathrm{y}} & -\omega_{\mathrm{z}} & 0 & \omega_{\mathrm{x}} \\ \omega_{\mathrm{z}} & \omega_{\mathrm{y}} & -\omega_{\mathrm{x}} & 0 \end{bmatrix} x + \begin{bmatrix} q_1 & q_2 & q_3 \\ -q_0 & q_3 & -q_2 \\ -q_3 & -q_0 & q_1 \\ q_2 & -q_1 & -q_0 \end{bmatrix} w, \tag{10}$$

式中: $\omega_{x,}\omega_{\mathrm{y}}, \omega_{\mathrm{z}}$分别表示无人机导航MEMS组件中的三轴陀螺仪测量值, w表示连续状态方程的过程噪声. 对状态方程进行离散化, 同时忽略高阶小量, 得到

$$A_{\mathrm{lin},k} = \begin{bmatrix} 1 & -\dfrac{\omega_{\mathrm{x}}^k \Delta t}{2} & -\dfrac{\omega_{\mathrm{y}}^k \Delta t}{2} & -\dfrac{\omega_{\mathrm{z}}^k \Delta t}{2} \\ \dfrac{\omega_{\mathrm{x}}^k \Delta t}{2} & 1 & \dfrac{\omega_{\mathrm{z}}^k \Delta t}{2} & -\dfrac{\omega_{\mathrm{y}}^k \Delta t}{2} \\ \dfrac{\omega_{\mathrm{y}}^k \Delta t}{2} & -\dfrac{\omega_{\mathrm{z}}^k \Delta t}{2} & 1 & \dfrac{\omega_{\mathrm{x}}^k \Delta t}{2} \\ \dfrac{\omega_{\mathrm{z}}^k \Delta t}{2} & \dfrac{\omega_{\mathrm{y}}^k \Delta t}{2} & -\dfrac{\omega_{\mathrm{x}}^k \Delta t}{2} & 1 \end{bmatrix}, \tag{11}$$

$$W_{\mathrm{lin},k} = \begin{bmatrix} q_1^k & q_2^k & q_3^k \\ -q_0^k & q_3^k & -q_2^k \\ -q_3^k & -q_0^k & q_1^k \\ q_2^k & -q_1^k & -q_0^k \end{bmatrix} \Delta t. \tag{12}$$

建立观测方程如式(13):

$$y = h(x,u) + v = \begin{bmatrix} 2\mathrm{g}(q_1 q_3 - q_0 q_2) \\ 2\mathrm{g}(q_2 q_3 + q_0 q_1) \\ \mathrm{g}(q_0^2 - q_1^2 - q_2^2 + q_3^2) \\ \arctan(-\dfrac{2(q_1 q_2 - q_0 q_3)}{q_0^2 - q_1^2 + q_2^2 - q_3^2}) \end{bmatrix} + u + v, \tag{13}$$

式中: $\mathrm{g} = 9.8\ \mathrm{m/s^2}$表示地球加速度常量, v表示连续观测方程的量测噪声. 离散化观测方程, 得到式(14):

$$H_{\mathrm{lin},k} = \begin{bmatrix} -2\mathrm{g}q_2 & 2\mathrm{g}q_3 & -2\mathrm{g}q_0 & 2\mathrm{g}q_1 \\ 2\mathrm{g}q_1 & 2\mathrm{g}q_0 & 2\mathrm{g}q_3 & 2\mathrm{g}q_2 \\ 2\mathrm{g}q_0 & -2\mathrm{g}q_1 & -2\mathrm{g}q_2 & 2\mathrm{g}q_3 \\ \dfrac{2q_3c_1 + 4q_0c_2}{c_1^2 + 4c_2^2} & \dfrac{-2q_2c_1 - 4q_1c_2}{c_1^2 + 4c_2^2} & \dfrac{-2q_1c_1 + 4q_2c_2}{c_1^2 + 4c_2^2} & \dfrac{2q_0c_1 - 4q_3c_2}{c_1^2 + 4c_2^2} \end{bmatrix}, \tag{14}$$

式中: $c_1 = q_0^2 - q_1^2 + q_2^2 - q_3^2$, $c_2 = q_1 q_2 - q_0 q_3$, $V_{\mathrm{lin},k}$为单位矩阵. 先验估计的初始迭代选用严格对准后姿态解算得到的初始四元数值.

2.2 控制系统(Control system)

针对飞行器建立飞行控制系统架构图如图1所示.

