doi: 10.3969/j.issn.0490-6756.2020.05.009

基于主动弹性防御策略的网络控制系统零动态攻击检测

蒲在毅, 张咏梅, 贾艳梅
(西华师范大学, 南充 637009)

摘 要: 研究了一种适用于零动态攻击的网络控制系统(NCSs)的弹性控制策略,基于控制输入和测量数据设计的隐式虚假数据注入攻击. 当网络化控制系统的控制信号受到网络攻击时,根据被动模型的故障检测和隔离方案,发现在攻击过程中,对设备状态变量的零动态攻击的结果是不可检测的,但在攻击结束后会变得明显. 对此,利用广义似然比检测器的主动版本给出的信息在线更新卡尔曼滤波器,设计了一种具有快速恢复攻击端后闭环系统行为能力的弹性线性二次高斯控制器. 实验结果显示,所提算法明显具有更高的攻击检测质量,并具有更佳的计算效率和内存利用效率,验证了算法有效性.

关键词: 弹性防御; 网络控制系统; 零动态; 攻击控制; 卡尔曼滤波
中图分类号: TP391.9 **文献标识码**: A **文章编号**: 0490-6756(2020)05-0879-08

Zero dynamic attack detection of network control systems based on active elastic defense strategy

PU Zai-Yi, ZHANG Yong-Mei, JIA Yan-Mei
(China West Normal University, Nanchong 637009, China)

Abstract: In this paper, an elastic control strategy for network control systems (NCSs) with zero dynamic attacks is studied, in which an implicit false data injection attack is designed based on input control and data measurement. When the control signal of networked control system is attacked by network, according to the fault detection and isolation scheme of passive model, it is found that the result of zero dynamic attack on device state variables is undetectable during the attack process, but it will become obvious after the attack. To solve this problem, an Elastic Linear Quadratic Gauss Controller (ELQGC) with the ability to quickly recover the behavior of the closed-loop system at the attack end is designed by using the information provided by the active version of the Generalized Likelihood Ratio Detector (GLR) to update the Kalman filter online. The experimental results show that the proposed algorithm has significantly higher attack detection quality, better computational efficiency and memory utilization efficiency, which demonstrate the effectiveness of the algorithm.

Keywords: Resilient defense; Networked control system; Zero dynamics; Attack control; Kalman filter

收稿日期: 2019-05-02
基金项目: 西华师范大学英才基金(17YC497)
作者简介: 蒲在毅(1974-), 男, 四川渠县人, 硕士, 副教授, 研究方向为网络安全. E-mail: zaiyipu1@126.com

1 引 言

网络控制系统是由执行器、传感器和控制器组成的空间分布系统,其通过通信网络上的信息交换进行协调控制. 运输系统、电力系统、化学工艺、水和天然气分配网络、制造和运输网络可被视为网络物理系统(Cyber Physical Systems,CPSs)应用领域示例. CPS 是通信能力、计算资源和物理过程的集成. 此类系统通常被视为大规模分布式物理过程,可通过使用对各种基础设施中的系统运行至关重要的监控和数据采集(Supervisory Control And Data Acquisition,SCADA)软件进行监控.

考虑到网络控制系统包丢失和包延迟影响的控制系统设计,NCS 还容易受到网络物理攻击的影响. 文献[1]指出当攻击者阻止控制器接收传感器测量或设备接收控制律时,需要高度重视网络控制系统的拒绝服务(Denial of Service,DoS)攻击. 文献[2]指出当攻击者发送关于传感器或执行器的虚假信息时,会引入欺骗攻击. 文献[3]讨论了当攻击者产生人工测量延迟时的重放攻击问题. 文献[4]通过故障检测和隔离(Fault Detection and Isolation,FDI)技术,考虑了接近传统故障的直接物理攻击问题. CPSs 中的协同攻击检测问题似乎与传统的基于模型的 FDI 方案中的多部件、传感器或执行器故障检测问题密切相关,但也存在多个故障可能被认为是一种随机发生在执行器、传感器或通信通道上的现象. 对此,文献[5]提出一种网络攻击检测自适应决策模型(Concept-adpting Very Fast Decision Tree,CVFDT),通过参数自适应过程简化算法设定,具有更广泛的适应性,但是参数自适应过程具有一定随机性,精度受到影响且资源占用较高;文献[6]提出一种网络攻击检测动态概率标记模型(Dynamic Probabilistic Packet Marking,DPPM),将网络的攻击行为简化为一个概率模型,简化了模型表达形式,但是计算精度不高;文献[7]提出一种网络攻击检测快速决策模型(Very Fast Decision Tre,VFDT),提高检测效率,但是检测精度相对较差.

本文研究了利用几何控制理论中的输出置零控制不变子空间设计的一种特殊的隐蔽攻击,即零动态攻击. 当攻击者和防御者都考虑同一个设备模型时,检测攻击的唯一机会是假设存在防御行动,迫使攻击者在有限的时间内执行恶意活动,并将有限长时间零动态攻击下的网络物理系统表示为两个连续脉冲作用下的线性时不变系统,提出事件检测的广义似然比(Generalized Likelihood Ratio,GLR)[8]主动测试版本.

