基于多信道博弈的ICPS虚假注入攻击防御策略

孙子文, 洪涛

引用本文:
孙子文,洪涛. 基于多信道博弈的ICPS虚假注入攻击防御策略[J]. 控制与决策, 2022, 37(5): 1357−1366.

在线阅读 View online: https://doi.org/10.13195/j.kzyjc.2020.1738

基于多信道博弈的ICPS虚假注入攻击防御策略

孙子文[1,2†], 洪 涛[1]

(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: 工业信息物理系统(ICPS)与基础设施的连接越来越密切,同时通信网络也易受到环境干扰和虚假数据注入攻击的影响. 鉴于此,研究基于多信道传输框架和minimax控制器,提高ICPS在攻击、环境和噪声干扰下的弹性. 通过设计minimax控制器以增强ICPS在噪音和干扰下的弹性,基于多信道传输框架建立发射机与攻击者之间的攻防博弈模型,通过多信道上的攻防博弈策略实现整个ICPS的弹性防御策略. 通过OPNET和Matlab的联调仿真,验证模拟数据注入攻击下基于多信道传输框架的ICPS控制系统的性能. 仿真结果表明,minimax控制器和多信道传输框架组成的弹性防御策略,能够同时提升系统在环境干扰下的稳定性并有效降低数据注入攻击对ICPS的影响.

关键词: 工业信息物理系统；数据注入攻击；零和博弈；多信道传输；minimax控制器

中图分类号: TP273 **文献标志码:** A

DOI: 10.13195/j.kzyjc.2020.1738

引用格式: 孙子文,洪涛. 基于多信道博弈的ICPS虚假注入攻击防御策略[J]. 控制与决策, 2022, 37(5): 1357-1366.

ICPS false injection attack defense strategy based on multi-channel game

SUN Zi-wen[1,2†], *HONG Tao*[1]

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

Abstract: The industrial cyber-physical system (ICPS) is increasingly connected to the infrastructure, meanwhile its communication network is vulnerable to environmental interference and false data injection attacks. Therefore, this paper studies a multi-channel transmission framework and a minimax controller to improve the elasticity of the ICPS under attack, environment interference and noise interference. The minimax controller is designed to enhance the elasticity of the ICPS under noise and interference. Furthermore, based on the multi-channel transmission framework, an attack-defense game model between the transmitter and the attacker is established, which uses the attack-defense game strategy to realize the elastic defense strategy of the whole ICPS. Through the joint debugging simulation of OPNET and Matlab, the performance of the ICPS control system based on the multi-channel transmission framework under data injection attacks is simulated. The simulation results show that the elastic defense strategy composed of the minimax controller and the multi-channel transmission framework can not only improve the stability of the system under environmental interference, but also reduce the impact of data injection attacks on the ICPS effectively.

Keywords: ICPS；data injection attacks；zero-sum game；multi-channel transmission；minimax controller

0 引 言

信息物理系统(cyber-physical-systems, CPS)是一种将网络与物理紧密连接的系统,它将传感、网络、控制、通信和计算技术集成到物理空间中[1], 旨在使它们更加安全、高效和可靠. 近年来,工业自动化控制与计算机、通信等技术深度结合,CPS被广泛应用于工业环境,形成了工业信息物理系统(industrial-cyber-physical-systems, ICPS)[2]. 然而, ICPS与许多关键基础设施的连接越来越密切,带来了遭受对手恶意网络攻击的风险. 在许多应用场景中,ICPS可能会因为这种干扰行为遭受严重的破坏[3],从而导致巨大的损失. 近年来已报道多起ICPS的安全事件,如在乌克兰电网遭受Black Energy 病毒袭击事件[4]、“Red October”行动破坏网络系统[5]、窃取世界各国凭据数据事件以及震惊世界的震网(Stuxnet)病毒袭击伊朗核电站系统事件[6]. 因此,网络攻击是ICPS不可忽视

收稿日期: 2020-12-13；**录用日期:** 2021-03-16.

基金项目: 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).

责任编委: 虞文武.

†通讯作者. E-mail: sunziwen@jiangnan.edu.com.

的威胁来源之一.

根据攻击模型的不同,将网络通信攻击分为拒绝服务(denial of service, DoS)攻击、虚假数据注入攻击和重放攻击[7],目前主要研究前两种网络攻击. 拒绝服务攻击着重于通过阻塞无线网络的通信通道并阻止远程端接收传输的数据来降低系统的性能. 与DoS攻击不同,虚假数据注入攻击通过拦截和修改传输的数据来恶化系统的性能,致力于破坏ICPS中传输数据的完整性和可用性. 虚假数据注入攻击者最关键的问题之一是如何保持隐身状态,即在不触发异常警报检测器的情况下注入伪造的信号.

近年来,已有专家学者在ICPS网络攻击领域开展了研究. 对虚假数据注入攻击在ICPS方面的安全问题研究主要聚焦于两方面:一是攻击方的最优攻击策略,二是防御方的攻击检测和安全控制策略. 对于最优攻击策略的研究,文献[8]利用统计特征计算远程误差,并利用KL(kullback-leibler)散度和互信息的性质,得到最坏情况的ε隐身虚假数据注入攻击策略;文献[9]以降低数据注入攻击可检测性为代价,提出了隐身信号攻击模型;文献[10]通过使用数据规划优化器快速求解得到攻击策略. 对于虚假数据注入攻击的入侵检测,检查接收数据特征的方法被广泛应用[11-12],文献[13]部署了分布式检测系统以防御虚假数据注入攻击,并从加权最小平方检测[14]、基于卡尔曼滤波器的检测[15]以及改进型的欧几里得检测器[16]等方面进行了研究. 安全控制策略属于攻击容忍的范畴,可用来验证系统是否保留在安全区域中[17]. 一些文献聚焦于鲁棒控制[18]和最优控制[19]等角度,从控制论的方法寻求解决方式. 从弹性控制的角度,基于事件触发的控制策略来保证受到攻击时系统期望的稳定性[20]. 上述文献都在数据注入攻击方面提出了改进方法,但无论是基于检查接收数据特征的检测方式,还是基于事件触发的安全控制策略,均未考虑工业环境中的干扰、噪声和ICPS环境中有限的通信资源.

博弈论方法在网络攻击和防御方面的研究也开始出现. 针对传感器节点阻塞攻击,基于零和博弈模型,提出一种重要节点抵御DoS攻击的保护决策方法[21];针对物理-网络协同攻击,基于随机博弈论提出一种令系统整体损失最小的防御资源分配最优策略[22]. 在受噪声和信号衰减影响的不可靠通信信道中,基于随机零和博弈框架提出一类输出反馈minimax控制器[23]. 在通信资源的约束下,提出一种纳什Q学习算法,模拟双方之间的交互式决策制定了博弈框架[24]. 大量文献在利用博弈论方法防御DoS攻击的方面进行了充分研究,而针对数据注入攻击的研究较少.

本文针对虚假数据注入攻击隐蔽性强等特点,综合上述文献提到的问题,考虑结合博弈论和基于多信道传输框架与minimax控制器构成的弹性防御策略,寻求ICPS面对数据注入攻击及环境干扰时的解决方法. 首先,设计基于minimax方案的反馈控制器,以增强噪声和干扰下ICPS的弹性;然后,通过多信道传输框架,建立发射机与攻击者之间的攻防博弈模型,研究基于双人随机马尔可夫博弈的弹性控制策略. 本文的主要内容如下:1)设计minimax控制器,增强ICPS面对噪音和环境干扰时的弹性;2)提出基于多信道框架的攻防博弈策略,增加ICPS抵抗数据注入攻击的能力,并且与minimax控制器结合,实现整个ICPS的弹性防御策略.

