数据注入攻击下ICPS的自适应事件触发弹性控制

薛威峰[1], 孙子文[1,2†]

(1. 江南大学 物联网工程学院, 江苏 无锡 214122; 2. 物联网技术应用教育部工程研究中心, 江苏 无锡 214122)

摘要: 为使工业信息物理系统(ICPS)抵御数据注入攻击, 本文研究了事件触发弹性控制策略, 采用自适应事件触发以减少通信资源, 构建攻击估计器以降低攻击对系统性能的影响. 通过H_∞渐近稳定性准则推导估计器参数, 采用Lyapunov-Krasovskii函数推导事件触发、数据注入攻击、网络延迟和弹性控制器之间的定量关系. 以二自由度质量–弹簧–阻尼串联系统为被控对象, MATLAB仿真验证基于自适应事件触发的ICPS在数据注入攻击下的系统性能, 结果表明所采取策略能保证系统的稳定性, 并有效减少通信资源.

关键词: ICPS; 数据注入攻击; 自适应事件触发; 弹性控制

引用格式: 薛威峰, 孙子文. 数据注入攻击下ICPS的自适应事件触发弹性控制. 控制理论与应用, 2024, 41(5): 866 – 874

DOI: 10.7641/CTA.2023.20774

Adaptive event triggered resilient control of ICPS under data injection attack

XUE Wei-feng[1], SUN Zi-wen[1,2†]

(1. School of Internet of Things Engineering, Jiangnan University, Wuxi Jiangsu 214122, China;
2. Engineering Research Center of Internet of Things Technology Applications Ministry of Education, Wuxi Jiangsu 214122, China)

Abstract: To defend the false data injection attack in an industrial cyber physicsal system (ICPS), this article studies the event-triggered mechanism of the resilient control, where the adaptive event-triggered mechanism is introduced to reduce the communication resource, and an attack estimator is also built to reduce the impact of attack on the system's performance. The relevant parameters of the estimator are derived by H_∞ stability criterion, and the Lyapunov-Krasovskii function is used to get the quantitative relationship among event triggered parameters, the data injection attack, the network delay and the resilient controller. The simulation is conducted with MATLAB software to verify the performance of ICPS being based on the adaptive event triggered mechanism under data injection attack, where the two-degree-of-freedom mass-spring-damping series system is used as the plant. Simulation results show that the proposed mechanism, by using the combination of adaptive event triggered mechanism and attack estimator, can guarantee the system's stability and reduce communication resource.

Key words: ICPS; data injection attack; adaptive event-triggered; resilient control

Citation: XUE Weifeng, SUN Ziwen. Adaptive event triggered resilient control of ICPS under data injection attack. *Control Theory & Applications*, 2024, 41(5): 866 – 874

1 引言

信息物理系统(cyber physical systems, CPS)将计算网络、感知集成到物理过程[1–4], 其中的嵌入式传感器和执行器通过联网来感知、监控和管理整个物理过程, 被广泛应用于工业环境中, 形成工业信息物理系统(industrial CPS, ICPS)[5–6].

由于物理或技术限制, 传感器、执行器和其他联网部件之间的数据在没有安全保护下通过网络传输, 为恶意攻击者破坏ICPS提供了机会[7]. 例如2015年乌克兰电网遭受攻击, 导致三省停电[8], 2019年挪威海德鲁公司遭受攻击, 金属生产线中止工作[9], 2020年3月钢铁制造商EVRAZ公司北美分支机构遭受攻击导致裁员停产两周[10], 2021年4月份, 伊朗纳坦兹核设施断电事件[11], 2021年5月份, “Darkside”勒索病毒致使美国燃油管道运营商被迫关闭了整个管道系统[12]. 因此, 分析遭受网络攻击的ICPS, 保障控制系统弹

收稿日期: 2022−08−31; 录用日期: 2023−04−11.

†通信作者. E-mail: sunziwen@jiangnan.edu.cn; Tel. : +86 13915355548.

本文责任编委: 孙长银.

国家自然科学基金项目(61373126), 中央高校基本科研业务费专项资金项目(JUSRP51510), 江苏省自然科学基金项目(BK20131107)资助.

Supported by the National Natural Science Foundation of China (61373126), the Central University Fundamental Research Funds Special Funding (JUSRP51510) and the Jiangsu Provincial Natural Science Foundation Funded Project (BK20131107).

性、鲁棒性等性能具有积极意义.

虚假数据注入(false data injection, FDI)攻击受到广泛关注, 主要围绕攻击策略、攻击检测以及弹性控制展开. 在攻击策略方面, 分析系统性能的退化, 采用拉格朗日乘子法求解约束二次优化问题得到最优攻击策略[13]; 采用独立于CPS的实时数据生成FDI数据[14]. 在攻击检测方面, 通过求和检测器利用当前残差和历史残差检测FDI[15]; 采用主动数据修改方案, 使得攻击者因无法获得正确的系统模型而无法保证攻击的隐蔽性[16]. 在弹性控制方面, 为容忍更密集的拒绝服务(denial of service, DoS)攻击, 文献[17]首先利用DoS驻留时间有界的特性, 引入区间划分技术降低稳定性分析的保守性, 其次, 提供基于弹性观察器的控制器设计策略, 以提高抵御DoS攻击的弹性; 为减少网络负载和提高系统弹性, 考虑信息传输被异步DoS攻击的情况, 文献[18]采用动态事件触发的弹性控制方法, 并通过李雅普诺夫稳定性理论推导出稳定性判据. 从现有文献分析, FDI攻击和DoS攻击在系统中的表现分别为信号受损和信号中断, 对DoS攻击一般通过驻留时间有界的特性, 在不同区间内解决攻击造成的系统不稳定性, 确保系统的弹性; 而对于FDI攻击, 需要综合考虑对攻击的处理和控制器的设计, 来确保信号的完整性和系统的稳定性.

针对ICPS中存在干扰和噪声时测量通道遭受FDI攻击问题, 本文设计出自适应事件触发弹性控制策略, 主要贡献如下:

1) 为降低通信资源的占用率, 引入自适应事件触发机制, 当触发阈值随外部干扰和数据注入攻击按自适应率进行实时变化, 既保证系统的一定弹性, 也更加节约通信资源.

2) 为减少攻击对系统稳定性的不利影响, 攻击估计模块借助观测器和攻击估计器对数据注入攻击进行估计.

3) 为推导出控制器的充分条件, 实现自适应事件触发弹性控制, 构建Lyapunov-Krasovskii(L-K)函数综合考虑事件触发、网络延迟、弹性反馈控制器和数据注入攻击.

2　系统模型

2.1　数据注入攻击下的ICPS反馈控制模型

为减少数据注入攻击对系统稳定性的不利影响, 降低测量通道的数据资源传输量, 缓解带宽通信压力, 构建如图1所示的基于事件触发的ICPS输出反馈控制模型. 该模型主要有采样触发模块、攻击估计模块和控制模块, 采样触发模块包括传感器、采样器、事件触发器、缓存器, 攻击估计模块包括观测器和估计器, 控制模块包括零阶保持器、反馈控制器、执行器.

采样器以周期h(h为有限时间)对经由传感器的$y(t)$进行采样, 得到离散数据$y(nh)(n\in\mathbb{N})$, 采样触发模块至攻击估计模块之间的信号传输使用事件触发方式, 当离散数据满足触发条件, 采样时刻$t_k^x h$的输出信号通过无线传输网络进行传输.

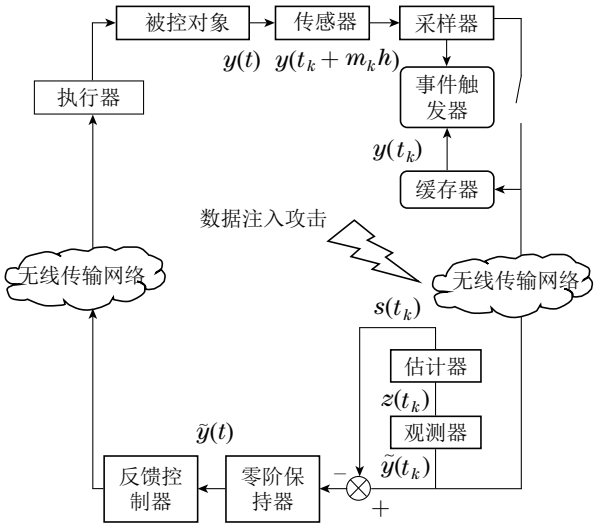

图 1　基于事件触发的ICPS输出反馈模型

Fig. 1　ICPS event-triggered output feedback model

攻击估计模块对FDI攻击进行预处理, 攻击后的输出值减去估计值后, 将数据传输至零阶保持器, 输出值由离散采样信号变为连续信号, 再传送至控制器.