2 网络控制系统的零动态攻击模型描述

2.1 控制系统模型

在本节中,我们提出了由物理设备和通信网络、线性二次高斯(Linear-Quadratic-Gaussian,LQG)控制器和异常检测器描述的网络控制系统中的网络/物理攻击检测问题[9],如图 1 所示.

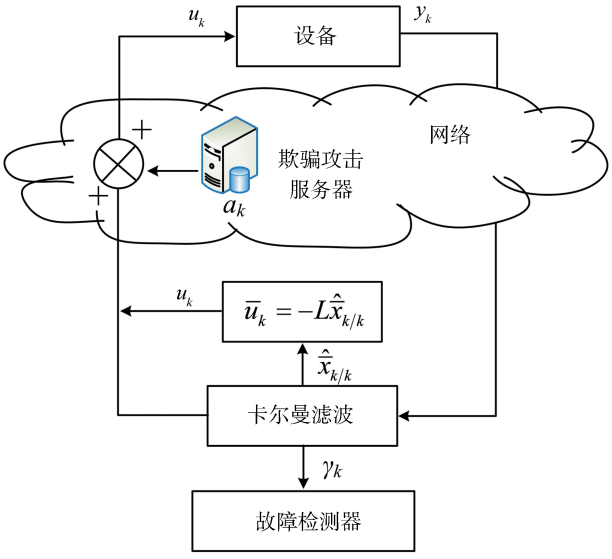

图 1 受 LQG 控制器攻击的网络控制系统

Fig. 1 Network control system attacked by LQG controller

如图 1 所示,受 LQG 控制器攻击的网络控制系统可由以下线性离散时间随机系统表示.

$$x_{k+1}=Ax_k+Bu_k+w_k \tag{1}$$

$$y_k=Cx_k+\varepsilon_k \tag{2}$$

式中,$x_k\in R^n$,$u_k\in R^q$ 和 $y_k\in R^m$ 是状态、输入和测量向量,$w_k\in R^n$ 和 $\varepsilon_k\in R^m$ 是零均值不相关高斯随机序列:

$$E\left\{\begin{bmatrix}\omega_k\\ \varepsilon_k\end{bmatrix}\begin{bmatrix}\omega_j\\ \varepsilon_j\end{bmatrix}^T\right\}=\begin{bmatrix}W & 0\\ 0 & V\end{bmatrix}\delta_{k,j} \tag{3}$$

其中,$W>0$,$V>0$. 假定初始状态 x_0 与 ω_k 和 ε_k 不相关,是高斯随机变量,且有

$$\begin{cases}E\{x_0\}=\bar{x}_0\\ P_0=E\{(x_0-\bar{x}_0)(x_0-\bar{x}_0)^T\}\end{cases} \tag{4}$$

对于所有的 z,状态对(A,C)是可检测的,状态对(A,B)是可稳定的,且有

$$\operatorname{rank}\left(\begin{bmatrix} Iz-A & -B \\ C & 0 \end{bmatrix}\right)=n+q \tag{5}$$

在无攻击情况下($u_k=\bar{u}_k$)，控制器观测到的设备模型描述如下.

$$\begin{cases} \bar{x}_{k+1}=A\bar{x}_k+B\bar{u}_k+w_k \\ y_k=C\bar{x}_k+\varepsilon_k \end{cases} \tag{6}$$

由此可得，网络控制系统的线性二次高斯控制律可定义为

$$J=\min\lim_{T\to\infty}E\left\{\frac{1}{T}\left[\sum_{k=0}^{T-1}\bar{x}_k^TQ\bar{x}_{k_k}+\bar{u}_k^TR\bar{u}_k\right]\right\} \tag{7}$$

其中，线性二次高斯控制器设计参数 $Q\geqslant 0$ 和 $R>0$ 由下式给出.

$$\bar{u}_k=-L\hat{\bar{x}}_{k/k} \tag{8}$$

其中，

$$\begin{cases} L=(B^TSB+R)^{-1}B^TSA \\ S=A^TSA+Q-A^TSB(B^TSB+R)^{-1}B^TSA \end{cases} \tag{9}$$

其中，$\hat{\bar{x}}_{k/k}$是由卡尔曼滤波器产生的无攻击下的最小方差无偏状态估计，且有

$$\begin{cases} \hat{\bar{x}}_{k/k}=\hat{\bar{x}}_{k/k-1}+K_k(y_k-C\hat{\bar{x}}_{k/k-1}) \\ \bar{P}_{k/k}=(I-K_kC)\bar{P}_{k/k-1}(I-K_kC)^T+K_kVK_k^T \\ K_k=\bar{P}_{k/k-1}C^T({}^C\bar{P}_{k/k-1}C^T+V)^{-1} \\ \hat{\bar{x}}_{k+1/k}=A\hat{\bar{x}}_{k/k}+\bar{B}u_k \\ \bar{P}_{k+1/k}=A\bar{P}_{k/k}A^T+W \end{cases} \tag{10}$$

式中，$\hat{\bar{x}}_{0/-1}=\bar{x}_0$，$\bar{P}_{0/-1}=P_0$. 为简化，假设网络设备有一个真正的不稳定不变零参数 λ，且有：

$$\operatorname{rank}\left(\begin{bmatrix} I\lambda-A & -B \\ C & 0 \end{bmatrix}\right)=n+q-1 \tag{11}$$

式中，$|\lambda|>1$，$\lambda\notin sp(A)$. $sp(A)$表示 A 的特征值. 错误的数据注入 a_k 会对设备造成灾难性的破坏，而从卡尔曼滤波器生成序列 $\gamma_k=y_k-C\hat{\bar{x}}_{k/k-1}$的标准 FDI 方案中无法检测到[10].

