控制与决策
Control and Decision

网络攻击下的信息物理系统安全性研究综述

叶丹, 靳凯净, 张天予

引用本文:
叶丹,靳凯净,张天予. 网络攻击下的信息物理系统安全性研究综述[J]. 控制与决策, 2023, 38(8): 2243-2252.

在线阅读 View online: https://doi.org/10.13195/j.kzyjc.2023.0386

网络攻击下的信息物理系统安全性研究综述

叶 丹[1,2†], 靳凯净[1], 张天予[1]

(1. 东北大学 信息科学与工程学院，沈阳 110819；
2. 东北大学 流程工业综合自动化国家重点实验室，沈阳 110819)

摘 要: 随着信息物理系统在现代工业和制造业中的广泛应用,其安全性逐渐成为关系社会健康发展的重要因素. 由于信息物理系统内部物理设备和通信网络的深度融合,网络攻击对系统安全的威胁日益凸显. 首先,从攻击者角度总结各类网络攻击的特点,揭示系统在不同攻击下的脆弱性;其次,针对不同网络攻击的特性,从防御者角度对信息物理系统的安全状态估计、攻击检测和安全控制进行介绍,并阐述各防御策略的主要应用场景和优势;最后,对信息物理系统安全性研究面临的主要挑战进行展望.

关键词: 信息物理系统；网络攻击；安全状态估计；攻击检测；安全控制

中图分类号: TP273 **文献标志码:** A

DOI: 10.13195/j.kzyjc.2023.0386

引用格式: 叶丹,靳凯净,张天予. 网络攻击下的信息物理系统安全性研究综述[J]. 控制与决策, 2023, 38(8): 2243-2252.

A survey on security of cyber-physical systems under network attacks

YE Dan[1,2†], *JIN Kai-jing*[1], *ZHANG Tian-yu*[1]

(1. College of Information Science and Engineering，Northeastern University，Shenyang 110819，China；2. State Key Laboratory of Synthetical Automation of Process Industries，Northeastern University，Shenyang 110819，China)

Abstract: With the wide application in modern industry and manufacturing, the security of cyber-physical systems has gradually become an important factor to ensure the healthy development of society, and has received extensive attention from scholars. Due to the deep integration of physical devices and communication networks within cyber-physical systems, the threat of network attacks on system security is becoming increasingly prominent. In this paper, we first summarize the characteristics of various network attacks from the attacker's perspective, and reveal the vulnerability of systems under different attacks. Secondly, in view of the characteristics of different network attacks, the secure state estimation, attack detection and secure control of cyber-physical systems are introduced from the defender's perspective, and the main application scenarios and advantages of each defense strategy are presented. Finally, the major challenges for the study of cyber-physical system security are proposed.

Keywords: cyber-physical systems；network attacks；secure state estimation；attack detection；secure control

0 引 言

控制技术、通信技术和计算机技术的快速发展,极大地推动了工业自动化进程,使得许多现代控制系统的物理演化过程和信息处理过程深度耦合. 为了描述这类将信息世界与物理世界紧密集成的复杂系统,信息物理系统(cyber-physical system, CPS)这一概念应运而生.

CPS一经提出便受到了学术界和工业界的广泛关注. 各国科研学者分别从CPS的系统模型和实现、运行环境构架以及理论方法等方面出发,展开了广泛的讨论和研究[1-3]. CPS具有通信、计算以及远程协同控制等功能,其在医疗服务、智能运输、智能电网、航天航空以及现代农业等领域都具有重要的应用价值[4-6]. CPS在实际工程中的广泛应用,可以帮助大型工业系统实现更加灵活高效的运营要求,提高市场竞争力. 因此,CPS的理论研究和实际应用具有深远意义,并极大地推动了全球信息化和智能化的发展.

CPS利用先进的传感、计算、通信和控制技术,实现了物理空间和信息空间的紧密联系,其结构如图1所示. 其中:物理空间一般包含了实际物理系统的组

收稿日期: 2023-03-31；**录用日期:** 2023-05-18.
基金项目: 国家自然科学基金项目(62173071)；中央高校基本科研业务费专项资金项目(N2204008, N2304001).
责任编委: 杨光红.
†通讯作者. E-mail: yedan@ise.neu.edu.cn.