2.2　无攻击下被控对象的数学模型

无攻击下被控对象的连续时间模型如下所示:

$$\begin{cases}\dot{x}(t)=A_px(t)+B_pu(t)+B_\omega\omega(t),\\ y(t)=C_px(t),\\ z(t)=F_px(t)+G_pu(t),\end{cases}\tag{1}$$

其中: $x(t)\in\mathbb{R}^n$为状态变量; $u(t)\in\mathbb{R}^m$为控制变量; $y(t)\in\mathbb{R}^p$为测量变量; $w(t)\in\mathbb{R}^q$为未知干扰, 且$w(t)\in L_2(0,\infty)$; $z(t)\in\mathbb{R}^z$为输出变量; n, m, p, q, z为状态变量、输入变量、输出变量和干扰的维度; $A_p, B_p, C_p, B_\omega, F_p$和$G_p$为具有相应维数的矩阵, 假设$(A_p, B_p)$可控, (A_p, C_p)可观.

2.3　事件触发机制

为减少采样信号$y(nh)$通过无线通信网络传输的次数, 引入事件触发机制, 事件触发机制主要设计触发条件中适当的触发参数ε.

事件触发发生在采样时刻$S=\{h,2h,3h,\cdots,nh\}$期间, 对相邻两个触发时刻进行如下划分:

$$t_{k+1}=t_k+\min_{m\in\mathbb{N}}\{m\ h|\mu(t)+\delta_1(\varepsilon\bar{y}^{\mathrm{T}}(t_k)\phi y(t_k)-\varphi^{\mathrm{T}}(t_k)\phi\varphi(t_k))\leqslant 0\},$$

其中: $t_k=t_k^{\mathrm{s}}h$为上一个触发时刻, t_k^{s}代表在采样时刻$t_k^{\mathrm{s}}h$触发成功; t_{k+1}为下一个触发时刻, 触发时刻$T=\{t_1^xh,t_2^xh,t_3^xh,\cdots\}, T\subseteq S$; $y(t_k)$为缓存器中最新数据, $y(t_k+mh)$为此刻的采样值; $\varphi(t_k)=y(t_k)-\bar{y}(t_k)$, $\bar{y}(t_k)=\dfrac{y(t_k)+y(t_k+mh)}{2}$; $\delta_1>0; 0<\varepsilon<1$; ϕ为正定权重矩阵.

当$\mu(t)=0$时, 其中$t\in[t_k,t_{k+1})$, 触发机制为固

定阈值事件触发, 固定阈值为ε, 触发条件为

$$\varepsilon\bar{y}^{\mathrm{T}}(t_k)\phi y(t_k)-\varphi^{\mathrm{T}}(t_k)\phi\varphi(t_k)\leqslant 0,$$

其中$\mu(t)$的初始值满足$\mu(0)\geqslant 0$, $\delta_2>0$, 所以$\mu(t)\neq 0$时, 自适应事件触发条件如下:

$$\mu(t)+\delta(\varepsilon\bar{y}^{\mathrm{T}}(t_k)\phi\bar{y}(t_k)-\varphi^{\mathrm{T}}(t_k)\phi\varphi(t_k))\leqslant 0. \quad (2)$$

触发阈值的自适应率满足

$$\dot{\mu}(t)=-\delta_2\mu(t)+\varepsilon^2\bar{y}^{\mathrm{T}}(t_k)\phi\bar{y}(t_k)-\varphi^{\mathrm{T}}(t_k)\phi\varphi(t_k). \quad (3)$$

注 1 固定阈值事件触发的触发阈值无法改变, 当遭受攻击时, 系统的信号值出现波动, 触发次数容易增加, 系统的恢复时间变长, 而采用自适应触发机制, 当信号遭受影响, 触发阈值根据系统信号的变化实时更新, 减少触发次数, 进而减少通信资源, 减短系统恢复时间, 减少攻击对系统造成的危害.

2.4 数据注入攻击数学模型

测量通道遭受FDI攻击, 攻击者将虚假数据注入测量通道传输的传感器输出信号, 损害传输数据的准确性, 进而损害系统的稳定性.

当攻击者对测量通道进行攻击时, 有建立描述攻击行为的攻击矩阵

$$\Gamma=\mathrm{diag}\{s_1,\cdots,s_i,\cdots,s_n\},$$

当$s_i=1$, 代表第i个传感器受到攻击; $s_i=0$代表该传感器安全.

当测量通道受到攻击后, 会有相应的攻击信号的注入, 导致控制器接收到错误数据, 攻击者的攻击信号序列如下所示:

$$f(\tilde{y}(t_k))=(f_1(\tilde{y}(t_k)),\cdots,f_j(\tilde{y}(t_k)),\cdots,f_n(\tilde{y}(t_k))),$$

其中$f_j(\tilde{y}(t_k))$代表第j个通道的攻击信号.

当系统遭受攻击后, 根据式(1), 测量通道的输出信号变为

$$\tilde{y}(t_k)=Cx(t_k)+\Gamma f(\tilde{y}(t_k)). \quad (4)$$

3 攻击估计模块数学模型

为减少攻击信号对系统信号完整性的影响, 使得系统渐近稳定, 通过观测器和攻击估计器估计攻击信号, 再将遭受攻击的测量通道输出信号减去估计值, 从而减少攻击信号对系统稳定性的不利影响.

3.1 观测器设计

观测器设计如下:

$$\begin{cases}\hat{x}(t_{k+1})=A_p\hat{x}(t_k)+B_pu(t)+\\ \qquad\qquad L(y(t_k)-\hat{y}(t_k)),\\ \hat{y}(t_k)=C_p\hat{x}(t_k),\end{cases} \quad (5)$$

其中: $\hat{x}(t_k)$为$x(t_k)$的估计值, $\hat{y}(t_k)$为$y(t_k)$的估计值, L为观测器的增益.

误差$e(t_{k+1})=x(t_{k+1})-\hat{x}(t_{k+1})$, 残差$z(t_k)=y(t_k)-\hat{y}(t_k)$, 根据式(1)(5)可得

$$\begin{cases}e(t_{k+1})=(A_p-LC_p)e(t_k)+B_ww(t),\\ z(t_k)=C_pe(t_k),\end{cases} \quad (6)$$

其中L的选取满足$\int_0^\infty z^{\mathrm{T}}z\mathrm{d}t_k<\gamma^2\int_0^\infty w^{\mathrm{T}}w\mathrm{d}t_k$.

3.2 估计器设计

根据式(6), 设计攻击估计器如下:

$$\begin{cases}\nu(t_{k+1})=A_av(t_k)+B_az(t_k),\\ s(t_k)=C_av(t_k)+D_az(t_k),\end{cases} \quad (7)$$

其中: $v(t_k)$为攻击估计变量, $s(t_k)$为测量通道攻击的估计值, A_a,B_a,C_a,D_a为具有合适维度的矩阵.

注 2 文献[19]中, 许多攻击估计模块都是依靠实际输出值与估计输出值之间的误差来修正估计, 本文的估计器也采用类似形式, 但为提高设计自由度, 综合考虑攻击引起的状态变量的变化, 引入中间变量状态的攻击估计变量$v(t_k)$, $v(t_k)=x(t_k)-\lambda\Gamma\hat{x}(t_k)$, λ为可调参数, 可以通过调整参数来改善估计性能.

攻击误差为 $e_y(t_k)=\Gamma f(\tilde{y}(t))-s(t_k)$, 根据式(6)–(7)可得

$$\begin{cases}\gamma(t_{k+1})=A_r\gamma(t_k)+B_r\varpi(t_k),\\ e_y(t_k)=C_r\gamma(t_k)+D_r\varpi(t_k),\end{cases} \quad (8)$$

其中: $\gamma(t_k)=[e^{\mathrm{T}}(t_k)\ \ v^{\mathrm{T}}(t_k)]$, $\varpi(t_k)=\begin{bmatrix}w(t_k)\\ f(\tilde{y}(t))\end{bmatrix}$,

$A_r=\begin{bmatrix}A_p-LC_p & 0\\ B_aC_p & A_a\end{bmatrix}$, $B_r=\begin{bmatrix}B_w & -L\Gamma\\ 0 & B_a\end{bmatrix}$, $C_r=[-D_aC_p\ \ -C_a]$, $D_r=[0\ \ \Gamma-D_a\Gamma]$.