2.2　零动态攻击模型

假设恶意代理可在入侵时间 k_0 实现特定的欺骗攻击 a_k，称为对控制信号的零动态攻击. 假设为了计算适当的攻击策略，攻击者可以访问系统的详细模型. 在欺骗攻击中，攻击者试图阻止执行器或传感器接收数据完整性. 其目的是通过从控制器或传感器发送错误信息，从实际值修改控制信号或传感器测量值. 错误信息可能是错误的发送者身份、错误的传感器测量、错误的控制输入或观察到测量时的不正确时间[11-12].

攻击者将假数据序列 $a_k\neq 0$，$\forall k\geqslant k_0$ 添加到控制器发送到设备的控制信号上时，设备接收控制信号为 $u_k=\bar{u}_k+a_k$，控制器观测到的设备模型变为

$$\begin{cases} x_{k+1}=Ax_k+B\bar{u}_k+Ba_k+w_k \\ y_k=Cx_k+\varepsilon_k \end{cases} \tag{12}$$

假定不受攻击的网络设备模型表示为：$x_k=\bar{x}_k+\Delta x_k^a$ 和 $y_k=C\bar{x}_k+\Delta y_k^a$，其中攻击的附加效果 Δx_k^a 和 Δy_k^a，可表示为

$$\begin{cases} \Delta x_{k+1}^a=A\Delta x_k^a+Ba_k \\ \Delta y_k^a=C\Delta x_k^a \end{cases} \tag{13}$$

式中，$\Delta x_{k_0}^a=0$. 当攻击者知道设备的状态模型时，可以从以下自治系统中设计一种特定的欺骗攻击 $a_k=-\sum\Delta\bar{x}_k^a$，称为零动态攻击.

$$\begin{cases} \Delta\bar{x}_{k+1}^a=(A-B\sum)\Delta\bar{x}_k^a, \\ \Delta\bar{y}_k^a=C\Delta\bar{x}_k^a \end{cases} \tag{14}$$

利用 Δx_k^a 近似值 $\Delta\bar{x}_k^a$ 进行模型初始化. 攻击者隐身策略包括确定$\sum$以便对于$\forall k\geqslant k_0$，存在下式.

$$\Delta\bar{y}_k^a=0,\lim_{k\to\infty}|\Delta x_k^a|\to\infty \tag{15}$$

式中，$\Delta\bar{x}_{k_0}^a$ 接近于 0. 结合式(11)，存在 ξ 和 g 的解，使得下式成立.

$$\begin{bmatrix} I\lambda-A & -B \\ C & 0 \end{bmatrix}\begin{bmatrix} \xi \\ g \end{bmatrix}=0\Leftrightarrow$$

$$\begin{bmatrix} I\lambda-(A-B\sum) & -B \\ C & 0 \end{bmatrix}\begin{bmatrix} \xi \\ g-\sum\xi \end{bmatrix}=0 \tag{16}$$

基于 $g=\sum\varepsilon$，利用式(16)可得$(A-B\sum)\xi=\lambda\xi$，$C\xi=0$，表明不变零参数 λ 成为不可观测的成对模式$(A-B\sum,C)$.

2.3　被动攻击检测方案

提出一种被动攻击检测方案，利用卡尔曼滤波器的创新序列设计的异常检测器来实现网络攻击防御. 定义 $d\delta_{k,k_0-1}$作为时刻 k_0-1 触发的 d 尺寸脉冲，其中 $\delta_{k,k_0-1}=0$、$\forall k\neq k_0-1$、$\delta_{k,k_0-1}=1$，对于 $k=k_0-1$，攻击模型(14)可改为

$$\begin{cases} \Delta\bar{x}_{k+1}^a=(A-B\sum)\bar{x}_k^a+\xi d\delta_{k,k_0-1} \\ \Delta\bar{y}_k^a=C\Delta\bar{x}_k^a \end{cases} \tag{17}$$

其中，$\Delta\bar{x}_{k_0-1}^a=0$. 基于式(17)和 $a_k=-\sum\Delta\bar{x}_k^a$ 可得出受攻击设备的增强状态模型为

$$\begin{bmatrix} x_{k+1} \\ \Delta\bar{x}_{k+1}^a \end{bmatrix}=\begin{bmatrix} A & -B\sum \\ 0 & A-B\sum \end{bmatrix}\begin{bmatrix} x_k \\ \Delta\bar{x}_k^a \end{bmatrix}+$$

$$\begin{bmatrix} B \\ 0 \end{bmatrix}\bar{u}_k+\begin{bmatrix} 0 \\ \xi \end{bmatrix}d\delta_{k,k_0-1}+\begin{bmatrix} I \\ 0 \end{bmatrix}\omega_k \tag{18a}$$

$$y_k=[C\quad 0]\begin{bmatrix}x_k\\ \Delta x_k^a\end{bmatrix}+\varepsilon_k \tag{18b}$$