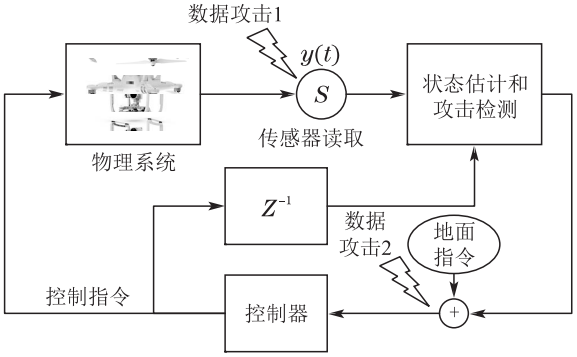


图 1 飞行控制系统架构图

Fig. 1 Framework of flight control system

图1中: Z^{-1}表示得到状态估计需要的上一时刻指令, 飞行控制系统根据任务需求接受地面指令, 完成任务计算和轨迹规划, 跟踪轨迹状态序列计算控制量, 对控制量进行处理和分配, 执行器执行飞行指令. 无人机在执行器作用下完成既定飞行, 将传感器和状态估计得到的位置和姿态信息反馈给控制系统不断修正控制量和轨迹, 完成既定任务. 飞行控制采用PID控制算法, 比例控制实现飞行器状态的稳定, 积分控制用于消除飞行器状态的稳态误差, 微分控制抑制飞行器的震荡, 避免被控量严重超调. PID参数调节根据被控过程飞行器状态的动态响应和稳态误差进行调节. 如图1所示, 针对无人机信息物理系统的数据攻击一般发生在传感器网络和地面指令信道中.

2.3 无人机状态估计攻击模型 (Unmanned aerial vehicle state estimation attack model)

假设攻击者攻击模式采用传感器网络攻击, 通

过控制或者改变传感器读数来对无人机的信息物理系统进行攻击, 考虑3种模式的传感器数据攻击[10]: 1) DoS攻击; 2) 随机攻击; 3) 恶意数据植入攻击.

1) 拒绝服务(DoS)攻击.

拒绝服务攻击是指攻击者通过发送源源不断的数据, 阻塞通信链路, 阻止数据传输来欺骗设备, 造成控制系统无法正常工作. DoS 攻击可以针对传感器数据、控制指令或者两者进行攻击. 在本文中, DoS 攻击认为传感器数据无法被控制系统接收.

2) 随机攻击.

在随机攻击中, 攻击者通过随机发送数据包企图试错绕过中控系统的检测机制从而对传感器发起攻击. 受到攻击后的传感器量测值如式(15)表示:

$$y'_k = h(x'_k, u_k, v_k) + y_{\mathrm{a},k}, \tag{15}$$

式中: $y_{\mathrm{a},k}$表示当前时刻下攻击者产生的随机攻击指令, y'_k和x'_k表示受到攻击后系统的观测量和状态量.

3) 恶意数据植入攻击.

对于恶意数据植入攻击而言, 攻击者已经认知系统模型, 包括系统的状态方程和量测方程的参数以及反馈增益K[17], 攻击者可以控制传感器的特定部分, 从而对控制系统进行特定功能的欺骗, 例如GPS欺骗, 错误航迹引导和姿态改变等. 受到攻击后的传感器量测量如下所示:

$$y'_k = h(x'_k, u_k, v_k) + \tau y_{\mathrm{a},k}, \tag{16}$$

式中: τ=diag$\{\gamma_1, \cdots, \gamma_{\mathrm{m}}\}$表示传感器选择攻击矩阵. 如果传感器受到攻击则$\gamma_i = 1$, 否则$\gamma_i = 0$, $y_{\mathrm{a},k}$表示攻击者的恶意输入数据.

3 攻击检测(Attack detection)

一般的基于卡尔曼滤波的故障检测或者攻击检测利用单步的量测估计值与实际的仪表读数进行比较. 如果这两者的差别超出设定的阈值, 则警报被触发, 从而提醒存在可能的设备故障或者攻击. 在故障检测中应用比较广泛的则是基于卡尔曼滤波的残差卡方检测[18], 在电力系统中也有学者利用此种故障检测的方法来检测传感器网络攻击[11]. 但上述检测方法存在估计精度不高, 检测震荡较大, 误检率较高的问题[19]. 本文采用基于残差新息序列的攻击检测, 通过设置检测滚动时域窗口, 利用窗口内残差信息的统计特性来进行检测, 同时与传统基于残差信息的卡方检测进行对比.