定理 1 如果存在一个正定矩阵$\bar{P}$, 对于给定的$\lambda_1>0$, 若满足

$$\begin{bmatrix}\Theta_{11} & *\\ \Theta_{21} & \Theta_{22}\end{bmatrix}<0, \quad (9)$$

其中: $\Theta_{11}=\begin{bmatrix}-\bar{P} & 0\\ 0 & -\lambda_1^2I\end{bmatrix}$, $\Theta_{21}=\begin{bmatrix}\bar{P}A_r & \bar{P}B_r\\ C_r & D_r\end{bmatrix}$,

$\Theta_{22}=\begin{bmatrix}-\bar{P} & 0\\ 0 & -I\end{bmatrix}$,

$$\begin{bmatrix}-\bar{P} & 0 & A_r^{\mathrm{T}}\bar{P} & C_r^{\mathrm{T}}\\ 0 & -\lambda_1^2I & B_r^{\mathrm{T}}\bar{P} & D_r^{\mathrm{T}}\\ \bar{P}A_r & \bar{P}B_r & -\bar{P} & 0\\ C_r & D_r & 0 & -I\end{bmatrix}<0, \quad (10)$$

则系统是均方指数稳定且具有H_∞性能.

证 构建Lyapunov函数$V(k)=\gamma^{\mathrm{T}}(t_k)\bar{P}\gamma(t_k)$, 则

$$\Delta V(k)=\gamma^{\mathrm{T}}(t_{k+1})\bar{P}\gamma(t_{k+1})-\gamma^{\mathrm{T}}(t_k)\bar{P}\gamma(t_k),$$

$$J(k)=\Delta V(k)+e_y^{\mathrm{T}}(t_k)e_y(t_k)-\lambda_1^2\varpi^{\mathrm{T}}(t_k)\varpi(t_k),$$

$$\sum_{k=0}^{\infty} J(k) = V(\infty) - V(0) + \sum_{k=0}^{\infty}(e_y^{\mathrm{T}}(t_k)e_y(t_k) - \lambda_1^2\varpi^{\mathrm{T}}(t_k)\varpi(t_k)) = \sum_{k=0}^{\infty}\begin{bmatrix}\gamma(t_k)\\ \varpi(t_k)\end{bmatrix}^{\mathrm{T}} \mathit{\Pi}\begin{bmatrix}\gamma(t_k)\\ \varpi(t_k)\end{bmatrix},$$

其中

$$\mathit{\Pi} = \begin{bmatrix} A_r^{\mathrm{T}}\bar{P}A_r + C_r^{\mathrm{T}}C_r - \bar{P} & A_r^{\mathrm{T}}\bar{P}B_r + C_r^{\mathrm{T}}D_r \\ B_r^{\mathrm{T}}\bar{P}A_r + D_r^{\mathrm{T}}C_r & B_r^{\mathrm{T}}\bar{P}B_r + D_r^{\mathrm{T}}D_r - \lambda_1^2 I \end{bmatrix}.$$

若$\sum_{k=0}^{\infty} J(k) < 0$, 即$\mathit{\Pi} < 0$, 则当系统满足零初始条件时, 有

$$\sum_{k=0}^{\infty} e_y^{\mathrm{T}}(t_k)e_y(t_k) < \lambda_1^2 \sum_{k=0}^{\infty} \varpi^{\mathrm{T}}(t_k)\varpi(t_k). \quad (11)$$

对式(9)使用Schur引理, 可以得

$$\mathit{\Pi} = \Theta_{11} - \Theta_{21}^{\mathrm{T}}\Theta_{22}^{-1}\Theta_{21} < 0,$$

则定理得证.　证毕.

为了让攻击估计器具有H_∞性能, 设计估计器的相关增益矩阵如下.

定理 2　如果存在正定矩阵$R_1, T_1, A, S_i, i = 1, 2, 3, 4$, 使得不等式成立, 则系统渐近稳定且具有$\mathrm{H}_\infty$性能.

$$\begin{bmatrix}\Phi_{11} & * \\ \Phi_{21} & \Phi_{22}\end{bmatrix} < 0, \quad (12)$$

其中: $\Phi_{11} = \begin{bmatrix}-T_1^{-1} & * \\ -T_1^{-1} & -R_1\end{bmatrix}$,

$$\Phi_{21} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ T_1^{-1}(A_p - LC_p) & T_1^{-1}(A_p - LC_p) \\ \Lambda_1 + S_2 & \Lambda_1 \\ -S_4 - S_3 & -S_4 \end{bmatrix},$$

$\Lambda_1 = S_1C_p + R_1(A_p - LC_p)$, $S_1 = AB_a$, $S_2 = AA_aB^{\mathrm{T}}T_1^{-1}, S_3 = C_aB^{\mathrm{T}}T_1^{-1}, S_4 = D_aC_p, \Phi_{31} =$

$$\begin{bmatrix} -\lambda_1^2 I & * & * & * & * \\ 0 & -\lambda_1^2 I & * & * & * \\ T_1^{-1} & -T_1^{-1}L\Gamma & -T_1^{-1} & * & * \\ R_1 & -R_1L\Gamma + S_1 & -T_1^{-1} & -R_1 & * \\ 0 & \Gamma - D_a\Gamma & 0 & 0 & -I \end{bmatrix}.$$

证　令$\bar{P} = \begin{bmatrix}R_1 & A \\ A^{\mathrm{T}} & R_2\end{bmatrix}$, $\bar{P}^{-1} = \begin{bmatrix}T_1 & B \\ B^{\mathrm{T}} & T_2\end{bmatrix}$, 其中$R_1, R_2, T_1, T_2$为正定矩阵.

定义矩阵$\Psi_1 = \begin{bmatrix}T_1 & I \\ B^{\mathrm{T}} & 0\end{bmatrix}$和$\Psi_2 = \bar{P}\Psi_1 = \begin{bmatrix}I & R_1 \\ 0 & A^{\mathrm{T}}\end{bmatrix}$, 对式(10)左乘diag$\{\Psi_1^{\mathrm{T}}, I, \Psi_1^{\mathrm{T}}, I\}$, 同时右乘diag $\{\Psi_1, I, \Psi_1, I\}$可得

$$\begin{bmatrix} -\Psi_2^{\mathrm{T}}\Psi_1 & * & * & * \\ 0 & -\lambda_1^2 I & * & * \\ \Psi_1^{\mathrm{T}}\bar{P}A_r\Psi_1 & \Psi_1^{\mathrm{T}}\bar{P}B_r & -\Psi_2^{\mathrm{T}}\Psi_1 & * \\ C_r\Psi_1 & D_r & 0 & -I \end{bmatrix} < 0. \quad (13)$$

对式(13)右乘$\{T_1^{-1}, I, I, I, T_1^{-1}, I, I\}$可得式(12), 定理得证, 且可得

$$\begin{cases} A_a = A^{-1}S_2T_1(I - R_1T_1)^{-1}A, \\ B_a = A^{-1}S_1, \\ C_a = S_3T_1(I - R_1T_1)^{-1}A, \\ D_a = S_4C_p^{-1}. \end{cases} \quad (14)$$

证毕.

注 3　定理2和定理3给出攻击估计器分析, 为保证定理2和3中的线性矩阵不等式(linear matrix inequality, LMI)有解, 有如下步骤:

步骤 1　为使设计的攻击估计器均方指数稳定且具有H_∞性能, 构造Lyapunov函数$V(k)$, 计算其导数并引入$J(k)$, 对式(9)使用Schur引理得到$\mathit{\Pi} = \Theta_{11} - \Theta_{21}^{\mathrm{T}}\Theta_{22}^{-1}\Theta_{21} < 0$, 所以$\sum_{k=0}^{\infty} J(k) < 0$, 存在一个正定矩阵$\bar{P}$, 对于给定的$\lambda_1 > 0$, 满足$\begin{bmatrix}\Theta_{11} & * \\ \Theta_{21} & \Theta_{22}\end{bmatrix} < 0$.

步骤 2　为求解攻击估计器增益矩阵, 在式(10)左乘diag$\{\Psi_1^T, I, \Psi_1^T, I\}$和右乘diag $= \{\Psi_1, I, \Psi_1, I\}$得式(13), 在式(13)左乘$\{T_1^{-1}, I, I, I, T_1^{-1}, I, I\}$和右乘$\{T_1^{-1}, I, I, I, T_1^{-1}, I, I\}$得式(12), 因此存在正定矩阵$R_1, T_1, A, S_i, i = 1, 2, 3, 4$, 满足$\begin{bmatrix}\Phi_{11} & * \\ \Phi_{21} & \Phi_{22}\end{bmatrix} < 0$.

假设 1　假设攻击有界且攻击频率$w_a \in [\underline{w}, \bar{w}]$, 则估计值有界且满足

$$e_y^{\mathrm{T}}(t_k)e_y(t_k) \leqslant \tilde{y}^{\mathrm{T}}(t)F^{\mathrm{T}}F\tilde{y}(t), \quad (15)$$

其中F为攻击相关矩阵.