通过设定$\begin{bmatrix}\bar{x}_k\\ \Delta\bar{x}_k^a\end{bmatrix}=T\begin{bmatrix}x_k\\ \Delta\bar{x}_k^a\end{bmatrix}$和$T=\begin{bmatrix}I & -I\\ 0 & I\end{bmatrix}$,可得模型形式为

$$\begin{bmatrix}\bar{x}_{k+1}\\ \Delta\bar{x}_{k+1}^a\end{bmatrix}=\begin{bmatrix}A & 0\\ 0 & A-B\sum\end{bmatrix}\begin{bmatrix}x_k\\ \Delta\bar{x}_k^a\end{bmatrix}+\begin{bmatrix}B\\ 0\end{bmatrix}\bar{u}_k+\begin{bmatrix}-\xi\\ \xi\end{bmatrix}d\delta_{k,k_0-1}+\begin{bmatrix}I\\ 0\end{bmatrix}\omega_k \tag{19a}$$

$$y_k=[C\quad C]\begin{bmatrix}x_k\\ \Delta\bar{x}_k^a\end{bmatrix}+\varepsilon_k \tag{19b}$$

根据$C\Delta\bar{x}_k^a=0$、$\Delta\bar{x}_k^a=d\xi\lambda^{k-k_0}$以及$C\xi=0$,公式(19)所示状态空间模型中$\Delta\bar{x}_k^a$是不可观测的,且$\bar{x}_k$的进化公式为

$$\begin{cases}\bar{x}_{k+1}=A\bar{x}_k+B\bar{u}_k-\xi d\delta_{k,k_0-1}+\omega_k\\ y_k=C\bar{x}_k+\varepsilon_k\end{cases} \tag{20}$$

如果攻击者选择接近零的d,并与不稳定特征值相关的特征向量ξ正交,则无法从卡尔曼滤波器的创新序列$\gamma_k=y_k-C\hat{\bar{x}}_{k/k-1}$上设计的异常检测器检测到脉冲$d\delta_{k,k_0-1}$.

3 弹性防御策略

3.1 零动态攻击检测

对 LQG 控制器产生的控制信号进行弹性防御策略注入,可以作用于 NCS 的状态变量,而对应

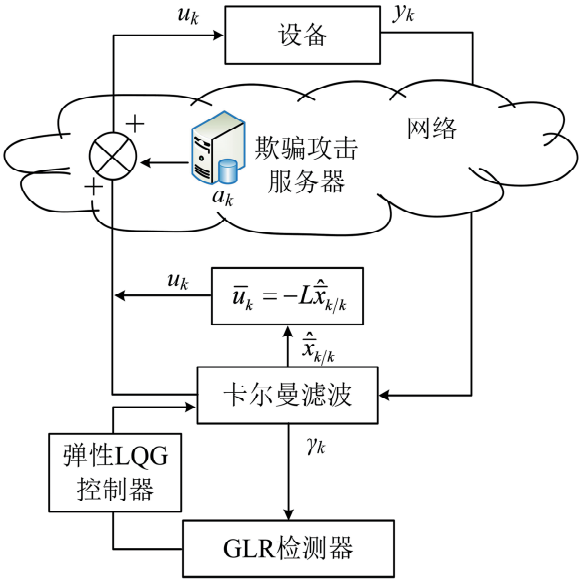

图 2 基于弹性 LQG 控制器的 NCS 攻击

Fig. 2 NCS attack based on elastic LQG controller

用于卡尔曼滤波器创新序列的任何被动检测器都不可检测[13]. 在本节中,我们给出了一个主动攻击检测方案,以揭示零动态攻击的存在,并研究了防御者可用于快速恢复 NCS 正常行为的弹性控制策略,见图 2.

当攻击在入侵时间k_f停止时,a_k的后果可以描述为

$$\Delta\bar{x}_{k+1}^a=A\Delta\bar{x}_k^a,\ \Delta\bar{y}_k^a=C\Delta\bar{x}_k^a \tag{21}$$

式中,$\Delta\bar{x}_{k_f}^a=d\xi\lambda^{k_f-k_0-1}$,$\Delta\bar{x}_{k_f-1}^a=0$. 根据$\upsilon\delta_{k,k_f-1}$以及$\upsilon=d\lambda^{k_f-k_0-1}$,公式(21)等价于下式.

$$\begin{cases}\Delta\bar{x}_{k+1}^a=A\Delta\bar{x}_k^a+\xi\upsilon\delta_{k,k_f-1}\\ \Delta\bar{y}_k^a=C\Delta\bar{x}_k^a\end{cases} \tag{22}$$

假设d接近零,用式(19)代替式(22),控制器$\forall k>k_f$的设备观测模型变成下式.

$$\begin{bmatrix}\bar{x}_{k+1}\\ \Delta\bar{x}_{k+1}^a\end{bmatrix}=\begin{bmatrix}A & 0\\ 0 & A\end{bmatrix}\begin{bmatrix}\bar{x}_k\\ \Delta\bar{x}_k^a\end{bmatrix}+\begin{bmatrix}B\\ 0\end{bmatrix}\bar{u}_k+\begin{bmatrix}0\\ \xi\end{bmatrix}\upsilon\delta_{k,k_f-1}+\begin{bmatrix}I\\ 0\end{bmatrix}\omega_k \tag{23a}$$

$$y_k=[C\quad C]\begin{bmatrix}\bar{x}_k\\ \Delta\bar{x}_k^a\end{bmatrix}+\varepsilon_k \tag{23b}$$