1 基于多信道传输框架的ICPS模型

虚假数据注入攻击可通过劫持物理设备或无线通信信道注入无用但存在安全隐患的数据,最终导致系统性能下降甚至崩溃. 虚假数据注入攻击需要知道系统相关模型知识,以便构成复杂的攻击策略绕过检测器的检测,该攻击具有一定的欺骗性,持续的虚假注入攻击会造成系统不稳定且令系统难以诊断,往往会造成比DoS攻击更大的威胁.

在无线网络的信息交换过程中,若传感器采用固定信道传输信息,则攻击者很容易通过频谱感测等技术快速检测到信号传输信道. 基于这些原因,设计基于多信道传输框架的ICPS模型,通过信道实时切换,采用多信道传输策略降低传输信号被网络攻击干扰的风险,提升系统对此类攻击的弹性.

1.1 基于多信道传输框架的ICPS模型分析

为降低数据注入攻击对系统的影响,同时针对数据注入攻击隐蔽性强、难以检测等特点,构建如图1所示的数据注入攻击下基于多信道传输框架的ICPS控制模型,主要包括被控对象、多信道传输框架、传感器系统、minimax控制器系统和执行器等. 多信道传输框架由多个发射机和接收器构成,每个发射机和相对应的接收器组成一条传输信道. minimax控制器系统包括缓存器、远程估计器和反馈控制器,缓冲器通过信息变化判断数据是否被篡改,远程估计器根据接收到的信号对系统状态进行动态估计,反馈控制器负责对系统进行反馈校正. 传感器系统获取到被控对象的各种状态,传递给决策者下一步的执行指令.

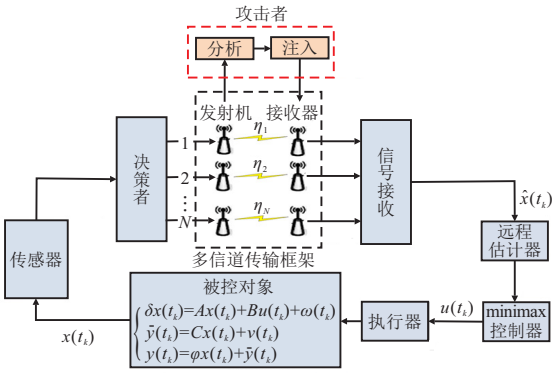

图 1　基于多信道传输框架的ICPS控制模型

假设控制器与被控对象通过可靠的网络连接,即控制器与被控对象之间的通信是安全的;同时假设传感器与动态估计器之间通过无线网络连接;决策者做出决策并发送信息,信号的发送和接收环节由N个发射机和接收器组成的多个无线信道完成,无线网络信道是不安全的.

1.1.1　虚假注入攻击模型

1) 攻击者能够对任意信息传输信道发起攻击. 攻击者在系统采样时刻t_k对N个信道的攻击策略矩阵为

$$\Gamma_k = \mathrm{diag}(\gamma_k^1, \ldots, \gamma_k^p, \ldots, \gamma_k^N). \tag{1}$$

其中$\gamma_k^p (p \in N \triangleq \{1, 2, \ldots, N\})$为攻击者的决策变量,表示攻击者对信道$p$发起的攻击.

2) 攻击发生后,攻击者通过传输信道向ICPS注入的偏差信号矢量为

$$\vec{a}_k = [a_k^1, \ldots, a_k^p, \ldots, a_k^N]^{\mathrm{T}}, \tag{2}$$

其中a_k^p为时刻t_k攻击者向信道p注入的偏差量. 基于攻击者具备的能力,建立虚假数据攻击数学模型

$$\tilde{x}_T(k) = x_T(k) + \Gamma_k a_k, \tag{3}$$

其中$\tilde{x}_T(k)$为系统受攻击后的远程估计器状态.

1.1.2　ICPS的离散线性时不变delta算子系统

鉴于delta算子方法可以有效克服由快速采样引起的数值刚度问题[25],在delta算子系统中,根据网络环境调整采样周期以减缓通信阻塞. 此外,连续时间和离散时间系统的相关结果在delta域中是统一的,因此本文系统在delta域中建立.

delta运算符为

$$\delta x(t_k) = \begin{cases} \mathrm{d}x(t)/\mathrm{d}t, \ h = 0; \\ (x(t_{k+1}) - x(t_k))/h, \ h \neq 0. \end{cases} \tag{4}$$

其中:h为采样周期,t为连续时间,$t_k = kh, k \in \boldsymbol{K} \triangleq \{0, 1, \ldots, K\}$为采样时刻,记$\{t_k\}$为采样时刻序列.

描述被控对象为离散线性时不变delta算子系统,有

$$\begin{aligned} \delta x(t_k) &= Ax(t_k) + Bu(t_k) + \omega(t_k), \\ \bar{y}(t_k) &= Cx(t_k) + v(t_k). \end{aligned} \tag{5}$$

其中:$x(t_k) \in R^{n_x}$、$u(t_k) \in R^{n_u}$分别为传感器获取的系统状态向量和控制输入向量; $\bar{y}(t_k) \in R^{n_y}$为系统未受攻击时的测量输出向量;n_x、n_u和n_y分别为状态向量、控制输入向量和测量输出向量的维度;$\omega(t_k) \in R^{n_\omega}$和$v(t_k) \in R^{n_v}$为干扰输入向量和测量噪声,$n_\omega$和$n_v$分别为其维度;$A$、$B$、$C$为时不变系统矩阵,分别是状态矩阵、控制矩阵和输出矩阵.

在受到攻击后,被控对象(5)更新为

$$\begin{aligned} \delta x(t_k) &= Ax(t_k) + Bu(t_k) + \omega(t_k), \\ y(t_k) &= \varphi(t_k)\bar{y}(t_k). \end{aligned} \tag{6}$$

虚假注入攻击对系统造成的影响由随机过程$\varphi(t_k)$体现,受到攻击的情况下系统接收到错误数据包时$\varphi(t_k) \neq 1$,即$y(t_k) = \varphi(t_k)\bar{y}(t_k)$;未受到攻击的情况下系统接收到正确数据包时$\varphi(t_k) = 1$,即$y(t_k) = \bar{y}(t_k)$. 令$\bar{\varphi} = \Pr\{\varphi(t_k) = 1\}$,$\bar{\varphi}$称为数据包平均正确率.

1.1.3　多信道传输机制

设N个信道对发射机和攻击者均具有独立的通信环境,即具有不同的信道增益. 设发射机与每条信道的增益为η_i,攻击者与每条信道的增益为ζ_i,每个信道i均具有不同的高斯白噪声δ_i^2,其中$i \in \boldsymbol{N} \triangleq \{1, 2, \ldots, N\}$.