3.1 卡方检测(Chi-square detection)

卡方检测是利用卡尔曼滤波的一种传统检测方法, 通过构造残差信息的卡方分布统计特征值, 并与通过标准卡方表得到的阈值进行比较从而进行检测. 定义时刻k处的残差z_k如下所示:

$$z_k = y_k - h(\hat{x}_k^-, u_k, 0), \tag{17}$$

定义

$$\beta_k = H_{\mathrm{lin},k} P_k^- H_{\mathrm{lin},k}^{\mathrm{T}} + V_{\mathrm{lin},k} R_k V_{\mathrm{lin},k},$$

容易证明z_k的协方差矩阵即为β_k, 此处省略证明. 根据卡方检测, 构造如下标量测试统计量:

$$\vartheta_k = z_k^{\mathrm{T}} \beta_k{}^{-1} z_k^{\mathrm{T}}. \tag{18}$$

如果系统正常工作, 则统计量ϑ_k满足卡方分布, 考虑以下两个假设:

$$\begin{aligned} &H_0:\ \text{无攻击},\\ &H_1:\ \text{攻击发生}. \end{aligned} \tag{19}$$

选择置信度水平

$$P\{\chi^2 > \chi^2_{\alpha,N\times m}\} = \alpha,\ 0 < \alpha < 1, \tag{20}$$

从标准卡方表中根据置信度水平α和自由度$N\times m$确定阈值$\chi^2_{\alpha,N\times m}$, 因此检测决策判断如下:

$$\begin{aligned} &H_0:\ \vartheta_k \leqslant \chi^2_{\alpha,N\times m},\\ &H_1:\ \vartheta_k > \chi^2_{\alpha,N\times m}, \end{aligned} \tag{21}$$

当统计值ϑ_k大于$\chi^2_{\alpha,N\times m}$, 可认为传感器受到攻击.

3.2 新息序列检测(Innovation sequence detection)

上述的卡方检测实际上是一种单点时刻的估计检测, 虽然考虑了之前时刻的状态影响, 但是对于数据传输频率较快的通信链路而言, 容易出现误判情况, 因此需要研究基于新息序列的攻击检测方法, 新息序列为滑动窗口内不断更新的数据序列. 当设置时间窗口$[k, k+1, \cdots, k+n]$, n表示窗口长度, 则位于此时间窗口的残差值$[z_k, z_{k+1}, \cdots, z_{k+n}]$就称作新息序列.

当系统遭受攻击, 式(17)中y_k用y'_k代替, 需要特别说明, 当传感器受到DoS攻击, 则无人机传感器网络相当于出现长时间丢包, 此时后验状态估计与先验估计等价, 即$\hat{x}_k = \hat{x}_k^-$, 此时的状态估计误差协方差矩阵为

$$P_{k+1} = P_{k+1}^- = A_{\mathrm{lin},k} P_k A_{\mathrm{lin},k}^T + W_{\mathrm{lin},k} Q_k W_{\mathrm{lin},k}. \tag{22}$$

在这种情况下, 残差信息不存在. 因此在计算过程中需要进行特殊处理. 考虑其他两种攻击模式, 即随机攻击和恶意数据植入攻击, 当y_k用y'_k代替, 残差z'_k表示为

$$z'_k = h(x'_k, u_k, v_k) + \tau y_{\mathrm{a},k} - h(\hat{x}_k^-, u_k, 0). \tag{23}$$

不失一般性, 仍用z_k表示系统的残差, 则可表示如下:

$$z_k =$$

$$\begin{cases} h(x'_k, u_k, v_k) + \tau y_{\mathrm{a},k} - h(\hat{x}_k^-, u_k, 0), \\ \qquad\qquad \text{如果无DoS攻击;} \\ \text{不存在, 如果DoS攻击发生.} \end{cases} \tag{24}$$

定理 1　攻击模式下基于EKF的系统残差满足零均值高斯分布, 且协方差矩阵β_k满足

$$\beta_k = H_{\mathrm{lin},k} P_k^- H_{\mathrm{lin},k}^{\mathrm{T}} + V_{\mathrm{lin},k} R_k V_{\mathrm{lin},k}. \tag{25}$$

根据式(24)和式(25)的定义, 考虑DoS攻击传感器无法传递数据, 可以假设此时仪表读数为0, 因此y_k=0, 正则化的残差表示如下:

$$e_k = \begin{cases} {\beta_k}^{-\frac{1}{2}} z_k, & \text{如果无DoS攻击,} \\ -{\beta_k}^{-\frac{1}{2}} h(\hat{x}_k^-, u_k, 0), & \text{如果DoS攻击发生.} \end{cases} \tag{26}$$

基于新息序列的检测, 构造标量检测统计量如下:

$$\vartheta_k = \frac{1}{n} \sum_{i=k-n+1}^{k} e_i^{\mathrm{T}} e_i. \tag{27}$$

对于文献 [17] 提及的避开检测机制的恶意数据植入攻击, 使得极限值 $\lim\limits_{t\to\infty} \|x' - x\| = \infty$, $\lim\limits_{t\to\infty} \|y' - y\| \leqslant 1$, 这意味着单点时刻的卡方检测方法可能会失效. 而按照新息序列方法进行攻击检测, 由于检测窗口的存在, 因此更容易通过攻击的后效作用对存在的攻击进行检测, 但会造成检测的延时, 同时延长警报解除的时间. 但两种检测方法都难以对机动过程的传感器数据攻击进行有效检测, 因为机动本身会造成传感器数据的跳变, 从而影响估计. 因此考虑利用卡方检测和新息序列检测的数值差对机动警报进行分离, 对正则化残差取$-\infty$ 范数$\zeta_i = \min|e_i|$作为检测指标, 同样基于新息序列, 构造修正后的标量检测统计量式(28), 检测决策判断与式(21)一致, λ表示松弛系数, 用于调整检测阈值:

$$\vartheta_k = \frac{\lambda}{n} \sum_{i=k-n+1}^{k} \zeta_i. \tag{28}$$

数据攻击检测算法流程图如图2所示.