基于$\begin{bmatrix}x_k\\ \Delta\bar{x}_k^a\end{bmatrix}=T^{-1}\begin{bmatrix}\bar{x}_k\\ \Delta\bar{x}_k^a\end{bmatrix}$,$T^{-1}=\begin{bmatrix}I & I\\ 0 & I\end{bmatrix}$,网络设备的增广状态模型参考(23)改写为

$$\begin{bmatrix}x_{k+1}\\ \Delta\bar{x}_{k+1}^a\end{bmatrix}=\begin{bmatrix}A & 0\\ 0 & A\end{bmatrix}\begin{bmatrix}x_k\\ \Delta\bar{x}_k^a\end{bmatrix}+\begin{bmatrix}B\\ 0\end{bmatrix}\bar{u}_k+\begin{bmatrix}\xi\\ \xi\end{bmatrix}\upsilon\delta_{k,k_f-1}+\begin{bmatrix}I\\ 0\end{bmatrix}\omega_k \tag{24a}$$

$$y_k=[C\quad 0]\begin{bmatrix}x_k\\ \Delta\bar{x}_k^a\end{bmatrix}+\varepsilon_k \tag{24b}$$

可简化为

$$\begin{cases}x_{k+1}=Ax_k+B\bar{u}_k+\xi\upsilon\delta_{k,k_f-1}+\omega_k\\ y_k=Cx_k+\varepsilon_k\end{cases} \tag{25}$$

基于$|\lambda|>1$(以$d\lambda^T$为上界),$\upsilon\delta_{k,k_f-1}$的尺寸$\upsilon=d\lambda^{k_f-k_0-1}$大于$d\delta_{k,k_0-1}$的尺寸$d$,并且脉冲$\upsilon\delta_{k,k_f-1}$现在有机会从异常检测器中检测到. 当设备模型从式(20)切换到式(25)时,基于主动模型的 FDI 方案可表示为

$$\begin{aligned}x_{k+1}&=Ax_k-B\bar{u}_k+\xi\upsilon\delta_{k,k_f-1}+\omega_k\\ y_k&=Cx_k+\varepsilon_k\end{aligned} \tag{26}$$

状态预测误差$e_{k/k-1}=x_k-\hat{x}_{k/k-1}$和卡尔曼滤波器输出$\gamma_k=y_k-C\hat{x}_{k/k-1}$可表示为

$$e_{k/k-1}=x_k-\hat{x}_{k/k-1},\ \gamma_k=y_k-C\hat{x}_{k/k-1} \tag{27}$$

式中,当$1<l\leqslant\tau$时,因为$\lambda>1$,则$\upsilon\delta_{k,k_f-1}$是未知

尺寸的脉冲. 脉冲 $d\delta_{k,k_f-1}$ 在 d 接近零的情况下选择不可检测，下一节建议从应用于卡尔曼滤波器创新序列的 GLR 检测器检测 $\upsilon\delta_{k,k_f-1}$. 为了避免多次检测 $\upsilon\delta_{k,k_f-1}$，卡尔曼滤波器将根据检测到的事件进行在线更新. 第二节 LQG 控制器的卡尔曼滤波更新策略将产生一个主动弹性 LQG 控制器. 其中，对卡尔曼滤波器的状态预测误差 $\bar{e}_{k/k-1}=\bar{x}_k-\hat{\bar{x}}_{k/k-1}$ 和更新序列 $\bar{\gamma}_k=y_k-C\hat{\bar{x}}_{k/k-1}$ 的增量效应可表示为

$$\begin{cases} e_{k+1/k}=\bar{e}_{k+1/k}+f(k,k_f-1)\upsilon \\ \gamma_k=\bar{\gamma}_k+h(k,k_f-1)\upsilon \end{cases} \tag{28}$$

式中，$f(k,k_f-1)$ 和 $h(k,k_f-1)$ 可递归计算为

$$\begin{cases} f(k,k_f-1)=(A-K_kC)f(k-1,k_f-1)-\xi\delta_{k,k_f-1} \\ h(k,k_f-1)=Cf(k,k_f-1),\ f(k_f-1,k_f-1)=0 \end{cases} \tag{29}$$

假设 H_0 表示不存在攻击的无效假设；H_1 表示 k_f 时的攻击结束假设. 假设 H_1 可以面对无效假设 H_0，因为：

$$\begin{cases} H_0:E\{\gamma_j\}=0,k>j>0 \\ H_1:E\{\gamma_j\}=h(j,k_f-1)\upsilon \end{cases} \tag{30}$$