发射机采用基于随机通信协议的马尔可夫跳跃机制选择传输信道. 设在采样时刻t_k发射机选择的信道$\theta_k = i$,在时刻t_{k+1}发射机选择的信道$\theta_{k+1} = j$,则发射机选择发送数据信道转移概率用条件概率为

$$p_T^{ij} = \Pr\{\theta_{k+1} = j | \theta_k = i\}, \ i, j \in \boldsymbol{N}. \tag{7}$$

攻击者采用同样的传输机制选择信道发起注入数据攻击. 用σ_k表示攻击者在时刻t_k选择的传输信道,则注入数据攻击信道的转移概率为

$$p_A^{ij} = \Pr\{\sigma_{k+1} = j | \sigma_k = i\}, \ i, j \in \boldsymbol{N}. \tag{8}$$

发射机和攻击者的转移概率可由功率分别表示[24]为

$$p_T^{ij} = \begin{cases} \mathrm{e}^{-W_T/a_i}, \ j = i; \\ a_j(1 - \mathrm{e}^{-W_T/a_i}) \Big/ \displaystyle\sum_{l \neq i}^{N} a_l, \ j \neq i. \end{cases} \tag{9}$$

$$p_A^{ij} = \begin{cases} \mathrm{e}^{-W_A/b_i}, \ j = i; \\ b_j(1 - \mathrm{e}^{-W_A/b_i}) \Big/ \displaystyle\sum_{l \neq i}^{N} b_l, \ j \neq i. \end{cases} \tag{10}$$

其中: W_T 和 W_A 分别为 t_k 时发射机和攻击者的发射功率; 参数 a_i、$b_i(i \in \boldsymbol{N})$ 为选择每条信道的期望, a_i 和 b_i 反映网络负载状况和信道增益, 其值越大, 网络环境越好[21], 反之网络环境越差.

比较式(9)两式可知, 当 $a_i < W_T/\ln\left(2+\sum\limits_{l\neq i,j}^{N} a_l\right)$ 时, 有 $p_T^{ii} < p_T^{ij}$, 此时发射机的发射功率 W_T 与 a_i 呈负相关, a_i 越小 W_T 越大, 不等式更容易成立. 由式(10)也能得出类似结论. 因此, 如果信道 i 上的传输环境越差, 即 a_i 或 b_i 越小, 则发射机或攻击者在其上消耗的功率越高, 意味着它们在下一个时刻越倾向于跳跃到转移概率值最大的信道 j 上去. 因此, 在 a_i 和 b_i 固定的情况下, 为达到减少功率消耗和网络堵塞的目的, 可通过调整发射功率的值得到合适的转移概率.

1.2 基于多信道传输框架的ICPS模型设计

为了增强系统在虚假数据注入攻击下的弹性, 建立多信道传输框架. 同时, 由于ICPS通信资源的有限性, 还需结合无线通信资源的合理使用策略, 研究minimax方案的控制器, 保证ICPS合理利用通信资源, 提高系统在攻击、环境和噪声干扰下的弹性.

1.2.1 缓存器设计

在信号接收端与估计器之间设置缓存器, 将缓冲器中的数据与当前时刻接收到数据相比较, 判断经过多信道传输的数据是否遭受到虚假数据注入攻击.

设采样时刻 t_k 缓存器中存储了 e 个历史接收到的数据, 即

$$\{y(t_{k-e}), y(t_{k-e+1}), \ldots, y(t_{k-2}), y(t_{k-1})\}, \tag{11}$$

则时刻 t_k 缓存器中数据的均值为

$$\bar{y}_e(t_k) = \sum_{i=k-e+1}^{k-1} y(t_i). \tag{12}$$

给出系统在时刻 t_k 是否受到攻击的初始估计判断

$$\begin{cases} |y(t_k) - \bar{y}_e(t_k)| \leqslant \Delta, \text{ security;} \\ |y(t_k) - \bar{y}_e(t_k)| > \Delta, \text{attacked.} \end{cases} \tag{13}$$

其中 Δ 为一个系统正常工作能容忍的偏差.

对于式(6)中的 $\varphi(t_k)$, 令 $\varphi(t_k)=\alpha$, 有

$$\alpha = \begin{cases} 1, \ |y(t_k) - \bar{y}_e(t_k)| \leqslant \Delta; \\ 1 - \dfrac{|y(t_k) - \bar{y}_e(t_k)|}{\bar{y}_e(t_k)}, \ |y(t_k) - \bar{y}_e(t_k)| > \Delta. \end{cases} \tag{14}$$

当 $\alpha = 1$ 时, 系统未受到攻击; 当 $\alpha \neq 1$ 时, 系统受到虚假注入攻击, 接收到了错误数据包.

1.2.2 多信道结构模型

多信道结构模型由传感器系统、通信系统和远程估计器3部分组成.

最新技术的ICPS中, 传感器通常被设计为采用先进嵌入式技术的“智能系统”[26], 集成具备存储和计算功能的多功能芯片, 同时使传感器节点还可以执行一些简单的递归算法来处理收集信息. 在图1的传感器系统部分, 传感器节点先按照采样时刻序列进行测量, 再运行集成的卡尔曼滤波器来估计状态 $x(t_k)$.

定义时刻 t_k 时 $x(t_k)$ 的局部最小均方误差为

$$\hat{x}^s(t_k) = E[x(t_k)|y(t_0), \ldots, y(t_k)], \tag{15}$$

对应的估计误差为

$$e^s(t_k) \triangleq x(t_k) - \hat{x}^s(t_k), \tag{16}$$

误差协方差为

$$P^s(t_k) \triangleq E[(e^s(t_k))(e^s(t_k))'|y(t_0), \ldots, y(t_k)]. \tag{17}$$

上述值通过卡尔曼滤波器计算, 从 $\hat{x}^s(t_0) = 0$ 开始迭代. 通信系统部分由 N 个传输信道组成, 其中每个信道均有独立的通信环境和不同的高斯白噪声. 在计算获得 $\hat{x}^s(t_k)$ 后, 传感器将通过通信系统将数据包发送给远程估计器.

对于远程估计器部分, 设 $x(t_k)$ 在远程估计器上的局部最小均方误差为 $\hat{x}(t_k)$, 利用过程(18)获得状态估计值[27]: 如果通过信道传输的信号准确到达, 即成功获取 $\hat{x}^s(t_k)$, 则估算器将同步其估算值 $\hat{x}(t_k)$, 否则估算器会根据系统模型(6)使用上一刻的估算值进行估计预测. 有

$$\hat{x}(t_k) = \begin{cases} \hat{x}^s(t_k), \ \varphi(t_k) = 1; \\ A\hat{x}(t_{k-1}), \ \varphi(t_k) \neq 1. \end{cases} \tag{18}$$

同理, 远程估计器上的误差协方差 $P(t_k)$ 在采样时间 t_k 服从下式:

$$P(t_k) \triangleq E[(x(t_k) - \hat{x}(t_k))(x(t_k) - \hat{x}(t_k))'] = \begin{cases} \bar{P}, \varphi(t_k) = 1; \\ h(P_{k-1}), \varphi(t_k) \neq 1. \end{cases} \tag{19}$$

定义Lyapunov运算符 h 和Riccati运算符 $\tilde{g}$, 有

$$h(X) \triangleq AXA' + Q,$$

$$\tilde{g}(X) \triangleq X - XC'[CXC' + R]^{-1}CX.$$

则误差协方差 $P^s(t_k)$ 指数收敛到属于 $h \circ \tilde{g}$ 的唯一固定点 $\bar{P}$[28].

1.2.3 minimax控制器设计

为了在受到环境和噪声干扰时获得最佳输出反馈控制器, 设计minimax控制器, 在干扰最大的情况下保持控制器的成本函数最小, 针对环境干扰和控制器本身采用零和动态博弈达到目的.