考虑到网络引起的延迟$\tau_k \in [\underline{\tau}, \bar{\tau}]$, 因此通过事件触发机制传输的采样数据都是在时刻$[t_1^s h + \tau_1, t_2^s h + \tau_2, \cdots, t_k^s h + \tau_s, \cdots]$, 到达零阶保持器, 当考虑受到数据注入攻击时, 进入控制器的输出信号变为

$$y(t) = \tilde{y}(t_k) - s(t_k), \quad (16)$$

其中$t \in \left[t_k^s h + \tau_k, t_{k+1}^s h + \tau_{k+1}\right)$, 将其划分成$\ell_k$个子区间, 长度为一个采样周期, 即

$$\left[t_k^s h + \tau_k, t_{k+1}^s h + \tau_{k+1}\right) = \bigcup_{j=0}^{\ell_k} \varpi_j^{t_k}, \quad (17)$$

式(17)又可以变化为

$$\begin{cases} [t_k^s h + jh, t_k^s h + (j+1)h), & j = 0, \cdots, \ell_k - 1, \\ \left[t_k^s h + jh, t_{k+1}^s h\right), & j = \ell_k, \end{cases} \quad (18)$$

其中$\ell_k = t_{k+1}^x - t_k^x - 1$.

根据式(16)可得

$$y(t) = 2\varphi(t) + y(t - \kappa(t)) + e_y(t_k),\ t \in \varpi_j^{t_k}. \quad (19)$$

其中$\kappa(t)=t-t_k-\ell_k h$, 且满足$\kappa(t)\in[\underline{\tau},\bar{\tau}+h]$.

由于内部结构复杂, 系统的状态变量难以测得, 再加上攻击影响, 因此引入动态反馈控制器

$$\begin{cases}\dot{x}_{\rm c}(t)=A_{\rm c}x_{\rm c}(t)+B_{\rm c}x_{\rm c}(t-\eta(t))+C_{\rm c}y(t),\\ u(t)=Kx_{\rm c}(t),\end{cases}\tag{20}$$

其中: $x_{\rm c}(t)$, $y(t)$和$u(t)$分别表示动态反馈控制器的状态变量、输入变量和输出变量; $A_{\rm c}$, $B_{\rm c}$, $C_{\rm c}$和K为待设计的增益矩阵, 输出信号$u(t)$考虑到了受到攻击的信号$y(t)$和历史状态变量$x_{\rm c}(t-\eta(t))$, 确保设计的控制器的弹性.

根据式(1)(8)(20), 闭环系统变为

$$\begin{cases}\dot{\zeta}(t)=\bar{A}_p\zeta(t)+\tilde{A}_p\zeta(t-\eta(t))+\bar{B}_p\varphi(t)+\\ \qquad\tilde{B}_pe_y(t_k)+\bar{B}_ww(t),\\ z(t)=\bar{F}_p\zeta(t),\end{cases}\tag{21}$$

其中: $\zeta(t)=\begin{bmatrix}x(t)\\ x_{\rm c}(t)\end{bmatrix}$, $\bar{A}_p=\begin{bmatrix}A_p & B_pK\\ 0 & A_{\rm c}\end{bmatrix}$, $\tilde{A}_p=\begin{bmatrix}0 & 0\\ C_{\rm c}C_p & B_{\rm c}\end{bmatrix}$, $\bar{B}_p=\begin{bmatrix}0\\ 2C_{\rm c}\end{bmatrix}$, $\tilde{B}_p=\begin{bmatrix}0\\ C_{\rm c}\end{bmatrix}$, $\bar{B}_w=\begin{bmatrix}B_w\\ 0\end{bmatrix}$, $\bar{F}_p=[F_p\ \ G_pK]$.

4 闭环系统稳定性分析

当遭受数据注入攻击后, 事件触发机制(2)–(3)下的闭环系统(21)需要综合考虑网络延迟、攻击造成的不稳定等因素, 为此, 通过构造L-K泛函, 利用Schur引理和LMI, 给出系统满足渐近稳定和$\rm H_\infty$性能的条件.

定理 3 对于给定的采样周期$h>0$, 由无线传输网络引起的延迟$\bar{\tau}>\tau>\underline{\tau}>0$, 攻击相关矩阵$M>0$, 参数$\varepsilon>0$, 以及$\rm H_\infty$指标$\lambda_2>0$, 如果存在矩阵$\phi>0, P>0, S>0, R>0, Q_i>0(i=1,2,3)$, U, 使得

$$\begin{bmatrix}Q_2 & *\\ U^{\rm T} & Q_2\end{bmatrix}>0,\tag{22}$$

$$\begin{bmatrix}\Sigma_{11} & *\\ \Sigma_{21}^{\rm T} & \Sigma_{22}\end{bmatrix}<0,\tag{23}$$

则系统渐近稳定且满足$\rm H_\infty$性能.

证 构造L-K泛函如下:

$$\begin{aligned}V(t)&=V_1(t)+V_2(t)+V_3(t),\\ V_1(t)&=\zeta^{\rm T}(t)P\zeta(t)+\int_{t-\sigma}^{t}\varsigma^{\rm T}(s)S\varsigma(s){\rm d}s+\\ &\quad\int_{t-\eta_1}^{t}\zeta^{\rm T}(s)R\zeta(s){\rm d}s,\\ V_2(t)&=\eta_1\int_{-\eta_1}^{0}\int_{t+v}^{t}\dot{\zeta}^{\rm T}(s)Q_1\dot{\zeta}(s){\rm d}s{\rm d}v+\\ &\quad\eta_{31}\int_{-\eta_3}^{-\eta_1}\int_{t+v}^{t}\dot{\zeta}^{\rm T}(s)Q_2\dot{\zeta}(s){\rm d}s{\rm d}v+\\ &\quad\eta_{23}\int_{-\eta_2}^{-\eta_3}\int_{t+v}^{t}\dot{\zeta}^{\rm T}(s)Q_3\dot{\zeta}(s){\rm d}s{\rm d}v.\end{aligned}$$

$$V_3(t)=\mu(t),$$

其中: $\eta_1=\underline{\tau}$, $\eta_2=h+\bar{\tau}$, $\eta_3=\dfrac{\eta_1+\eta_2}{2}$, $\eta_{31}=\eta_3-\eta_1$, $\eta_{23}=\eta_2-\eta_3$, $\sigma=\dfrac{\eta_2-\eta_1}{2}$, $\varsigma(t)$ 为增广列向量 $\{\zeta(t-\eta_1),\zeta(t-\eta_3)\}$.

对$V(t)$求导, 可得

$$\begin{aligned}\dot{V}_1(t)=&\zeta^{\rm T}(t)P\dot{\zeta}(t)+\dot{\zeta}^{\rm T}(t)P\zeta(t)+\\ &\zeta^{\rm T}(t)R\zeta(t)-\zeta^{\rm T}(t-\eta_1)R\zeta(t-\eta_1)+\\ &\varsigma^{\rm T}(t)S\varsigma(t)-\varsigma^{\rm T}(t-\sigma)S\varsigma(t-\sigma),\end{aligned}\tag{24}$$

$$\begin{aligned}\dot{V}_2(t)=&\dot{\zeta}^{\rm T}(t)(\eta_1^2Q_1+\eta_{31}^2Q_2+\eta_{23}^2Q_3)\dot{\zeta}(t)-\\ &\eta_1\int_{t-\eta_1}^{t}\dot{\zeta}^{\rm T}(v)Q_1\dot{\zeta}(v){\rm d}v-\\ &\eta_{31}\int_{t-\eta_{31}}^{t-\eta_1}\dot{\zeta}^{\rm T}(v)Q_2\dot{\zeta}(v){\rm d}v-\\ &\eta_{23}\int_{t-\eta_2}^{t-\eta_{23}}\dot{\zeta}^{\rm T}(v)Q_3\dot{\zeta}(v){\rm d}v,\end{aligned}\tag{25}$$

$$\begin{aligned}\dot{V}_3(t)=&-\delta_2\mu(t)+\varepsilon^2\bar{y}^{\rm T}(t_k)\phi\bar{y}(t_k)-\\ &\varphi^{\rm T}(t_k)\phi\varphi(t_k).\end{aligned}\tag{26}$$

定义$\xi(t)=\{\zeta(t),\ \zeta(t-\eta_1),\ \zeta(t-\eta(t)),\ \zeta(t-\eta_2),\zeta(t-\eta_3),\varphi(t),e_y(t_k),w(t)\}$, $e_i=[0_{2n\times2(i-1)n}\ \ I_{2n}\ \ 0_{2n\times2(5-j)n}\ \ 0_{2n\times(p+m+q)}], i=1,2,3,4,5$, $e_6=[0_{n\times10n}\ \ I_p\ \ 0_{p\times(p+q)}]$, $e_7=[0_{p\times(10n+q+p)}\ \ I_p]$, $e_8=[0_{q\times(10n+p)}\ \ I_q\ \ 0_{p\times q}]$.