4　仿真与验证(Simulation and verification)

为验证基于新息序列的检测方法的有效性, 本文选取两种工作模式的四旋翼无人机进行检测: 情形1表示悬停模式下的攻击检测, 情形2表示定高飞行模式下的攻击检测, 攻击模式覆盖前文提及的随机攻击, 恶意数据植入攻击和DoS攻击.

四旋翼无人机的相关物理参数如表1所示. 定高飞行模式下, PID参数选取如表2所示. 选取估计状态误差协方差矩阵$P_k^0 = I_4$, 过程噪声协方差矩阵$Q_k = 1\times10^{-7} I_4$, 测量噪声协方差$R_k = 1\times10^{-5} I_4$, 仿真频率取100 Hz, 误警率$\alpha = 10^{-4}$, 窗口长度n = 100, 即时间长度$t_{\mathrm{w}} = 1$ s, 则警报门限值$\chi^2_{\alpha,N\times m}$ = 15.14; 定高机动状态下, 接受地面指令时刻为t_{sg} = 1.0 s, 攻击发起时间为$t_{\mathrm{a}} = 1.0\ \mathrm{s} \sim 10.0\ \mathrm{s}$.

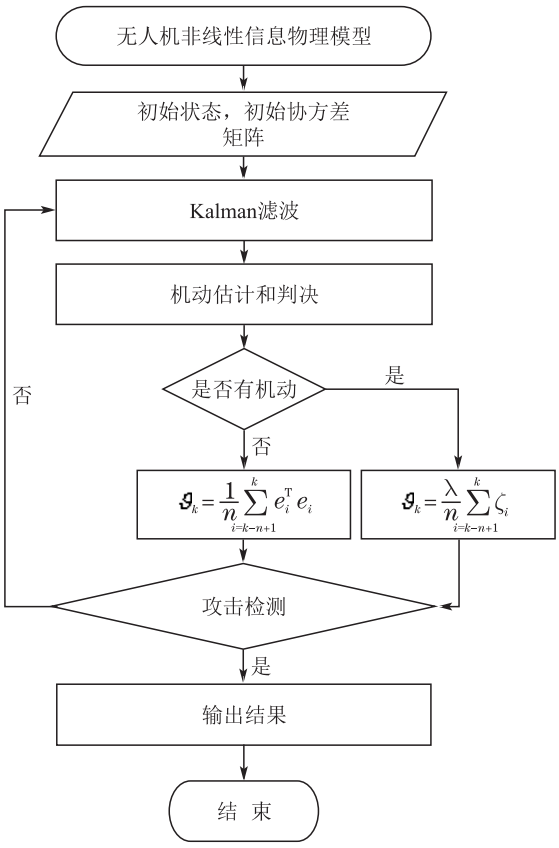


图 2　基于新息序列的无人系统数据攻击检测算法

Fig. 2　Data attacks detection algorithm for unmanned systems based on innovation sequence

表 1　四旋翼飞行器参数

Table 1　Quadrotor parameters

参数	数值	参数	数值
m/kg	0.25	$I_{\mathrm{x}}\times10^{-2}/(\mathrm{kg}\cdot\mathrm{m}^2)$	3.31
l/m	30.4	$I_{\mathrm{y}}\times10^{-2}/(\mathrm{kg}\cdot\mathrm{m}^2)$	3.31
$k_{\mathrm{t}}\times10^{-5}/((\mathrm{N}\cdot\mathrm{s}^2)\cdot\mathrm{m}^{-2})$	3.13	$I_{\mathrm{z}}\times10^{-2}/(\mathrm{kg}\cdot\mathrm{m}^2)$	6.12
$k_{\mathrm{d1}}\times10^{-6}/((\mathrm{N}\cdot\mathrm{s}^2)\cdot\mathrm{m}^{-2})$	3.15	$k_{\mathrm{d2}}\times10^{-4}/((\mathrm{N}\cdot\mathrm{s}^2)\cdot\mathrm{m}^{-2})$	7.51

表 2　各通道PID参数

Table 2　PID controller parameters

通道	K_{P}	K_{I}	K_{D}
垂直高度通道	2	0.01	1.0
滚转通道	2	6.00	0.1
俯仰通道	3	0.01	1.0
偏航通道	2	8.00	0.1

4.1 悬停模式攻击检测(Hover mode attack detection)

3种类型传感器网络数据攻击的卡方检测结果如图3−5所示: g表示单点时刻卡方检测统计量, gin表示新息序列估计的检测统计量. 蓝色实线表示传感器的值, 包括加速度计的3个分量和航向角; 上方蓝色实线表示加速度垂直分量(z方向); 下方蓝色线表示加速度计水平前向分量和侧向(x方向和y方向)以及航向角; 红色虚线表示对应状态估计量.