假设系统是基于用户数据报协议(user datagram

protocal, UDP)的通信,在采样时刻t_k传输给远程估计器的信息表示为$\mathcal{I}(t_k)$. 定义控制器的控制策略为μ,环境干扰的干扰策略为v,控制策略和干扰策略为

$$u(t_k)=\mu(\mathcal{I}(t_k)),\ k\in K;$$
$$\omega(t_k)=v(\mathcal{I}(t_k)),\ k\in K. \tag{20}$$

设控制器的最小化成本函数为

$$\mathcal{T}_\mu^K=\sup_{x(t_0),\omega(t_k),k\in\boldsymbol{K}}\frac{J^K(\mu,\nu)^{1/2}}{E\Big\{\|x(t_0)\|_{Q_0}^2+T_k\sum\limits_{k=0}^{K-1}\mathcal{M}(t_k)\Big\}^{1/2}}. \tag{21}$$

其中: $J^K(\mu,v)$为状态和控制输入引起的成本函数, $\mathcal{M}(t_k)$为由干扰和噪音引起的成本函数,且有

$$J^K(\mu,\nu)=E\Big\{\|x(t_K)\|_{Q_K}^2+T_k\sum_{k=0}^{K-1}(\|x(t_k)\|_Q^2+\|u(t_k)\|_R^2)\Big\},$$
$$\mathcal{M}(t_k)=\|\omega(t_k)\|^2+\beta(t_k)\|v(t_k)\|^2,$$
$$Q\geqslant 0, Q_K\geqslant 0, R>0, Q_0>0. \tag{22}$$

式(16)可看作是H_∞最优控制问题,引入零和动态博弈解决H_∞最优控制问题(21), 博弈的元素为: 1) 参与者,主动方为干扰,从动方为控制器; 2) 动作,干扰策略v和控制策略μ.

针对系统(5),控制器的收益函数由式(22)中的第1式更新为

$$J_\gamma^K(\mu,\nu)=E\Big\{\|x(t_K)\|_{Q_K}^2-\gamma^2\|x(t_0)\|_{Q_0}^2+T_k\sum_{k=0}^{K-1}(\|x(t_k)\|_Q^2+\|u(t_k)\|_R^2-\gamma^2\mathcal{M}(t_k))\Big\}, \tag{23}$$

其中γ为干扰衰减参数,用于衡量系统对环境干扰的鲁棒性,最小的γ可以描述系统在干扰和不利环境下的操作范围[29].

在博弈中,控制器的目标是使式(23)最小化, 即$\min\limits_{\mu}J_\gamma^K(\mu,\nu^*)$,干扰的目标是使式(23)最大化,即$\max\limits_{\nu}J_\gamma^K(\mu^*,\nu)$.

定义1　双人控制器干扰博弈中,若下式存在:

$$J_\gamma^K(\mu^*,\nu)\leqslant J_\gamma^K(\mu^*,\nu^*)\leqslant J_\gamma^K(\mu,\nu^*), \tag{24}$$

则(μ^*,ν^*)为零和动态博弈系统(23)基于γ的鞍点.

基于γ的零和动态博弈(18),其成本函数最小化问题是找到一个鞍点解,而鞍点解取决于γ,这意味着在minimax控制器下,将通过最小的γ值获得J_γ^K的有限值. 因此,需要先描述出最小的干扰衰减参数γ,用$\hat{\gamma}$表示. 根据定义1,对于任意$\gamma>\hat{\gamma}$,鞍点解(μ^*,ν^*)存在,但前提为$\hat{\gamma}$是有限的.

为了求解出鞍点解,获得最合适的控制策略和干扰策略,从而得到最佳的输出反馈minimax控制器,引出定理1.

定理1　考虑式(23)中的零和动态博弈,对于固定的$\gamma>0$,可以得到以下结论:

1) 当且仅当对于所有$k\in\boldsymbol{K}\setminus K$,存在一个唯一的输出反馈鞍点解决方案

$$R+T_kB^{\mathrm{T}}(t_k)Z(t_{k+1})B(t_k)>0,$$
$$T_kD^{\mathrm{T}}(t_k)Z(t_{k+1})D(t_k)<\gamma^2I. \tag{25}$$

其中Z_k满足耦合广义Riccati方程(GREs):

$$\begin{aligned}-\delta Z(t_k)=&Q+P_u^{\mathrm{T}}(t_k)RP_u(t_k)-\gamma^2P_\omega^{\mathrm{T}}(t_k)P_\omega(t_k)+\\&T_k\mathcal{A}^{\mathrm{T}}(t_k)Z(t_{k+1})\mathcal{A}(t_k)+\\&\mathcal{A}^{\mathrm{T}}(t_k)Z(t_{k+1})+Z(t_{k+1})\mathcal{A}(t_k),\\Z(t_k)=&Z(t_{k+1})-T_k\delta Z(t_k).\end{aligned} \tag{26}$$

其中

$$\begin{aligned}P_u^{\mathrm{T}}(t_k)=&(R+T_kB^{\mathrm{T}}(t_k)\Lambda_u(t_k)Z(t_{k+1})B(t_k))^{-1}\times\\&B^{\mathrm{T}}(t_k)\Lambda_u(t_k)Z(t_{k+1})(T_kA(t_k)+I),\\P_\omega^{\mathrm{T}}(t_k)=&(\gamma^2I-T_kD^{\mathrm{T}}(t_k)\Lambda_\omega(t_k)Z(t_{k+1})D(t_k))^{-1}\times\\&D^{\mathrm{T}}(t_k)\Lambda_\omega(t_k)Z(t_{k+1})(T_kA(t_k)+I),\\\mathcal{A}(t_k)=&A(t_k)-B(t_k)P_u(t_k)+D(t_k)P_\omega(t_k),\\M_1(t_k)=&R+T_kB^{\mathrm{T}}(t_k)Z(t_{k+1})B(t_k),\\M_2(t_k)=&\gamma^2I-T_kD^{\mathrm{T}}(t_k)Z(t_{k+1})D(t_k),\\\Lambda_u(t_k)=&I+T_kZ(t_{k+1})D(t_k)M_2^{-1}(t_k)D^{\mathrm{T}}(t_k),\\\Lambda_\omega(t_k)=&I-T_kZ(t_{k+1})B(t_k)M_1^{-1}(t_k)B^{\mathrm{T}}(t_k).\end{aligned} \tag{27, 28}$$

2) 相应的鞍点解(μ^*,ν^*)如下:

$$u^*(t_k)=-P_u(t_k)x(t_k),$$
$$\omega^*(t_k)=P_\omega(t_k)x(t_k). \tag{29}$$

由此,得到最佳的输出反馈minimax控制器.

2　虚假数据注入攻击下的多信道ICPS防御策略

为使ICPS免于遭受虚假数据注入攻击,建立基于多信道传输框架的信息跳跃机制,以降低攻击影响. 通过建立发射机与攻击者之间的攻防博弈模型,进一步引入系统在多信道上的攻防博弈策略,从而实现整个ICPS的弹性防御策略.

2.1　攻防博弈模型

设计一个双人马尔可夫随机博弈处理发射机与攻击者之间的交互过程. 双人马尔可夫随机博弈的

元素如下:

1) 参与者:安装在传感器中的发射机和进行虚假注入攻击的攻击者.

2) 状态:将双方的状态r_k定义为在发送方和攻击方的通道选择,即$r_k = (\theta_k, \sigma_k)$. θ_k表示采样时刻t_k发射机选择的信道,σ_k表示采样时刻t_k攻击者选择的信道.