且有 $E\{\gamma_j\}=0,k_f-1>j\geqslant 0$. 令 $P(\gamma_j/H_1)$，$P(\gamma_j/H_0)$ 是 γ_j 在 H_1,H_0 条件下的高斯概率密度函数，并将似然比定义为

$$\lambda(k,k_f-1)=\frac{P(\frac{\gamma_{k_f}-1}{H_1})P(\frac{\gamma_{k_f}}{H_1})\cdots P(\frac{\gamma_k}{H_1})}{P(\frac{\gamma_{k_f-1}}{H_0})P(\frac{\gamma_{k_f}}{H_0})\cdots P(\frac{\gamma_k}{H_0})} \tag{31}$$

因为 $h(k_f-1,k_f-1)=0,h(k_f,k_f-1)=0$ 以及 $C\xi=0$，则可得 $P(\frac{\gamma_{k_f-1}}{H_1})=P(\frac{\gamma_{k_f-1}}{H_0}),P(\frac{\gamma_{k_f}}{H_1})=P(\frac{\gamma_{k_f}}{H_0})$，似然比式(31)变成下式.

$$\lambda(k,k_f-1)=\frac{\exp\left(-\frac{1}{2}\sum_{j=k_f+1}^{k}\|\gamma_j-h(j,k_f-1)\upsilon\|^2_{\bar{Q}_j^{-1}}\right)}{\exp\left(-\frac{1}{2}\sum_{j=k_f+1}^{k}\|\gamma_j\|^2_{\bar{Q}_j^{-1}}\right)} \tag{32}$$

式中，$\bar{Q}_j=C\bar{P}_{j/j-1}C^T+V\gamma_j$ 是 γ_j 的协方差. 在 k_f 条件下，脉冲强度的最大似然估计为

$$\hat{\upsilon}(k,k_f-1)=\frac{b(k,k_f-1)}{a(k,k_f-1)} \tag{33}$$

式中，

$$\begin{cases} a(k,k_f-1)=\sum_{j=k_f+1}^{k}[h_{j,k_f-1}^T(\bar{Q}_j)^{-1}h_{j,k_f-1}] \\ b(k,k_f-1)=\sum_{j=k_f+1}^{k}[h_{j,k_f-1}^T(\bar{Q}_j)^{-1}\gamma_j] \end{cases} \tag{34}$$

通过利用 $\hat{\upsilon}(k,k_f-1)$ 替换 υ，对数似然比 $T(k,k_f-1)=2\log(\lambda(k,k_f-1))$ 可由在 H_1 条件下脉冲的标准化估计值 $a(k,k_f-1)^{-1/2}b(k,k_f-1)$ 表示为 $T(k,k_f-1)=\hat{\bar{\upsilon}}(k,k_f-1)$，GLR 检测器判定规则为

$$T(k)=\max_{k_f\in[0,k-1]}\{\hat{\bar{\upsilon}}(k,k_f-1)^2\} \tag{35}$$

式中，ε 是阈值级别. 对于(35)的实现，可在有限大小的滑动窗口上实现最大化. 假警报、漏检和良好的决策率取决于决策级别的选择和滑动窗口的大小[14].

3.2　弹性 LQG 控制器

当 $T(k)>\varepsilon$ 时，通过使用 Kalman 滤波器更新策略，可以避免多次检测同一脉冲 $\upsilon\delta_{k,k_{f-1}}$，可表示为如下形式.

$$\begin{cases} \hat{\bar{x}}'_{k/k}=\hat{\bar{x}}'_{k/k}+f(k,\hat{k}_f-1)\hat{\upsilon}(k,\hat{k}_f-1) \\ \bar{P}'_{k/k}=\bar{P}_{k/k}+f(k,\hat{k}_f-1)a(k,\hat{k}_f-1)-1f(k,\hat{k}_f-1)^T \end{cases} \tag{36}$$

式中，$a(k,\hat{k}_f-1)^{-1}$ 表示 $\hat{\upsilon}(k,\hat{k}_f-1)$ 的协方差. $\hat{\bar{x}}'_{k/k}$ 和 $\hat{\bar{x}}_{k/k}$ 分别表示新的和旧的最小方差无偏估计. 攻击结束时间估计 $\hat{k}_f$ 可表示为

$$\hat{k}_f=\arg\left(\max_{k_f\in[k-1-M,k-1]}\{\hat{\bar{\upsilon}}(k,\hat{k}_f-1)^2\}\right) \tag{37}$$

然后，根据卡尔曼滤波器(5)上应用的更新策略(36)，可推导出自主弹性 LQG 控制器. 为评估所获得的弹性 LQG 控制器整体特性，需研究与攻击信号最大持续时间 τ 相关性能标准.

4　实验分析

4.1　实验设置

为了对所提网络控制系统零动态攻击控制过程的有效性进行验证，这里选取 Ubuntu 14.04 操作系统＋硬件设置进行实验平台搭建，系统为 64 位系统，CPU 主频为 i5-6500K 2.4 GHz，系统 RAM 大小为 ddr4-1800K 16GB. 仿真平台中，安装有 Wireshark 1.10.3，并结合 ZigBee 模块对研究网络数据进行检测和读取，实现数据实时监控.

系统中采用的是 Arduino 屏蔽,其通过嵌入式 802.15.4 模块以及 Digi XBee802.15.4 RF 模块进行实现,其所具有的优点是传输距离长,可达到数百米,主要用于低功耗网络数据传输中,存在的问题容易受到攻击干扰的影响,这也是本文选取其作为实验对象的主要原因.