将式(21)代入式(24), $\dot{V}_1(t)$满足

$$\begin{aligned}\dot{V}_1(t)=&\xi^{\rm T}(t){\rm sym}\{e_1^{\rm T}P\Omega_1\}\xi(t)+\zeta^{\rm T}(t)P\dot{\zeta}(t)+\\ &\dot{\zeta}^{\rm T}(t)P\zeta(t)+\varsigma^{\rm T}(t)S\varsigma(t)-\\ &\varsigma^{\rm T}(t-\sigma)S\varsigma(t-\sigma)+\zeta^{\rm T}(t)R\zeta(t)-\\ &\zeta^{\rm T}(t-\eta_1)R\zeta(t-\eta_1),\end{aligned}\tag{27}$$

$$\begin{aligned}\dot{V}_1(t)=&\xi^{\rm T}(t){\rm sym}\{e_1^{\rm T}P\Omega_1\}\xi(t)+\\ &\xi^{\rm T}(t)(\begin{bmatrix}e_2^{\rm T} & e_5^{\rm T}\end{bmatrix}S\begin{bmatrix}e_2\\ e_5\end{bmatrix}-\\ &\begin{bmatrix}e_5^{\rm T} & e_4^{\rm T}\end{bmatrix}S\begin{bmatrix}e_5\\ e_4\end{bmatrix})\xi(t)+\\ &\xi^{\rm T}(t)(e_1^{\rm T}Re_1-e_2^{\rm T}Re_2)\xi(t),\end{aligned}\tag{28}$$

其中$\Omega_1=\bar{A}_pe_1+\tilde{A}_pe_3+\bar{B}_pe_6+\tilde{B}_pe_7+\bar{B}_we_8$.

对式(25)使用Jensen不等式, $\dot{V}_2(t)$满足

$$\begin{aligned}\dot{V}_2(t)\leqslant&\xi^{\rm T}(t)\Omega_1^{\rm T}(\eta_1^2Q_1+\eta_{31}^2Q_2+\eta_{23}^2Q_3)\Omega_1\xi(t)-\\ &\zeta_1^{\rm T}Q_1\zeta_1-\zeta_2^{\rm T}Q_2\zeta_2-\zeta_3^{\rm T}Q_2\zeta_3-\\ &{\rm sym}\{\zeta_2^{\rm T}U_2\zeta_3\}-\zeta_4^{\rm T}Q_3\zeta_4.\end{aligned}\tag{29}$$

其中: $\zeta_1=\zeta(t)-\zeta(t-\eta_1)$, $\zeta_2=\zeta(t-\eta(t))-\zeta(t-\eta_3)$, $\zeta_3=\zeta(t-\eta_1)-\zeta(t-\eta(t))$, $\zeta_4=\zeta(t-\eta_3)-\zeta(t-\eta_2)$.

$$\begin{aligned}\dot{V}_2(t)\leqslant&\xi^{\rm T}(t)\Omega_1^{\rm T}(\eta_1^2Q_1+\eta_{31}^2Q_2+\eta_{23}^2Q_3)\Omega_1\xi(t)-\\ &\xi^{\rm T}(t)((e_1-e_2)^{\rm T}Q_2(e_1-e_2))\xi(t)-\end{aligned}$$

$$\xi^{\mathrm{T}}(t)((e_3-e_5)^{\mathrm{T}}Q_1(e_3-e_5))\xi(t)-$$
$$\xi^{\mathrm{T}}(t)(\mathrm{sym}\{(e_3-e_5)^{\mathrm{T}}U(e_2-e_3)\})\xi(t)-$$
$$\xi^{\mathrm{T}}(t)((e_5-e_4)^{\mathrm{T}}Q_3(e_5-e_4))\xi(t)-$$
$$\xi^{\mathrm{T}}(t)((e_2-e_3)^{\mathrm{T}}Q_2(e_2-e_3))\xi(t). \quad (30)$$

将式(2)–(3)和式(19)代入式(26), $\dot{V}_1(t)$满足

$$\dot{V}_3(t)=-\delta_2\mu(t)+\varepsilon^2\bar{y}^{\mathrm{T}}(t)\phi\bar{y}(t)-\varphi^{\mathrm{T}}(t_k)\phi\varphi(t_k)\leqslant$$
$$\varepsilon^2\bar{y}^{\mathrm{T}}(t)\phi\bar{y}(t)-\varphi^{\mathrm{T}}(t_k)\phi\varphi(t_k)=$$
$$\xi^{\mathrm{T}}(t)(\Omega_2^{\mathrm{T}}\varepsilon^2\phi\Omega_2-e_6^{\mathrm{T}}\phi e_6)\xi(t), \quad (31)$$

其中$\Omega_2=3e_6+C_pE_ne_6$.

根据式(15)(28)(30)–(31), $\dot{V}(t)$满足

$$\dot{V}(t)\leqslant\xi^{\mathrm{T}}(t)\Sigma\xi(t)+e_y^{\mathrm{T}}(t)e_y(t)-e_y^{\mathrm{T}}(t)e_y(t)+$$
$$\lambda_2^2w^{\mathrm{T}}(t)w(t)-\lambda_2^2w^{\mathrm{T}}(t)w(t)+$$
$$z^{\mathrm{T}}(t)z(t)-z^{\mathrm{T}}(t)z(t)\leqslant$$
$$\xi^{\mathrm{T}}(t)\tilde{\Sigma}\xi(t)+\lambda_2^2w^{\mathrm{T}}(t)w(t)-z^{\mathrm{T}}(t)z(t), \quad (32)$$

其中:

$$\Sigma=\mathrm{sym}\{e_1^{\mathrm{T}}P\Omega_1\}+e_1^{\mathrm{T}}Re_1-e_2^{\mathrm{T}}Re_2+$$
$$\varepsilon^2\Omega_2^{\mathrm{T}}\phi\Omega_2+\Omega_1^{\mathrm{T}}(\eta_1^2Q_1+\eta_{31}^2Q_2+\eta_{23}^2Q_3)\Omega_1-$$
$$e_6^{\mathrm{T}}\phi e_6+\begin{bmatrix}e_2^{\mathrm{T}} & e_5^{\mathrm{T}}\end{bmatrix}S\begin{bmatrix}e_2\\e_5\end{bmatrix}-\begin{bmatrix}e_5^{\mathrm{T}} & e_4^{\mathrm{T}}\end{bmatrix}S\begin{bmatrix}e_5\\e_4\end{bmatrix}-$$
$$(e_1-e_2)^{\mathrm{T}}Q_2(e_1-e_2)-(e_3-e_5)^{\mathrm{T}}Q_1(e_3-e_5)-$$
$$(e_2-e_3)^{\mathrm{T}}Q_2(e_2-e_3)-(e_5-e_4)^{\mathrm{T}}Q_3(e_5-e_4)-$$
$$\mathrm{sym}\{(e_3-e_5)^{\mathrm{T}}U(e_2-e_3)\}, \quad (33)$$

$$\tilde{\Sigma}=\Sigma-e_7^{\mathrm{T}}e_7-\lambda_2^2e_8^{\mathrm{T}}e_8+e_1^{\mathrm{T}}\bar{F}_p^{\mathrm{T}}\bar{F}_pe_1+$$
$$(2e_6+C_pE_ne_3)^{\mathrm{T}}F^{\mathrm{T}}F(2e_6+C_pE_ne_3), \quad (34)$$

$$\Sigma_{12}=\mathrm{col}(\varepsilon\Omega_2,\Omega_3,\eta_1\Omega_1,\eta_{31}\Omega_1,\eta_{23}\Omega_3,M\Omega_4),$$
$$\Sigma_{22}=\mathrm{diag}\{-\phi^{-1},-I,-Q_1^{-1},-Q_2^{-1},-Q_3^{-1},-I\},$$

令$\Omega_3=\bar{F}_pe_1$, $\Omega_4=2e_6+C_pE_ne_3$, 得

$$\Sigma_{11}=\mathrm{sym}\{e_1^{\mathrm{T}}P\Omega_1\}+e_1^{\mathrm{T}}Re_1-e_2^{\mathrm{T}}Re_2-e_6^{\mathrm{T}}\phi e_6+$$
$$\begin{bmatrix}e_2^{\mathrm{T}} & e_5^{\mathrm{T}}\end{bmatrix}S\begin{bmatrix}e_2\\e_5\end{bmatrix}-\begin{bmatrix}e_5^{\mathrm{T}} & e_4^{\mathrm{T}}\end{bmatrix}S\begin{bmatrix}e_5\\e_4\end{bmatrix}-$$
$$(e_1-e_2)^{\mathrm{T}}Q_2(e_1-e_2)-(e_5-e_4)^{\mathrm{T}}Q_3(e_5-e_4)-$$
$$(e_3-e_5)^{\mathrm{T}}Q_1(e_3-e_5)-(e_2-e_3)^{\mathrm{T}}Q_2(e_2-e_3)-$$
$$\mathrm{sym}\{(e_3-e_5)^{\mathrm{T}}U(e_2-e_3)\}-\lambda_2^2e_8^{\mathrm{T}}e_8-e_7^{\mathrm{T}}e_7.$$

使用Schur引理, $\tilde{\Sigma}=\Sigma_{11}-\Sigma_{12}^{\mathrm{T}}\Sigma_{22}^{-1}\Sigma_{12}<0$, 定理3得证.　证毕.