3) 动作:发射机的动作用发射功率$W_T^k \in W_T \triangleq [0, W_T^{\max}]$表示,攻击者的动作用干扰功率$W_A^k \in W_A \triangleq [0, W_A^{\max}]$表示.

4) 过渡概率:由式(7)~(10)可知,下一时刻t_{k+1}状态是基于t_k时刻的过程状态,发送者的行为和攻击者的行为分别为W_T^k和W_A^k. 状态转移概率为

$$\Pr(r_{k+1}|r_k, W_T, W_A) = \Pr\{\theta_{k+1}|\theta_k\}\Pr\{\sigma_{k+1}|\sigma_k\} = p_T^{\theta_k\theta_{k+1}} p_A^{\sigma_k\sigma_{k+1}}. \quad (30)$$

5) 成本:发射机在t_k时刻的成本函数定义为

$$R_k(r_k, W_T^k, W_A^k) = c_0\hat{\gamma}(k) + c_1 W_T^k - c_2 W_A^k + C_0. \quad (31)$$

其中:正标量c_0、c_1、c_2为权重系数,参数C_0为固有成本,$\hat{\gamma}(k)$为代表ICPS 的系统性能.成本函数(31)意味着防御策略的目的旨在将控制系统的干扰衰减参数降至最低,同时将其能耗也降至最低.

博弈双方会考虑长期收益,发射机和攻击者总的贴现成本为

$$Q_T(r_0) = Q(r_0),\ Q_A(r_0) = -Q(r_0), \quad (32)$$

$$Q(r_0) = \sum_{n=1}^{+\infty} \rho^k R_k(r_k, W_T^k, W_A^k). \quad (33)$$

其中:$Q_T(r_0)$为发射机的贴现成本,$Q_A(r_0)$为攻击者的贴现成本,参数ρ为贴现因子,$\rho \in [0, 1)$,r_0为双方的初始状态.

在博弈过程中,攻防双方都尽力采取最优控制策略力求实现回报最大化.在博弈过程中出现的平衡点成为纳什均衡点,双方若在该点改变策略均不会获得更好的回报,因此双方一般都不会在该点主动改变策略.根据纳什均衡点定义,旨在寻求式(33)中贴现成本函数的纳什均衡,使得下式成立:

$$Q(W_T^*, W_A) \leqslant Q(W_T^*, W_A^*) \leqslant Q(W_T, W_A^*). \quad (34)$$

其中$Q = [Q^*(1), Q^*(2), \ldots, Q^*(r), \ldots]$.

在求解时,纳什均衡点对应的攻防策略集合(W_T^*, W_A^*)总是成对出现,同时求解. 在攻防过程中,攻防双方根据各自的策略集合,根据概率分布随机抽取各自的攻防目标采取攻防动作.

2.2 弹性防御策略

发射机为了达到纳什均衡,实现系统的弹性防御策略,引入引理1.

引理1 对于式(33)提出的纳什均衡条件,可以将其视为马尔可夫决策过程中的贴现成本问题,其最优值$Q^*(r)$满足以下贝尔曼方程:

$$Q^*(r) = \min_{T_k}\max_{W_k}\{R(r, W_T, W_A) + \rho\sum_{r'\in \boldsymbol{R}} \Pr\{r'|r, W_T, W_A\}Q^*(r)\}. \quad (35)$$

由于发射机和攻击者的传输功率是有限的,即$W_T^k \in W_T \triangleq [0, W_T^{\max}]$, $W_A^k \in W_A \triangleq [0, W_A^{\max}]$,物理元件之间的功率传输并非采用模拟信号,而是粗略量化之后将其发送. 假设存在一个有限的功率水平L,发射机和攻击者的功率水平分别为$W_T = \{W_T^1, W_T^2, \ldots, W_T^{L_T}\}$, $W_A = \{W_A^1, W_A^2, \ldots, W_A^{L_A}\}$. 定义一个辅助矩阵

$$K(r) = [K(r)]_{L_T\times L_A},\ r \in \boldsymbol{R}. \quad (36)$$

其中

$$K^{ij}(r, W_T^i, W_A^j) = R(r, W_T^i, W_A^j) + \rho\sum_{r'\in \boldsymbol{R}} \Pr\{r'|r, W_T^i, W_A^j\}Q^*(r'). \quad (37)$$

引入定理2给出最佳混合策略.

定理2 贴现零和随机博弈(24)具有最优值$Q^*(r), \forall r \in \boldsymbol{R}$,且为以下方程的唯一解:

$$Q^*(r) = \min_{\pi_T}\max_{\pi_W}\{K(r)\}, \quad (38)$$

其中$\pi_T \in P(W_T)$、$\pi_W \in P(W_A)$、$P(W_T)$和$P(W_A)$分别为功率水平集W_T和W_A上的概率分布集.定理2 可以通过Shapley定理进行证明[22],此略.

采用值迭代方法可以求解式(38)中的随机零和博弈,通过引理1和定理2提出计算最小干扰衰减参数$\hat{\gamma}$算法和ICPS总体弹性防御策略算法,算法流程分别如图2和图3 所示.

算法1 最小干扰衰减参数$\hat{\gamma}$算法.

step 1: 对于确定的数据包平均正确率$\bar{\varphi}$,取一个足够大的值$\gamma > 0$和一个足够小的标量$\Delta\gamma$.

step 2: 当$\gamma > 0$时,计算式(21)中的Riccati方程,如果计算结果满足式(20), 则取$\gamma = \gamma - \Delta\gamma$,转至step 1.

step 3: 若step 2的计算结果不满足式(20),则此时获得的γ为对应$\bar{\varphi}$的最小干扰衰减参数.

算法2 ICPS总体弹性防御策略算法.