4.2 攻击检测精度

本实验中选取的网络攻击检测模型精度评价指标是混淆矩阵,一般采用的是攻击检测正确数据数量占总体攻击数据总量的比例,分为网络攻击数据的准确率指标以及网络攻击数据的假阳性率指标,其定义形式分别如下.

$$T_{DA}=\frac{TP+TN}{N_{\text{total}}} \tag{38}$$

$$T_{FPR}=\frac{FP}{FP+FN} \tag{39}$$

式中,参数 TN 是网络攻击检测的真阴性值;TP 是网络攻击检测的真阳性值;FN 是网络攻击检测的真阴性值;FP 是网络攻击检测的假阳性值. 为更加充分的验证所提算法有效性,选取以下 3 种算法进行实验对比分析:网络攻击检测自适应决策模型(CVFDT)、网络攻击检测动态概率标记模型(DPPM)、网络攻击检测快速决策模型(VFDT). 实验对比数据见表 1 所示.

表 1 实验对比数据

Tab.1 Experimental comparison data

评估指标		VFDT		DPPM		CVFDT		本文模型	
		精度/%	假阳性率/%	精度/%	假阳性率/%	精度/%	假阳性率/%	精度/%	假阳性率/%
攻击数据量	1 000	88.4	9.6	90.1	8.6	91.4	6.2	95.6	3.5
	2 000	88.8	8.5	91.2	7.4	92.5	5.3	96.8	2.7
	3 000	89.4	7.4	92.1	6.8	93.7	4.4	97.4	2.3
	4 000	91.2	6.6	93.2	5.2	94.6	3.8	98.3	1.6
	5 000	92.3	5.7	93.4	4.2	96.7	2.3	98.9	1.2
攻击信号持续时间	1 s	72.1	12.3	74.5	10.3	76.3	9.6	79.5	7.2
	3 s	85.6	6.2	88.4	5.7	89.7	5.2	92.3	4.1
	5 s	97.3	2.3	97.5	1.2	98.1	1.1	98.9	0.9
	7 s	99.2	0.9	99.4	0.7	99.5	0.6	99.7	0.5

通过对比表 1 中实验结果可知,网络攻击检测模型精度性能上,所提基于主动弹性防御策略的网络控制系统零动态攻击检测精度保持在 95.6%~98.9%结果区间内,该精度指标要显著的优于 CVFDT 网络攻击检测算法模型(91.4%~96.7%取值区间)、DPPM 网络攻击检测算法模型(90.1%~93.4%取值区间)、VFDT 网络攻击检测算法模型(88.4%~92.3%). 对于选取的假阳性评估指标,本文所提算法网络攻击检测的假阳性率指标为 1.2%~3.5%,要明显低于 CVFDT 算法网络攻击检测的假阳性率指标(2.3%~6.2%)、DPPM 算法网络攻击检测的假阳性率指标(4.2%~8.6%)以及 VFDT 算法网络攻击检测的假阳性率指标(5.7%~9.6%). 通过实验分析,结果表明所提网络攻击检测模型相对于选取的对比检测算法模型具有更高的检测精度.

同时,根据表 1 实验数据中针对攻击信号持续时间的实验结果可知,随着攻击持续时间的增加几种算法的攻击识别精度均不断上升,假阳性率均逐渐下降,表现出相对一致的实验结果变化趋势. 从几种算法的横向对比看,本文算法的实验结果要优于选取的几种对比算法,验证了所提算法的有效性.

4.3 计算资源效率对比

本节实验中计算资源效率对比选取的指标主要有两个:计算内存占用比例和 CPU 处理时间. 网络攻击数据数量区间是 1 000~5 000,计算资源效率对比情况见图 3 结果所示.

根据图 3 所示计算资源效率实验结果可知,对于选取的相同数量的网络攻击样本,本文算法模型的样本攻击检测所需要的 CPU 处理时间要显著的少于选取的 CVFDT、VFDT 和 DPPM 三种网络攻击检测算法模型,其中 DPPM 网络攻击检测算法模型在计算资源效率指标上要优于 CVFDT 和 VFDT 网络攻击检测算法模型. CVFDT 因为在网络攻击检测过程中增加了概率比较适应过程,因此

其 CPU 处理时间最长.

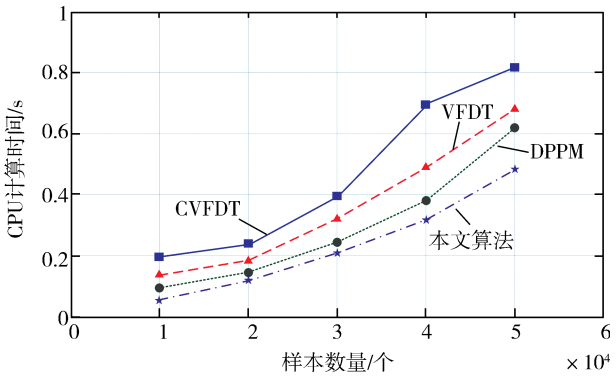

图 3　计算资源效率实验结果

Fig. 3　Experimental results of computational resource efficiency

采取相似方式，对网络攻击数据数量区间是 1 000～5 000 内，几种对比网络攻击检测算法模型的内存占用指标实验结果进行对比分析，见图 4.