1) 随机攻击.

随机攻击取攻击指令$y_{\mathrm{a},k}=1.0\,\mathrm{rand}(\cdot)$, $\mathrm{rand}(\cdot)$由MATLAB产生, 攻击频率与仿真频率一致, 上分图表示状态估计结果, 下分图表示检测状态. 针对传感器的随机数据攻击, 攻击发起时间从$t_{\mathrm{a}}=1.0$ s开始. 图3显示新息序列检测相比卡方检测延迟时间$t_{\mathrm{lag}}=0.2$ s, 卡方检测在攻击初始检测概率达到峰值, 且震荡较大, 警报频繁触发解除, 因此不能准确反映攻击状况. 而新息序列检测存在一定延时之后始终使得警报处于触发状态, 且检测概率基本维持恒定.

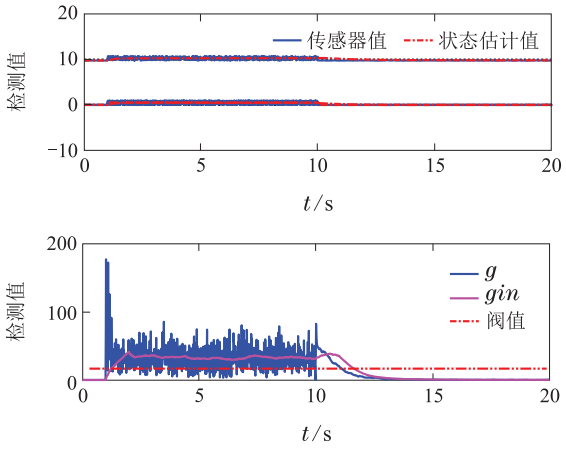
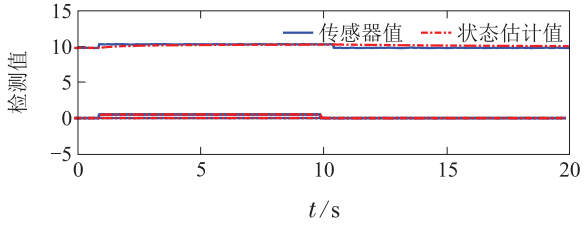


图 3 随机攻击的攻击检测

Fig. 3 Attack detection of random attacks

2) 恶意数据植入攻击.

恶意数据取攻击指令$y_{\mathrm{a},k}=[0.5\ \ 0.5\ \ 0.5\ \ 0.0]^{\mathrm{T}}$. 检测响应如图4所示. 针对传感器的恶意数据攻击, 同样新息序列检测存在一定的时延现象, 且检测概率有所下降. 在攻击中段, 两种检测方法都无法准确检测到数据攻击, 在攻击解除后反而触发警报, 出现误警.



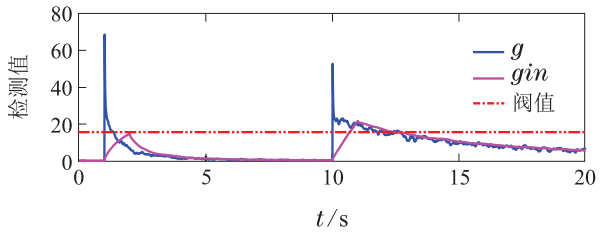


图 4 恶意数据攻击的攻击检测

Fig. 4 Attack detection of false data attacks

3) DoS攻击.

DoS攻击中根据前文假设传感器数据无法传输, 则传感器接收输入数据为零. 检测曲线如图5所示.