step 1: 给定贴心因子ρ、功率水平集W_T和W_A、权重系数c_0、c_1和c_2以及固有成本C_0. 初始化参数

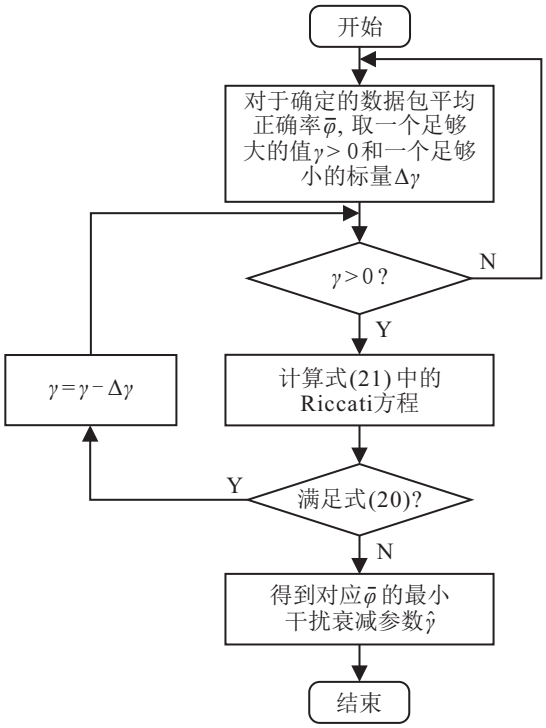

图 2　计算最小干扰衰减参数$\hat{\gamma}$算法流程

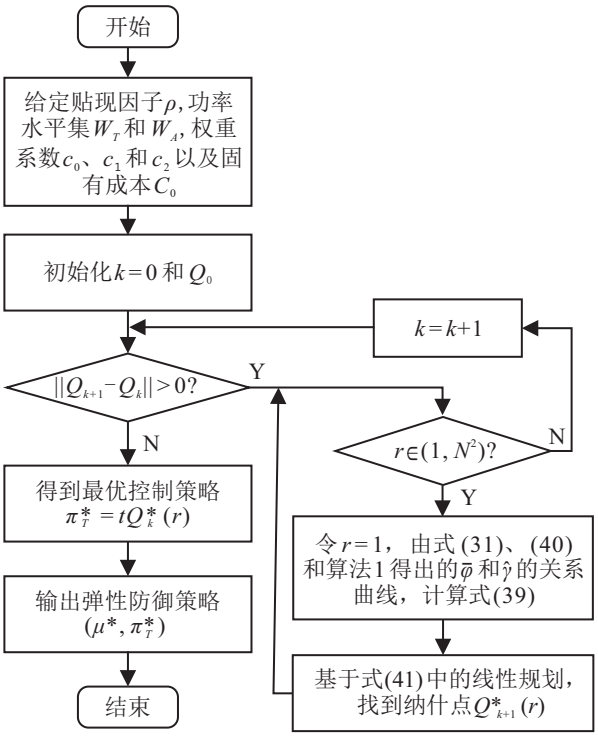

图 3　ICPS弹性防御策略算法流程

Q_0, 令$k=0$.

step 2: 当$\|Q_{k+1}-Q_k\|>0$成立时, 在集合$(1,N^2)$的范围内, 令r从1开始, 计算如下价格矩阵:

$$K_k(r)=[K_k^{ij}(r)]_{L_T\times L_A}. \tag{39}$$

式(39)是基于算法1中$\bar{\varphi}$与$\hat{\gamma}$的关系曲线、式(31)和下式得到的:

$$K_k^{ij}(r,W_T^i,W_A^j)=R_k(r,W_T^i,W_A^j)+\rho\sum_{r'\in\boldsymbol{R}}\Pr\{r'|r,W_T^i,W_A^j\}Q_k^*(r'). \tag{40}$$

step 3: 计算下式的线性规划:

$$\begin{cases}1/Q_{k+1}^*(r)=\max\limits_t t^{\mathrm{T}}1_{L_T},\\ K_k^{\mathrm{T}}(r)t\leqslant 1_{L_A},\ t\geqslant 0,\end{cases} \tag{41}$$

根据计算结果找到纳什点$Q_{k+1}^*(r)$.

step 4: r在$(1,N^2)$的范围内计算完毕后, 令$k=k+1$, 再次判断$\|Q_{k+1}-Q_k\|>0$是否成立. 如果成立, 则转至step 2进行计算, 否则说明得到了最优控制策略$\pi_T^*=tQ_k^*(r)$. 通过求解式(41)的对偶问题可以得到攻击者的最优混合策略π_W^*, 输出此时的弹性防御策略(μ^*,π_T^*).

3　仿真与结果

以倒立摆为对象, 通过Matlab的Simulink/Truetime与OPNET联调仿真, 验证minimax控制器对抵御干扰和噪声的有效性, 以及弹性防御策略对抵御数据注入攻击的弹性.

3.1　仿真模型与参数设置

采用一级直线型倒立摆系统[30]作为被控对象, 倒立摆系统主要由倒立摆机构、传输信道和计算机控制端3部分构成, 如图4所示. 倒立摆作为一个经典的控制装置, 其控制目标是使摆杆始终保持在垂直方向上. 计算机控制端经过采集通过无线传感器传输的摆杆角位移参数与小车的位移量等参数, 采用算法计算出控制量, 再将控制信号通过无线网络发送回小车. 控制信号再经数模转换驱动执行器直流电机转化为施加在小车上的力, 从而实现倒立摆的实时控制, 使其处于垂直状态. 在无线通信传输过程中, 攻击者可以对倒立摆系统的任意信道发起虚假数据注入攻击.

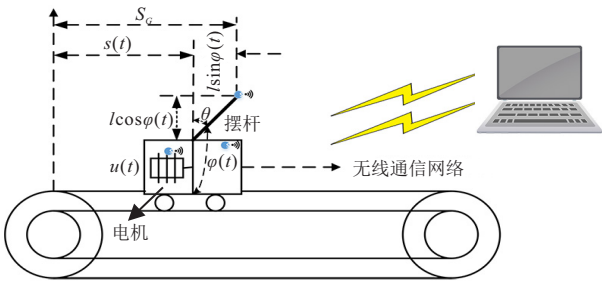

图 4　倒立摆系统

忽略空气阻力以及物体之间的摩擦力, 将倒立摆系统抽象为均质摆杆和小车组成的系统. 设M和m分别为小车和摆杆的质量, l为摆杆的转动轴心到摆杆质心的长度, I为摆杆惯量, $u(t)$为小车受到的水

平方向的力,b为小车的摩擦系数,$s(t)$和$\theta(t)$分别为小车相对初始点的位置以及摆杆与垂直方向向上的夹角,$\varphi(t)$为摆杆与垂直方向向下的夹角,其中$s(t)$、$\theta(t)$和$\varphi(t)$均可由传感器节点实时测量. 倒立摆的参数设置[30]为: $M = 1.096\,\text{kg}, m = 0.109\,\text{kg}, b = 0.1, l = 0.25\,\text{m}, I = 1.003\,4$. 倒立摆平衡方程为

$$\ddot{\theta}(t) = \frac{X_1}{X}\theta(t) - \frac{ml}{X}u(t), \tag{42}$$

$$\ddot{s}(t) = -\frac{X_2}{X}\theta(t) + \frac{X_3}{X}. \tag{43}$$

其中

$$X = (M+m)I + Mml^2,\ X_1 = m(m+M)gl,$$
$$X_2 = m^2gl^2,\ X_3 = I + ml^2.$$

应用牛顿-欧拉方程对系统进行线性化,可得系统的连续状态空间表达式

$$\begin{bmatrix}\dot{s}\\ \ddot{s}\\ \dot{\theta}\\ \ddot{\theta}\end{bmatrix} = \begin{bmatrix}0 & 1 & 0 & 0\\ 0 & \dfrac{-X_3b}{X} & \dfrac{X_2}{X} & 0\\ 0 & 0 & 0 & 1\\ 0 & \dfrac{-(mlb)}{X} & \dfrac{X_1}{X} & 0\end{bmatrix}\begin{bmatrix}s\\ \dot{s}\\ \theta\\ \dot{\theta}\end{bmatrix} + \begin{bmatrix}0\\ \dfrac{X_3}{X}\\ 0\\ \dfrac{ml}{X}\end{bmatrix}u, \tag{44}$$

$$y = \begin{bmatrix}s\\ \theta\end{bmatrix} = \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 0 & 1 & 0\end{bmatrix}\begin{bmatrix}s\\ \dot{s}\\ \theta\\ \ddot{\theta}\end{bmatrix}. \tag{45}$$

将表1中的参数代入式(25)和(26),采样周期取$h = 0.01\,\text{s}$,进行离散化得到

$$A = \begin{bmatrix}1.38 & -0.207\,7 & 6.715 & -5.676\\ -0.581\,4 & -4.29 & 0 & 0.675\\ 1.067 & 4.273 & -6.654 & 5.893\\ 0.048 & 4.273 & 1.343 & -2.104\end{bmatrix},$$

$$B = \begin{bmatrix}0\\ 0.051\\ 0\\ 0.015\end{bmatrix},\ C = \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 0 & 1 & 0\end{bmatrix}.$$

干扰输入$\omega(t_k)$和测量噪声$v(t_k)$的大小为$[-0.4, 0.4]$的均匀分布.