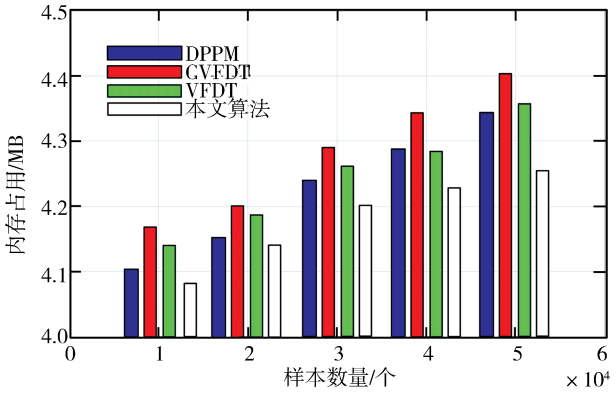

图 4　内存占用指标实验结果

Fig. 4　Experimental results of memory occupancy index

根据图 4 所示内存占用指标实验结果可知，对于选取的相同数量的网络攻击样本，本文算法模型的样本攻击检测所需要的内存占用指标要显著的少于选取的 CVFDT、VFDT 和 DPPM 三种网络攻击检测算法模型，其中 DPPM 网络攻击检测算法模型在内存占用指标上要优于 CVFDT 和 VFDT 网络攻击检测算法模型. CVFDT 同样因为增加了概率参数的自适应过程，而导致其内存占用指标相对 VFDT 模型较高. 上述实验结果验证了所提算法在计算效率上的性能优势.

5　结　论

本文研究了线性离散随机系统零动态攻击的弹性控制策略. 当网络物理系统的防御机制限制了对手的攻击窗口时，本文的第一部分表明，传统的基于模型的故障检测和隔离方案无法检测到零动态攻击，通过实时数据集攻击检测结果显示，所提算法明显具有更高的攻击检测质量. 在第二部分中，设计了一个弹性线性二次高斯控制器，能够快速恢复闭环系统行为，可利用广义似然比检测器给出的信息在线更新卡尔曼滤波器，得到了弹性线性二次高斯控制器，通过算法资源利用效率实验结果显示所提算法具有更佳的计算效率和内存利用效率，验证了算法的有效性.

参考文献：

[1] Liu J, Ji J C, Zhou J. Synchronization of networked multibody systems using fundamental equation of mechanics [J]. Mech Appl Math, 2016, 37: 555.

[2] Wu Y P, Wu Y. A novel predictive control scheme with an enhanced smith predictor for networked control system [J]. Autom Control Comp S, 2018, 52: 126.

[3] 唐彰国，李焕洲，张健. 基于组合神经网络的启发式工控系统异常检测模型[J]. 四川大学学报：自然科学版，2017，54：65.

[4] Yan S, Shen M Q, Zhang G M. Extended event-driven observer-based output control of networked control systems [J]. NLM, 2016, 86: 1639.

[5] Lu R Q, Yang P J, Bai J J, *et al*. Quantized observer-based sliding mode control for networked control systems via the time-delay approach [J]. Circ Syst Signal Pr, 2016, 35: 1563.

[6] Tebani K, Amari S, Kara R. Closed-loop control of constrained discrete event systems: application to a networked automation system [J]. Int J Adv Manuf Ttch, 2017, 90: 1295.

[7] Li C J, Chen L M, Guo Y N, *et al*. Formation-containment control for networked Euler-Lagrange systems with input saturation [J]. Nonlinear Dynam, 2018, 91: 1307.

[8] Mahmoud M S. Networked control systems analysis and design: an overview [J]. Arab J Sci Eng, 2016, 41: 711.

[9] Pang Z H, Liu G P, Zhou D H, *et al*. Data-based predictive control for networked nonlinear systems with packet dropout and measurement noise[J]. J Syst Sci Complex, 2017, 30: 1072.

[10] Sun J, Chen J, Gan M G. A necessary and sufficient stability criterion for networked predictive control systems[J]. Sci China-Technol Sci, 2016, 59: 2.

[11] Yu M, Bai S, Yang T, *et al*. Quantized output feedback control of networked control systems with packet dropout [J]. Int J Control Autom, 2018, 16: 2559.

[12] Hua C C, Yu S C, Guan X P. Finite-time control for a class of networked control systems with short time-varying delays and sampling jitter[J]. Int J Automat Comput, 2015, 12: 448.

[13] Kang Y, ZhaoY B. Dynamic data packing towards the optimization of QoC and QoS in networked control systems[J]. Sci China: Technol Sci, 2016, 59: 72.

[14] 王辉, 茹鑫鑫, 戴田旺, 等. 基于 NAPG 模型的攻击增益路径预测算法[J]. 吉林大学学报: 理学版, 2019, 57: 1169.

引用本文格式:

中 文: 蒲在毅, 张咏梅, 贾艳梅. 基于主动弹性防御策略的网络控制系统零动态攻击检测[J]. 四川大学学报: 自然科学版, 2020, 57: 879.

英 文: Pu Z Y, Zhang Y M, Jia Y M. Zero dynamic attack detection of network control systems based on active elastic defense strategy [J]. J Sichuan Univ: Nat Sci Ed, 2020, 57: 879.