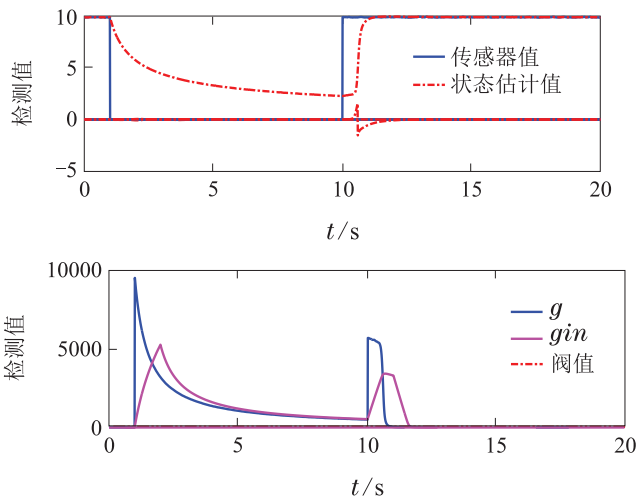


图 5 DoS攻击的攻击检测

Fig. 5 Attack detection of DoS attacks

从仿真结果看基于EKF的状态估计能以较快速度对四旋翼的量测状态进行估计, 传统的卡方检测对传感器的攻击和变化尤为敏感, 因此容易受外界干扰, 使得检测准确度大大降低. 而基于新息序列的检测机制更容易反映攻击特性, 但存在一定程度的延时, 与前文分析结果一致. 图4显示, 卡方检测和新息序列检测方法都能以特定设计的恶意数据避开检测, 因此如果攻击者掌握足够的系统信息对控制系统发起恶意数据植入攻击, 检测方法难以真正有效地对攻击进行检测, 这与文献[11]的结果一致. 对于DoS攻击, 数据异常较为明显, 因此两种检测机制都更容易检测到数据攻击.

4.2 机动模式攻击检测(Motion mode attack detection)

定高机动模式, 控制器控制飞行器飞行至定高1 m高度, 攻击发生在指令执行中, 即攻击发生在飞行器执行定高飞行过程中, 响应曲线如图6所示. 图7–10表示采用未判断机动的新息序列数据攻击检测方法的检测情况. 图11表示判断机动后的新息序列

范数修正检测方法的检测情况. 图7显示即使传感器未遭受攻击, 攻击警报仍被触发, 且卡方检测对无人机的机动尤为敏感[20]. 图8–9显示在悬停模式下能明显影响飞行器状态的攻击方式在机动模式下已难以体现. 图10 显示DoS攻击效果明显, 较易识别.

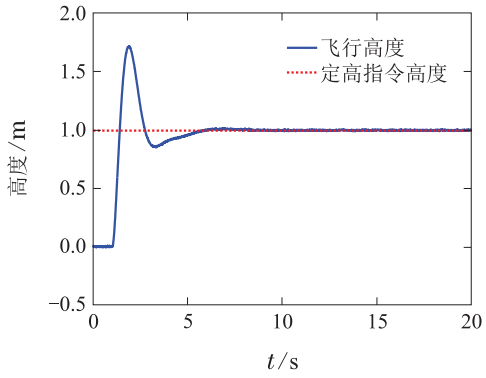


图 6　飞行器高度时间响应曲线

Fig. 6　Response profile of flight altitude with time

1) 传感器未遭受攻击. 如图7所示.

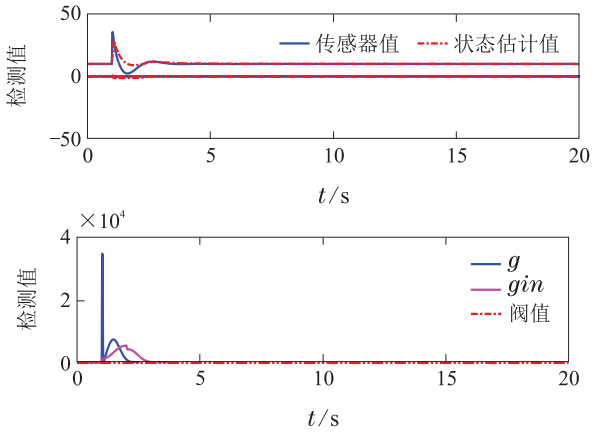


图 7　机动模式飞行器未受攻击的攻击检测

Fig. 7　Attack detection with no attack in motion mode

2) 随机攻击. 如图8所示.

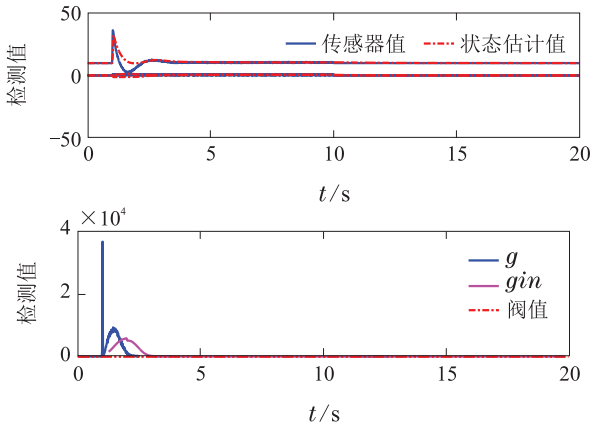


图 8　机动模式下随机攻击的攻击检测

Fig. 8　Detection of random attack in motion mode

3) 恶意数据植入攻击. 如图9所示.