3.2 仿真结果与分析

Truetime工具箱没有对信道的建模过程,难以引入干扰攻击节点,因此利用OPNET的无线信道建模功能对ICPS的多信道进行建模,同时添加数据注入攻击节点,对受到数据注入攻击的ICPS的稳定性能进行仿真. OPNET的网络仿真参数如表1所示.

在ICPS仿真模型中,仿真时长设置为10 s,采样周期为$h = 0.01\,\text{s}$,需通过无线网络发送1 000次数据,$K = 500$,干扰衰减参数设置为$\gamma = 20$.

表 1 OPNET网络仿真参数

场景及节点参数	取值
仿真工具版本	OPNET14.5
MAC层	TDMA
传输速率/(Kbit/s)	250
工作频段/GHz	2.4
包大小/byte	256
仿真范围/m	10×10
节点个数	5

3.2.1 minimax控制器抵御环境干扰的性能

图5显示了系统未受到攻击时摆杆的偏移角度. PSM (perfect state measurements)为系统未受到干扰和噪声影响的理想状态测量, IPSM (imperfect state measurements)为系统受到干扰和噪声影响的非理想状态测量. 初始状态下摆杆的偏移角度为0.35 rad, 0时刻后因小车受到作用力的干扰,摆杆开始摆动,其偏移角度受时间、PSM/IPSM和是否受到数据注入攻击等因素的影响.

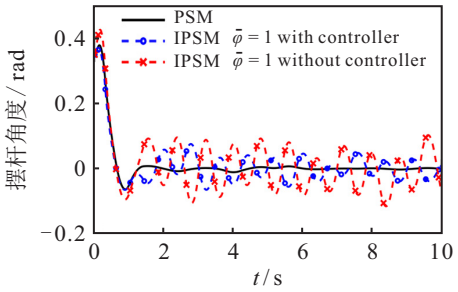

图 5 未受攻击时摆杆的偏移角度

1) 在理想测量状态:摆杆从最大偏移角度快速降低,在0.9 s时偏移到反方向的最大角度,并在1.5 s左右调节至0 rad,随后摆杆一直保持接近竖直的状态.

2) 在非理想测量状态且$\bar{\varphi} = 1$:当minimax控制器没有发挥作用时,摆杆在1 s后的平均偏移角度为0.139 9 rad;当minimax发挥作用时,摆杆的平均偏移角度为0.071 8 rad,相比前者降低了48.68 %.

可见,不理想的测量状态会降低ICPS的性能,而minimax控制器对抵御环境干扰和噪声具有一定作用.

3.2.2 弹性防御策略的性能

1) 注入攻击对系统稳定性的影响.

图6为系统在受到攻击情况下摆杆偏移情况. 当系统未受到数据注入攻击,只受到干扰和噪声影响时,摆杆在最大偏移角度回调之后一直保持接近竖直的状态;当系统受到数据注入攻击影响后,摆杆开始剧烈震荡,$\bar{\varphi}$越接近于0震荡越剧烈,系统变得越不稳定. 当$\bar{\varphi} = 1$时,摆杆的平均偏移角度为0.071 8 rad,当$\bar{\varphi}$的值变为0.7和0.3时,摆杆的平均偏移角度则变为0.078 9 rad和0.106 6 rad. 可见,数据注入攻击会显

著降低ICPS的性能.

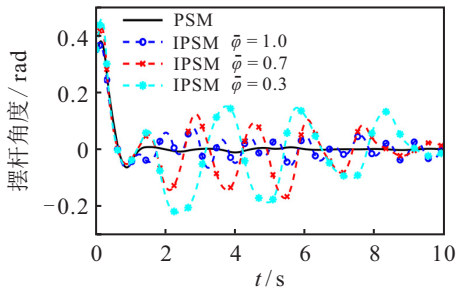

图 6　受攻击时摆杆的偏移角度

2) 弹性防御策略的有效性.

假设信道1和信道2是两个具有不同特性的通道,对于发射机和攻击者,不同的信道选择与弹性防御策略算法中算法迭代次数k的关系如图7所示. 迭代初始值$Q_0=[5.5\ \ 3.5\ \ 6.8\ \ 3.5]$. 两个信道的参数设置为: $\eta_1=0.6,\eta_2=0.4,\xi_1=0.4,\xi_2=0.2,\alpha_1=0.4,\alpha_2=0.5,\beta_1=0.9,\beta_2=0.3$. 对于式(31)中发射机的成本函数,参数$c_0=0.4,c_1=0.12,c_2=0.2,C_0=\begin{bmatrix}0.45 & 0.3\\ 0.3 & 0.45\end{bmatrix}$. 通过使用弹性防御策略算法,在4种组合中,每个参与者的最佳混合策略如表2所示,信道选择(i,j)表示发射机选择信道i,攻击者选择信道j. 结果表明,随着迭代次数的增加,4种组合的贴现成本Q均在$k=2$时达到最大值,而后逐渐降低,在$k=8$时,4种组合均达到稳定值,其中信道选择$(1,2)$的贴现成本在稳定后最低.

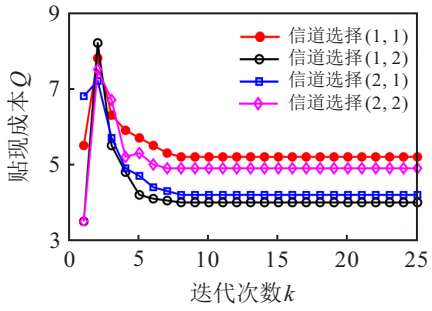

图 7　贴现成本Q_k随迭代次数k的变化

表 2　4种信道组合下每个参与者的最佳混合策略

传输信道选择	π_T^*	π_W^*
(1, 1)	[0.353　0.657]	[0.595　0.405]
(1, 2)	[0　1]	[1　0]
(2, 1)	[0.478　0.522]	[0.147　0.853]
(2, 2)	[0.156　0.844]	[0.673　0.327]

图8为系统中有无弹性防御策略对摆杆的偏移角度的影响. 在PSM下,摆杆在最大偏移角度回调后保持接近竖直的状态. 在IPSM下,$\bar{\varphi}$值为0.3时: 弹性防御策略未发挥作用时摆杆的平均偏移角度为0.106 6 rad,弹性防御策略发挥作用时摆杆的平均偏移角度变为0.037 5 rad,降低了64.8 %. 仿真结果表明,弹性防御策略可降低数据注入攻击对系统的影响.

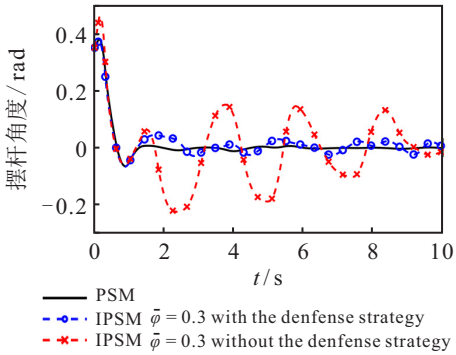

图 8　弹性防御策略对摆杆的偏移角度的影响

为发射机和攻击者随机选择每个信道的信道增益,即$\eta_i\in[0.2,0.5],\zeta_j\in[0.1,0.3]$,参数$a_i$和$b_j$均在区间$[0.1,1]$随机选取,其他参数设置不变. 分别对1～6个信道应用算法迭代100次,得出干扰衰减参数$\hat{\gamma}$随信道数量变化的关系如表3所示. 可见,传输信道越多,$\hat{\gamma}$的值越小,即更多的传输信道会提升系统的性能. 在使用6个信道时,系统相比只使用1个信道提升了38.82 %,表明了多信道防御策略的有效性.