5　反馈控制器设计

当$\tilde{\Sigma}<0$, 系统渐近稳定, 但是控制器各个增益矩阵存在耦合, 为求解增益矩阵, 需要解耦合.

定理 4　对于给定的采样周期$h>0$, 由网络引起的延迟$\bar{\tau}>\tau>\underline{\tau}>0$, 攻击相关矩阵$M>0$, 触发参数$\varepsilon>0$, 以及$\mathrm{H}_\infty$指标$\lambda_2>0$, 如果存在矩阵$\phi>0$, $\bar{S}>0,\bar{R}>0,\bar{Q}_i>0(i=1,2,3),\bar{U}_2,\bar{U}_3,X,M,Y$使得

$$\begin{bmatrix}\bar{Q}_2 & *\\ \bar{U}^{\mathrm{T}} & \bar{Q}_2\end{bmatrix}>0, \quad (35)$$

$$\begin{bmatrix}\bar{\Sigma}_{11} & *\\ \bar{\Sigma}_{21}^{\mathrm{T}} & \bar{\Sigma}_{22}\end{bmatrix}<0, \quad (36)$$

则系统渐近稳定且满足H_∞性能.

证　分解正定矩阵P可以得

$$P=\begin{bmatrix}X & Y\\ Y^{\mathrm{T}} & X_1\end{bmatrix},\ P^{-1}=\begin{bmatrix}M & N\\ N^{\mathrm{T}} & M_1\end{bmatrix},$$

其中$X,Y,X_1\in\mathbb{R}^{n\times n}$为正定矩阵.

定义矩阵$\Lambda_1=\begin{bmatrix}M & I\\ N^{\mathrm{T}} & 0\end{bmatrix}$, $\Lambda_2=P\Lambda_1=\begin{bmatrix}I & X\\ 0 & Y^{\mathrm{T}}\end{bmatrix}$.

当$X_1=Y^{\mathrm{T}}(X-M^{-1})^{-1}Y$, 对$P$使用Schur引理, 可得

$$T=\begin{bmatrix}M & I\\ I & X\end{bmatrix}>0.$$

定义矩阵$\Xi_1=\mathrm{diag}\{\Lambda_1,\Lambda_1\}$, $\Xi_2=\mathrm{diag}\{\Lambda_1,\Lambda_1,\Lambda_1,\Lambda_1,\Lambda_1,I,I,I,I,\Lambda_2,\Lambda_2,\Lambda_2,\Lambda_2,I\}$.

$$\begin{bmatrix}\bar{Q}_2 & *\\ \bar{U}^{\mathrm{T}} & \bar{Q}_2\end{bmatrix}=\Xi_1^{\mathrm{T}}\begin{bmatrix}Q_2 & *\\ U^{\mathrm{T}} & Q_2\end{bmatrix}\Xi_1>0,$$
$$\begin{bmatrix}\bar{\Sigma}_{11} & *\\ \bar{\Sigma}_{21}^{\mathrm{T}} & \bar{\Sigma}_{22}\end{bmatrix}=\Xi_2^{\mathrm{T}}\begin{bmatrix}\Sigma_{11} & *\\ \Sigma_{21}^{\mathrm{T}} & \Sigma_{22}\end{bmatrix}\Xi_2<0.$$

将式(23)中参数变化为

$$\bar{\Sigma}_{11}=$$
$$\mathrm{sym}\{e_1^{\mathrm{T}}\bar{\Omega}_1\}+e_1^{\mathrm{T}}\bar{R}e_1-e_2^{\mathrm{T}}\bar{R}e_2-e_6^{\mathrm{T}}\phi e_6+$$
$$\begin{bmatrix}e_2^{\mathrm{T}} & e_5^{\mathrm{T}}\end{bmatrix}\bar{S}\begin{bmatrix}e_2\\e_5\end{bmatrix}-\begin{bmatrix}e_5^{\mathrm{T}} & e_4^{\mathrm{T}}\end{bmatrix}\bar{S}\begin{bmatrix}e_5\\e_4\end{bmatrix}-$$
$$(e_1-e_2)^{\mathrm{T}}\bar{Q}_2(e_1-e_2)-(e_5-e_4)^{\mathrm{T}}\bar{Q}_3(e_5-e_4)-$$
$$(e_3-e_5)^{\mathrm{T}}\bar{Q}_1(e_3-e_5)-(e_2-e_3)^{\mathrm{T}}\bar{Q}_2(e_2-e_3)-$$
$$\mathrm{sym}\{(e_3-e_5)^{\mathrm{T}}\bar{U}_2(e_2-e_3)\},$$
$$\bar{\Sigma}_{12}=\mathrm{col}(\varepsilon\bar{\Omega}_2,\bar{\Omega}_3,\eta_1\bar{\Omega}_1,\eta_{31}\bar{\Omega}_1,\eta_{23}\bar{\Omega}_3,M\bar{\Omega}_4),$$
$$\bar{\Sigma}_{22}=\mathrm{diag}\{-\phi^{-1},-I,-T\bar{Q}_1^{-1}T,-T\bar{Q}_2^{-1}T,$$
$$-T\bar{Q}_3^{-1}T,-I\},$$

其中:

$$\bar{\Omega}_1=A_1e_1+A_2e_3+A_3e_6+A_4e_7+A_5e_8,$$
$$\bar{\Omega}_2=3e_6+A_6e_6,\ \bar{\Omega}_3=A_7e_1,$$
$$\bar{Q}_i=\Lambda_1^{\mathrm{T}}Q_i\Lambda_1,\ i=1,2,3,$$
$$\bar{U}=\Lambda_1^{\mathrm{T}}U\Lambda_1,\ \bar{S}=\Xi_1^{\mathrm{T}}S\Xi_1,\ \bar{R}=\Lambda_1^{\mathrm{T}}R\Lambda_1.$$
$$A_1=\begin{bmatrix}A_pM+B_pKN^{\mathrm{T}} & A_p\\ X^{\mathrm{T}}A_pM+X^{\mathrm{T}}B_pKN^{\mathrm{T}}+YA_{\mathrm{c}}N^{\mathrm{T}} & X^{\mathrm{T}}A_p\end{bmatrix},$$

$$A_2=\begin{bmatrix}0 & 0\\ YC_cC_pM+YB_cN^{\mathrm{T}} & YC_cC_p\end{bmatrix},$$

$$A_3=\begin{bmatrix}0\\ 2YC_c\end{bmatrix},\ A_4=\begin{bmatrix}0\\ YC_c\end{bmatrix},\ A_5=\begin{bmatrix}B_w\\ X^{\mathrm{T}}B_w\end{bmatrix},$$

$$A_6=[C_pM\ \ C_p],\ A_7=[F_pM\ \ G_pK].$$

令 $Z_1=YA_cN^{\mathrm{T}}$, $Z_2=YC_cC_pM+YB_cN^{\mathrm{T}}$, $Z_3=X^{\mathrm{T}}A_pM+X^{\mathrm{T}}B_pKN^{\mathrm{T}}+YA_cN^{\mathrm{T}}$, $Z_4=YC_c$.

由上述条件得到控制器相关增益矩阵

$$\begin{cases}N^{\mathrm{T}}=Y^{-1}(I-XM),\\ A_c=Y^{-1}Z_1(N^{\mathrm{T}})^{-1},\\ B_c=Y^{-1}(Z_3-Z_4C_pM)(N^{\mathrm{T}})^{-1},\\ C_c=Y^{-1}Z_4,\\ K=(X^{\mathrm{T}}B_p)^{-1}(Z_2-X^{\mathrm{T}}A_pM-Z_1)(N^{\mathrm{T}})^{-1}.\end{cases}\tag{37}$$

证毕.

注 4 定理3和定理4给出数据注入攻击下ICPS的自适应事件触发弹性控制分析, 为保证定理3和4中的LMI有解, 有如下步骤:

步骤 1 为使系统(21)渐近稳定且具有H_∞性能, 构造Lyapunov函数$V(t)$, 计算其导数得到式(24)–(26), 再通过Jesen不等式得到式(27)–(31), 根据式子(15)(28)(30)–(31)和假设1, 得到式(33)–(34), 对式子使用Schur引理, 得到$\dot V(t)<0$, 所以存在$\phi>0, P>0, S>0, R>0, Q_i>0(i=1,2,3), U$, 使得$\begin{bmatrix}Q_2 & *\\ U^{\mathrm{T}} & Q_2\end{bmatrix}>0$和$\begin{bmatrix}\Sigma_{11} & *\\ \Sigma_{21}^{\mathrm{T}} & \Sigma_{22}\end{bmatrix}<0$成立.