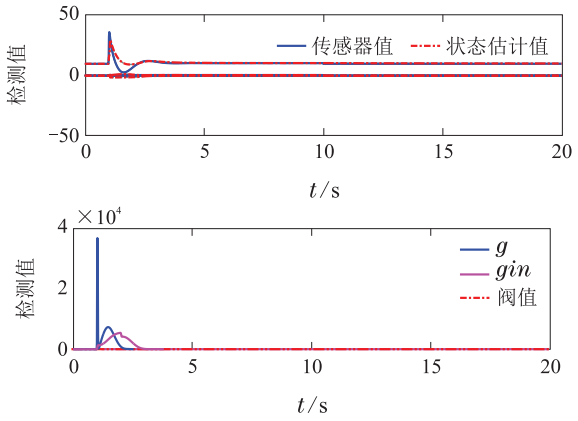


图 9　机动模式下恶意数据植入攻击的攻击检测

Fig. 9　Detection of false data attack in motion mode

4) DoS攻击. 如图10–11所示.

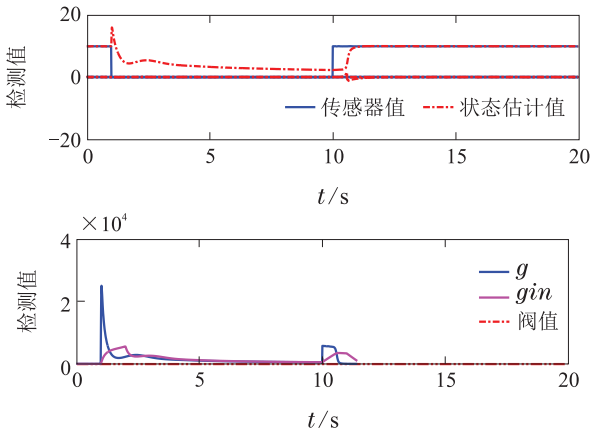


图 10　机动模式下DoS攻击的攻击检测

Fig. 10　Detection of DoS attack in motion mode

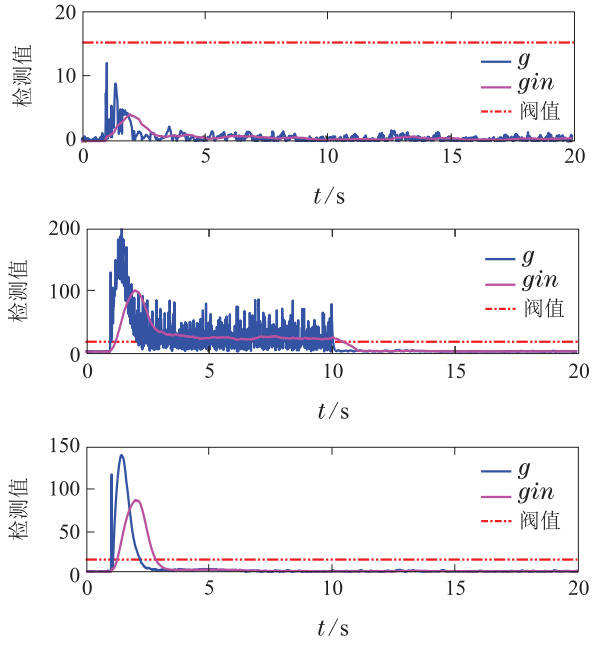


图 11　采用$-\infty$范数的新息序列检测方法

Fig. 11　Detection with innovation sequence method applying the $-\infty$ norm

仿真结果显示, 未经修正的卡方检测和新息序列检测都无法准确检测机动状况下的传感器数据攻击. 而修正后的检测方法能分离机动检测与数据攻击, 同时对存在的数据攻击进行有效检测. 新息序列经平均处理相比单点卡方检测更为稳定, 同样存在一定时间滞后, 但不影响检测结果.

5 结论(Conclusions)

本文研究分析了无人机控制系统状态估计中数据攻击带来的安全威胁, 提出了新息序列驱动的无人机控制系统数据攻击的检测方法. 以四旋翼无人机为例, 研究了悬停和机动两种飞行模式下的攻击检测, 攻击类型包括随机攻击、恶意数据植入攻击和拒绝服务攻击. 仿真实验结果表明, 本文新息序列驱动的数据攻击检测方法能对无人机控制系统状态估计的数据攻击进行有效的检测, 相比单点时刻的卡方攻击检测, 能有效消除野值和干扰带来的影响, 同时利用范数修正后的机动检测方法有效分离机动检测和数据攻击检测, 降低数据攻击检测的误检率.

参考文献(References):

[1] SAMPIGETHAYA K, POOVENDRAN R. Cyber-physical integration in future aviation information systems [C] //*IEEE/AIAA 31st Digital Avionics Systems Conference (DASC)*. VA: IEEE, 2012, 225: 7C2-1 – 7C2-12.