表 3　最小干扰衰减参数$\hat{\gamma}$与传输信道数量N的关系

N	1	2	3	4	5	6
$\hat{\gamma}$	4.92	4.23	3.81	3.67	3.33	3.01

4　结　论

本文研究了在虚假数据注入攻击下,基于多信道传输框架的ICPS的联合防御策略. 为增强系统抵御噪音和干扰以及注入攻击的弹性,设计了minimax控制器和多信道博弈策略. 仿真结果表明,本文的联合弹性防御策略能够在一定程度上同时降低干扰和数据注入攻击对系统的影响. 未来的研究将在以下方面进行拓展: 1) 在研究一个发射机与一个攻击者之间进行博弈的基础上,进一步开展涉及多个发射机或者多个攻击者的研究; 2) 在考虑对虚假注入攻击进行被动性弹性防御控制的基础上,进一步设计有效的攻击补偿方法.

参考文献(References)

[1] Giraldo J, Sarkar E, Cardenas A A, et al. Security and privacy in cyber-physical systems: A survey of surveys[J]. IEEE Design & Test, 2017, 34(4): 7-17.

[2] Hu F, Lu Y, Vasilakos A V, et al. Robust cyber-physical systems: Concept, models, and implementation[J]. Future Generation Computer Systems, 2016, 56: 449-475.

[3] 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[J]. Neurocomputing, 2019, 338: 101-115.

[4] Khan R, Maynard P, McLaughlin K, et al. Threat analysis of BlackEnergy malware for synchrophasor based real-time control and monitoring in smart grid[J]. BCS Learning & Development, 2016, 23(7): 53-63.

[5] Li Y Z, Quevedo D E, Dey S, et al. SINR-based DoS attack on remote state estimation: A game-theoretic approach[J]. IEEE Transactions on Control of Network Systems, 2017, 4(3): 632-642.

[6] Langner R. Stuxnet: Dissecting a cyberwarfare weapon[J]. IEEE Security & Privacy, 2011, 9(3): 49-51.

[7] 孙子文, 张炎棋. 工业信息物理系统的攻击建模研究[J]. 控制与决策, 2019, 34(11): 2323-2329.
(Sun Z W, Zhang Y Q. Research on attack modeling of industrial cyber physical systems[J]. Control and Decision, 2019, 34(11): 2323-2329.)

[8] Wu G Y, Sun J, Chen J. Optimal data injection attacks in cyber-physical systems[J]. IEEE Transactions on Cybernetics, 2018, 48(12): 3302-3312.

[9] Zhang R C, Venkitasubramaniam P. Stealthy control signal attacks in linear quadratic Gaussian control systems: Detectability reward tradeoff[J]. IEEE Transactions on Information Forensics and Security, 2017, 12(7): 1555-1570.

[10] Sou K C, Sandberg H, Johansson K H. Computing critical k-tuples in power networks[J]. IEEE Transactions on Power Systems, 2012, 27(3): 1511-1520.

[11] Li Y Z, Shi L, Chen T W. Detection against linear deception attacks on multi-sensor remote state estimation[J]. IEEE Transactions on Control of Network Systems, 2018, 5(3): 846-856.

[12] Mo Y L, Chabukswar R, Sinopoli B. Detecting integrity attacks on SCADA systems[J]. IEEE Transactions on Control Systems Technology, 2014, 22(4): 1396-1407.

[13] Guan Y P, Ge X H. Distributed attack detection and secure estimation of networked cyber-physical systems against false data injection attacks and jamming attacks[J]. IEEE Transactions on Signal and Information Processing Over Networks, 2018, 4(1): 48-59.

[14] Deng R L, Xiao G X, Lu R X. Defending against false data injection attacks on power system state estimation[J]. IEEE Transactions on Industrial Informatics, 2017, 13(1): 198-207.

[15] Rawat D B, Bajracharya C. Detection of false data injection attacks in smart grid communication systems[J]. IEEE Signal Processing Letters, 2015, 22(10): 1652-1656.

[16] 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[J]. IEEE Transactions on Control of Network Systems, 2014, 1(4): 370-379.

[17] Zhu M H, Martínez S. On the performance analysis of resilient networked control systems under replay attacks[J]. IEEE Transactions on Automatic Control, 2014, 59(3): 804-808.

[18] Kwon C, Hwang I. Cyber attack mitigation for cyber-physical systems: Hybrid system approach to controller design[J]. IET Control Theory & Applications, 2016, 10(7): 731-741.

[19] Guo Z Y, Shi D W, Johansson K H, et al. Optimal linear cyber-attack on remote state estimation[J]. IEEE Transactions on Control of Network Systems, 2017, 4(1): 4-13.

[20] Sun Y C, Yang G H. Periodic event-triggered resilient control for cyber-physical systems under denial-of-service attacks[J]. Journal of the Franklin Institute, 2018, 355(13): 5613-5631.

[21] Li Y Z, Shi L, Cheng P, et al. Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach[J]. IEEE Transactions on Automatic Control, 2015, 60(10): 2831-2836.

[22] Wei L F, Sarwat A I, Saad W, et al. Stochastic games for power grid protection against coordinated cyber-physical attacks[J]. IEEE Transactions on Smart Grid, 2018, 9(2): 684-694.

[23] Moon J, Baar T. Minimax control over unreliable communication channels[J]. Automatica, 2015, 59: 182-193.

[24] Ding K M, Li Y Z, Quevedo D E, et al. A multi-channel transmission schedule for remote state estimation under DoS attacks[J]. Automatica, 2017, 78: 194-201.

[25] Yang H J, Xia Y Q, Shi P, et al. Analysis and synthesis of delta operator systems[M]. Berlin, Heidelberg: Springer, 2012: 1-274.

[26] Hovareshti P, Gupta V, Baras J S. Sensor scheduling using smart sensors[C]. The 46th IEEE Conference on Decision and Control. New Orleans, 2007: 494-499.

[27] Wu J F, Yuan Y, Zhang H S, et al. How can online schedules improve communication and estimation tradeoff?[J]. IEEE Transactions on Signal Processing, 2013, 61(7): 1625-1631.

[28] Brian D O Anderson, John B Moore. Optimal filtering[M]. Englewood: Prentice-Hall, 1979: 1-358.

[29] Basar T, Bernhard P. H_∞ optimal control and related minimax design problems: A dynamic game approach[M]. Boston: Birkhäuser, 1991: 1-409.

[30] Sun Z W, Liu Y H. Packet loss control of wireless control system based on security path and packet loss compensation[J]. Control and Decision, 2019, 34(4): 799-804.

作者简介

孙子文(1968−), 女, 教授, 博士生导师, 从事控制理论与控制工程、模式识别、无线传感网络理论与技术等研究, E-mail: sunziwen@jiangnan.edu.com;

洪涛(1997−), 男, 硕士生, 从事控制理论与控制工程的研究, E-mail: 6191905020@stu.jiangnan.edu.com.

(责任编辑：郑晓蕾)