步骤 2 由于控制器增益矩阵与P之间存在耦合, 对定理3中的式(23)解耦, 分解正定矩阵P, 在式(23)左乘Ξ_1^{T}和右乘Ξ_1得式(35), 在式(24)左乘Ξ_2^{T}和右乘Ξ_2得式(36), 因此存在矩阵$\phi>0, \bar S>0, \bar R>0, \bar Q_i>0(i=1,2,3), \bar U_2$和$\bar U_3$, X, M, Y,使得$\begin{bmatrix}\bar Q_2 & *\\ \bar U^T & \bar Q_2\end{bmatrix}>0$和$\begin{bmatrix}\bar\Sigma_{11} & *\\ \bar\Sigma_{21}^{\mathrm{T}} & \bar\Sigma_{22}\end{bmatrix}<0$成立.

注 5 本文目的在于通过LKF推导出事件触发、数据注入攻击、网络延迟和弹性控制器之间的定量关系, 使系统渐近稳定且具有H_∞性能. 控制器增益矩阵需要通过式(36)求解得到, 而式(36)已保证系统渐近稳定且具有H_∞性能, 因此通过充分条件得到的控制器增益矩阵满足系统性能要求.

6 仿真

采用MATLAB仿真软件进行数据注入攻击下基于事件触发的ICPS模型的仿真. 以文献[20]系统简化的二自由度质量–弹簧–阻尼串联系统(结构如图2所示)为被控对象, 控制两个质量块的位移, 来验证所设计的模型的有效性和系统受到数据注入攻击时自适应事件触发和攻击估计模块对系统稳定性的影响.

为使两个质量块位移不发生偏移, 引入无线网络传输传感器测得两个质量块位移, 将数据传输至远程计算机, 通过控制器中的控制率得到相应的控制量, 再通过无线网络传输给质量块, 实现二自由度质量–弹簧–阻尼串联系统的质量块零位移控制.

图2中x_1, x_2, x_3, x_4分别代表质量块1和2的位移和速度, u_1和u_2为两个质量块受到的外力, $m_{1,2}$, $a_{1,2,3}$和$s_{1,2,3}$分别为质量、弹簧刚度和阻尼系数.

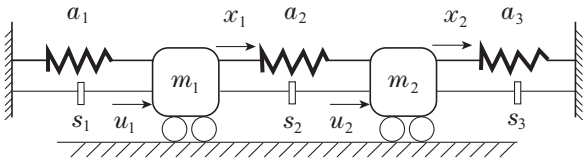

图 2 二自由度质量–弹簧–阻尼串联系统

Fig. 2 Two-degree-of-freedom mass-spring-damping series system

忽略摩擦等外界因素, 根据牛顿第二定律,可以得线性化的状态空间表达式为

$$\begin{bmatrix}\dot x_1\\ \ddot x_1\\ \dot x_2\\ \ddot x_2\end{bmatrix}=\begin{bmatrix}0 & 1 & 0 & 0\\ -\dfrac{a_1+a_2}{m_1} & -\dfrac{s_1+s_2}{m_1} & \dfrac{a_2}{m_1} & \dfrac{s_2}{m_1}\\ 0 & 0 & 0 & 1\\ \dfrac{a_2}{m_2} & \dfrac{s_2}{m_2} & -\dfrac{a_2+a_3}{m_2} & -\dfrac{s_2+s_3}{m_2} & 0\end{bmatrix}\times\begin{bmatrix}x_1\\ \dot x_1\\ x_2\\ \dot x_2\end{bmatrix}+\begin{bmatrix}0 & 0\\ 1 & 0\\ 0 & 0\\ 0 & 1\end{bmatrix}\begin{bmatrix}u_1\\ u_2\end{bmatrix},\tag{38}$$

$$y=\begin{bmatrix}x_1\\ x_2\end{bmatrix}=\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 0 & 1 & 0\end{bmatrix}\begin{bmatrix}x_1\\ \dot x_1\\ x_2\\ \dot x_2\end{bmatrix}.\tag{39}$$

令$a_1=a_2=a_3=s_1=s_2=s_3=0.01$, 得

$$A=\begin{bmatrix}0 & 1 & 0 & 0\\ -0.02 & -0.02 & 0.01 & 0.01\\ 0 & 0 & 1 & 0\\ 0.01 & 0.01 & -0.02 & -0.02\end{bmatrix},\ B=\begin{bmatrix}0 & 0\\ 1 & 0\\ 0 & 0\\ 0 & 1\end{bmatrix},$$

$$C=\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 0 & 1 & 0\end{bmatrix},\ B_w=\begin{bmatrix}0.01\\ 0.01\\ 0.01\\ 0.01\end{bmatrix},\ F_p=[1\,0\,0\,0],$$

$G_p=[0\ 0\ 0\ 0]$, $w(t)=\sin t$, $\lambda_2=2.168$,

$$F=\begin{bmatrix}0.8 & 0\\ 0 & 0.8\end{bmatrix},$$

采样周期$h=0.1$ s, 网络延迟下界$\underline{\tau}=0$ s, 延迟上界$\bar\tau=0.09$ s, 质量块速度与位移初始值$x_0=\begin{bmatrix}0.7\\ 0.6\\ -0.5\\ -0.4\end{bmatrix}$, 控制信号初始值为$\begin{bmatrix}0\\ 0\\ 0\\ 0\end{bmatrix}$, 攻击信号$f(\tilde y(t))=\begin{bmatrix}0.1y_2(t)\\ 0.1y_1(t)\end{bmatrix}$, 根据定理1和定理4, 再借助LMI工具箱可

以得

$$L=\begin{bmatrix}-0.0073 & 0.0037\\ -0.0195 & 0.0097\\ 0.0037 & -0.0073\\ 0.0097 & -0.01945\end{bmatrix},$$

$$B_a=\begin{bmatrix}-0.0005 & 0.0002\\ -0.1380 & -0.0018\\ 0.0002 & -0.0005\\ -0.0018 & -0.1380\end{bmatrix},$$

$$A_a=\begin{bmatrix}0.0164 & 1.0818 & -0.0082 & -0.0005\\ 0.1803 & -0.0212 & 0.0009 & 0.0107\\ -0.0082 & -0.0005 & 0.0164 & 1.0818\\ 0.0009 & 0.0106 & 0.1803 & -0.0212\end{bmatrix},$$

$$C_a=\begin{bmatrix}-0.0541 & 0.0003 & 0.0020 & -0.0001\\ 0.0020 & -0.0001 & -0.0541 & 0.0003\end{bmatrix},$$

$$D_a=\begin{bmatrix}0.1298 & -0.0015\\ -0.0015 & 0.1298\end{bmatrix},$$

$$A_c=\begin{bmatrix}1.7001 & 0.2769 & 0.8596 & 0.1240\\ -24.2849 & -3.3058 & -4.8419 & -0.8776\\ 0.8649 & 0.1238 & 1.6648 & 0.2740\\ -4.6747 & -0.8507 & -23.6266 & -3.2448\end{bmatrix},$$

$$B_c=\begin{bmatrix}-0.2083 & -0.0137 & -0.0260 & -0.0063\\ -0.1123 & -0.0081 & -0.0449 & -0.0054\\ -0.0261 & -0.0063 & -0.2085 & -0.0137\\ -0.0449 & -0.0054 & -0.1127 & -0.0081\end{bmatrix},$$

$$C_c=\begin{bmatrix}-0.5516 & 0.0432\\ -0.2963 & -0.0621\\ 0.0433 & -0.5525\\ -0.0622 & -0.2961\end{bmatrix},$$

$$K=\begin{bmatrix}0.3983 & 0.0537 & 0.0979 & 0.0164\\ 0.0956 & 0.0160 & 0.3877 & 0.0527\end{bmatrix}.$$

为系统稳定时间尽可能小和通信资源尽可能少, 图3中, 固定阈值事件触发参数ε选为0.0435, 引入的触发率等于触发次数除以采样次数, 固定阈值触发次数为415次, 触发率为41.5%, 节省通信资源58.5%, 触发间隔为0.013201 s, 而在自适应触发机制下, 触发次数只有233次, 触发率为23.3%, 节省通信资源76.7%, 触发时间间隔为0.032967 s. 因此, 当系统遭受攻击时, 自适应事件触发可以更有效地减少发次数, 而触发时间间隔增大也可以减少信道传输数据的次数, 在系统达到稳定情况下, 通信资源得到了有效减少.

图4给出攻击估计器中攻击信号在成功触发时的实际值和估计值随时间变化情况, 对攻击信号的估计准确率能达到60%以上, 攻击信号$0.1y_1(t)$的估计情况与此类似.