[2] WEIMERSKIRCH A. Automotive and industrial data security [R]. *ESCRYPT Inc. Report*. Ann Arbor, MI, USA, 2012.

[3] LIU Wei, FENG Bingwen, WEN Jian. Survey on research of mini-drones security [J]. *Chinese Journal of Network and Information Security*, 2016 , 2(3): 39 – 45.
(刘炜, 冯丙文, 翁建. 小型无人机安全研究综述 [J]. 网络与信息安全学报, 2016, 2(3): 39 – 45.)

[4] JAVAID A Y, SUN W, DEVABHAKTUNI V K, et al. Cyber security threat analysis and modeling of an unmanned aerial vehicle system [C] //*Proceedings of the IEEE Conference on Technologies for Homeland Security*. Piscataway, NJ: IEEE, 2013, 43(4): 585 – 590.

[5] 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): 1 – 19.

[6] RANI C, MODARES H, SRIRAM R, et al. Security of unmanned aerial vehicle systems against cyber-physical attacks [J]. *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*, 2016, 13(3): 331 – 342.

[7] LINDQVIST J, AURA T, DANEZIS G, et al. Privacy-preserving 802.11 access-point discovery [C] //*Proceedings of the Second ACM Conference on Wireless Network Security*. Zurich: ACM, 2009: 123 – 130.

[8] HASHMI M J, SAXENA M, SAINI D R. Classification of DDoS attacks and their defense techniques using intrusion prevention system [J]. *International Journal of Computer Science & Communication Networks*, 2012, 2(5): 607 – 614.

[9] DEPREN O, TOPALLAR M, ANARIM E, et al. An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks [J]. *Expert Systems with Applications*, 2005, 29(4): 713 – 722.

[10] SEAH C E, HWANG I. Stochastic linear hybrid system: modeling, estimation, application in air traffic control [J]. *IEEE Transactions on Control System Technology*, 2009, 17(3): 563 – 575.

[11] KEBINA M, CAO X J, HU F, et al. Detection of faults and attacks including false data injection attack in smart grid using kalman filter [J]. *Control of Network Systems IEEE Transactions on Control of Network Systems*, 2013, 1(4): 370 – 379

[12] SHI L, MICHAEL E, MURRAY R. Kalman filtering over a packet-dropping network: a probabilistic perspective [J]. *IEEE Transactions on Automatic Control*, 2010, 55(3): 594 – 604.

[13] HU J, WANG C, DONG X. Fault detection for nonlinear discrete-time systems via deterministic learning [J]. *Control Theory and Technology*, 2016, 14(2): 159 – 175.

[14] FAWZI H, TABUADA P, DIGGAVI S. Secure state-estimation for dynamical systems under active adversaries [J]. *IEEE Transactions on Automatic Control*, 2011, 3(1): 337 – 344.

[15] LIU W Y, HWANG I. On hybrid state estimation for stochastic hybrid systems [J]. *IEEE Transactions on Automatic Control*, 2014, 59(10): 2615 – 2628.

[16] KHALIL H K. *Nonlinear Systems* [M]. 3rd ed. Upper Saddle River, NJ: Prentice Hall, 2002: 423 – 459.

[17] MO Y, SINOPOLI B. False data injection attacks in control systems [C] //*Proceedings of the 1st Workshop Secure Control System*. Stockholm, Sweden: [s.n.], 2010: 1 – 6.

[18] BRUMBACK B D, SRINATHA M D. Chi-square test for fault-detection in Kalman filters [J]. *IEEE Transactions on Automatic Control*, 1987, 32(6): 552 – 554.

[19] SHENG Hu, LI Xiaoming, QI Jianwen, et al. Input estimation algorithm based on modification of innovation sequence for maneuvering target tracking [J]. *Systems Engineering and Electronics*, 2009, 31(9): 2121 – 2124.
(盛琥, 李晓明, 齐建文, 等. 基于新息序列修正的输入估计算法 [J]. 系统工程与电子技术, 2009, 31(9): 2121 – 2124.)

[20] WOLF W. Key frame selection by motion analysis [C] //*IEEE International Conference on Acoustics, Speech, and Signal Processing*. Atlanta: IEEE, 1996, 2(2): 1228 – 1231.

作者简介:

肖佳平 (1991–), 男, 硕士研究生, 目前研究方向为导航与制导技术、最优控制和信息物理系统, E-mail: xjpmail@buaa.edu.cn;

蒋建春 (1971–), 男, 博士, 副研究员, 目前研究方向为网络信息安全和信息物理系统安全, E-mail: jianchun@nfs.iscas.ac.cn;

佘春东 (1971–), 男, 教授, 硕士生导师, 目前研究方向为移动互联网和通信网络及安全, E-mail: scd@bupt.edu.cn.