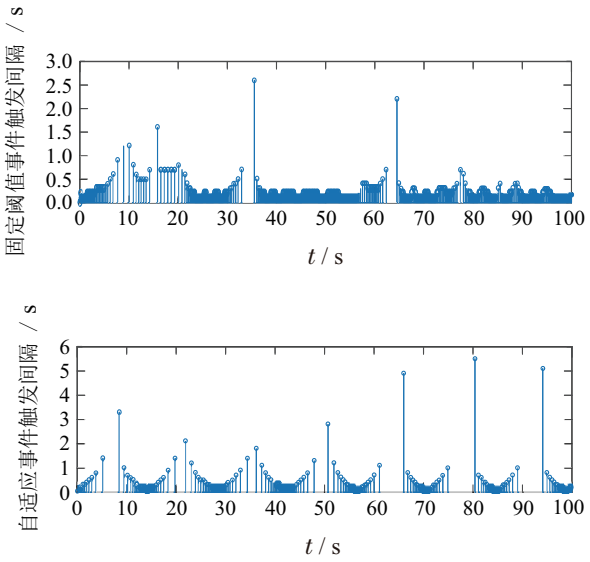

图 3　事件触发对比

Fig. 3　Event-triggered comparison

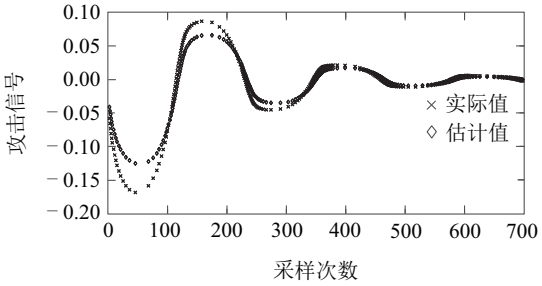

图 4　攻击估计

Fig. 4　Attack estimation

图5中, x_1为拥有攻击估计模块的自适应事件触发机制下的质量块2位移曲线, x_2为拥有攻击估计模块的固定阈值事件触发机制下的位移曲线, x_3为攻击估计模块的自适应事件触发机制下的位移曲线; x_1在56.7 s左右就可以到达零位移, x_2曲线需要66.2 s左右, x_3需要70 s, 而且x_1曲线位移变化的幅度最小, 相比较下, 攻击估计模块缓解了攻击对小车位移的影响, 而且自适应事件触发有利于遭受攻击后的系统恢复稳定.

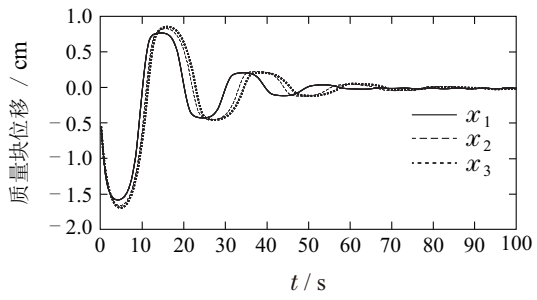

图 5　质量块2位移对比图

Fig. 5　Displacement comparison diagram of mass block 2

7　结论

为保证系统遭受数据注入攻击后的稳定和节省通信资源, 本文建立了事件触发控制下的ICPS模型, 通

过事件触发减少数据传输次数, 采用攻击估计模块和动态反馈控制器来缓解攻击对系统稳定性的影响, 采用MATLAB仿真, 以二自由度质量–弹簧–阻尼串联系统为仿真对象, 仿真结果表明, 采用事件触发机制的输出反馈模型以触发模块、攻击估计模块和控制器模块的组合, 可以缓解数据注入攻击对系统稳定性的影响, 有效减少通信资源的消耗. 本文的重点解决了恶意攻击对系统稳定性的影响, 并未指出攻击检测方法, 同时还需要提高攻击模块的精度. 未来的仿真将使用开源MATLAB工具箱epanetCPA[21]进行, 该工具箱可以快速设计各种攻击场景, 对配水系统的水力响应进行建模, 并通过EPANET仿真评估攻击的影响.

参考文献:

[1] WANG Zhongjie, XIE Lulu. Cyber-physical systems: A survey. *Acta Automatica Sinica*, 2011, 37(10): 1157 – 1166.
(王中杰, 谢璐璐. 信息物理融合系统研究综述. 自动化学报, 2011, 37(10): 1157 – 1166.)

[2] ARMANDO W C, STAMATIS K, CHRISTOPH H. Engineering human-focused industrial cyber-physical systems in industry 4.0 context. *Philosophical Transactions of the Royal Society A-Mathematical Physical and Engineering Sciences*, 2021, 379(2207): 20200366.

[3] DAFFLON B, MOALLA N, OUZROUT Y. The challenges, approaches, and used techniques of cps for manufacturing in industry 4.0: A literature review. *The International Journal of Advanced Manufacturing Technology*, 2021, 113(7): 2395 – 2412.

[4] GEISMANN J, BODDEN E. A systematic literature review of model-driven security engineering for cyber-physical systems. *Journal of Systems and Software*, 2020, 169: 110697.

[5] ZHANG D, CAI W, WANG Q G. A survey on attack detection, estimation and control of industrial cyber – physical systems. *ISA Transactions*, 2021, 116 : 1 – 16.

[6] LEE J, BAGHERI B, KAO H A. A cyber-physical systems architecture for Industry 4.0-based manufacturing systems. *Manufacturing Letters*, 2015, 3: 18 – 23.

[7] MAHMOUD M S, HAMDAN M M, BAROUDI U A. Modeling and control of cyber-physical systems subject to cyber attacks: A Survey of recent advances and challenges. *Neurocomputing*, 2019, 338: 101 – 115.

[8] XIANG Y M, WANG L F, LIU N. Coordinated attacks on electric power systems in a cyber-physical environment. *Electric Power Systems Research*, 2017, 149 : 156 – 168.

[9] HERBERT S. Why IIoT should make businesses rethink security. *Network Security*, 2019, 2019(7) : 9 – 11.

[10] MILLER T, STAVES A, MAESSCHALCK S, et al. Looking back to look forward: Lessons learnt from cyber-attacks on Industrial control systems. *International Journal of Critical Infrastructure Protection*, 2021, 35 : 100464.

[11] PETERSON J, HANEY M, BORRELLI R A. An overview of methodologies for cybersecurity vulnerability assessments conducted in nuclear power plants. *Nuclear Engineering and Design*, 2019, 346 : 75 – 84.

[12] CHAGANTI R, RAVI V, PHAM T D. A multi-view feature fusion approach for effective malware classification using deep learning. *Journal of Information Security and Applications*, 2023, 72: DOI: 10.1016/j.jisa.2022.103402.

[13] LI Y G, YANG G H. Optimal stealthy false data injection attacks in cyber-physical systems. *Information Sciences*, 2019, 481 : 474 – 490.

[14] ZHANG T Y, YE D. False data injection attacks with complete stealthiness in cyber – physical systems: A self-generated approach. *Automatica*, 2020, 120: 109117.

[15] YE D, ZHANG T Y. Summation detector for false data-injection attack in cyber-physical systems. *IEEE Transactions on Cybernetics*, 2019, 50(6) : 1 – 8.

[16] GUO H, PANG Z, SUN J, et al. Detection of stealthy false data injection attacks against networked control systems via active data modification. *Information Sciences*, 2021, 546: 192 – 205.

[17] ZHANG C L, YANG G H, LU A Y. Resilient observer-based control for cyber-physical systems under denial-of-service attacks. *Information Sciences*, 2021, 545 : 102 – 117.

[18] ZHANG Z H, LIU D, DENG C, et al. A dynamic event-triggered resilient control approach to cyber-physical systems under asynchronous DoS attacks. *Information Sciences*, 2020, 519: 260 – 272.

[19] ASTOLFI A, ORTEGA R. Immersion and invariance: A new tool for stabilization and adaptive control of nonlinear systems. *IEEE Transactions on Automatic Control*, 2003, 48(4) : 590 – 606.

[20] ZHANG X M, HAN Q L. Event-triggered dynamic output feedback control for networked control systems. *IET Control Theory and Applications*, 2014, 8(4) : 226 – 234.

[21] TAORMINA R, GALELLI S, TIPPENHAUER N O, et al. A toolbox for assessing the impacts of cyber-physical attacks on water distribution systems. *Environmental Modelling and Software*, 2018, 112 : 46 – 51.

作者简介:

薛威峰 硕士研究生, 目前研究方向为控制理论与控制工程, E-mail: 6201905052@stu.jiangnan.edu.cn;

孙子文 教授, 博士, 目前研究方向为控制理论与控制工程、模式识别、人工智能、无线传感网络理论与技术和信息安全, E-mail: sunziwen@jiangnan.edu.cn.