成元件,如传感器、执行器等设备,对物理系统进行状态感知以及根据从信息空间收到的决策指令进行精准控制;信息空间一般包含了数据处理元件,根据从物理空间收集到的信息进行计算分析,进而给出相应的决策. CPS强调物理空间和信息空间的深度集成,这使得原本封闭的物理设备更加开放,在带来技术优势的同时也导致CPS的安全风险不断增加. 近年来,世界各地频繁发生的重大安全事件将CPS的安全性提升到了前所未有的高度[7-8]. 例如,2003年,蓝宝石(SQL slammer)蠕虫病毒袭击美国Davis-Besse核电站,该攻击通过降低网络流量致使核电站安全监测系统长时间无法正常工作. 2008年,波兰某城市的地铁系统受到网络攻击入侵,攻击者越过交通控制系统,通过电视遥控器可直接挟持轨道扳道器,致使4节车厢脱轨. 2010年,“震网”病毒(StuxNet)利用操作系统漏洞入侵伊朗布什尔核电站,导致大量离心机因失控不断加速而最终报废. 2011年,美国伊利诺伊州城市供水系统受到网络攻击入侵,大量供水泵被烧毁. 2012年,极具破坏力的“火焰”病毒(Flame)在中东地区大量传播,严重影响了石油开采等重要工业控制系统的正常运行. CPS不断涌现的安全问题不仅极大地影响了社会的繁荣稳定,甚至有可能威胁到人类的生命安全,因此,保证CPS的安全性刻不容缓.

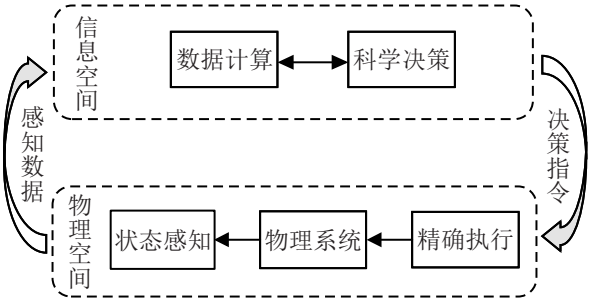

图1 信息物理系统结构框图

网络攻击通常由人为设计,因此研究CPS的安全性既要考虑攻击的潜在行为,也要以此为依据建立防御策略. 现有研究工作从攻击者和防御者两个角度出发对CPS安全进行了深入研究. 前者主要通过设计攻击策略对CPS造成破坏,这有助于分析CPS的脆弱性. 相反地,后者的重点是建立CPS的防御策略,降低网络攻击的负面影响,保障CPS的安全稳定运行.

本文将从如下几个方面对现有研究工作进行回顾:从攻击者角度介绍几类典型的网络攻击及其对CPS安全性的影响;从防御者角度介绍典型攻击下CPS的安全状态估计、攻击检测以及安全控制技术.

1 信息物理系统中的攻击行为

由于CPS中网络环境与物理进程的高度融合,通过入侵开放的无线通信网络进而降低整个系统性能的网络攻击成为CPS安全性的主要威胁. 根据网络攻击的实现形式和攻击意图,主要分为:拒绝服务(denial-of-service, DoS)攻击、窃听攻击、重放攻击和虚假数据注入(false data injection, FDI)攻击. CPS中的传感器和执行器通过信息网络与控制中心进行数据交互,因此传感器到控制中心和控制中心到执行器两个信道容易遭受网络攻击(如图2所示).

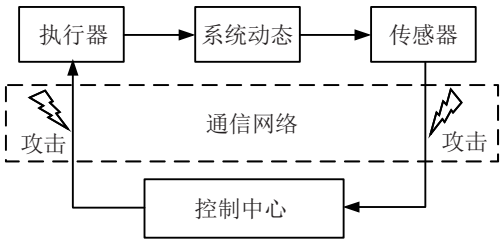

图2 网络攻击下的系统结构

1.1 DoS攻击研究现状

DoS攻击是CPS中一种较为常见的攻击形式,攻击者不需要精确的系统模型知识和实时数据,便可以通过发送大量无用请求阻塞通信频道,导致合法数据无法被及时接收[9].

从攻击者角度出发,现有的工作大多考虑攻击资源受限情况下的最优DoS攻击调度以及最优攻击下系统的性能变化. 以最大化平均状态协方差为攻击目标,文献[10]给出了最优DoS攻击的调度策略,即在有限的攻击次数下尽可能地连续发动DoS攻击. 文献[11]考虑传感器数据传输存在丢包的情况,以最大化终端状态协方差为攻击目标,给出了能量受限下的最优DoS攻击调度方案. 文献[12]提出了一个基于信号-干扰-噪声比的无线通信模型,在该模型中,不同的DoS攻击功率会导致不同的丢包率. 文献[12]将能量约束下的最优DoS攻击策略描述为马尔可夫决策过程,得到了具有阈值结构的最优攻击调度方案. 由于网络攻击和系统防御处于一个此消彼长、动态发展的过程中,一些学者通过攻防博弈刻画攻击者和防御者间的决策过程[13]. 文献[14]研究了传感器数据传输和DoS攻击间的零和博弈,证明了双方的最优策略符合纳什均衡. 文献[15]建立了一个马尔可夫博弈框架来刻画双方的决策过程,并采用纳什Q学习算法求解攻防双方的最优策略. 文献[16]考虑攻击者无法获取远程估计器到传感器的确认信息的情况,利用随机贝叶斯博弈模型给出了攻防双方的混合均衡策略.

1.2 窃听攻击研究现状

CPS通过信息网络对大量物理设备进行跨地域的协同调控,各元件间通常需要进行广域无线通信. 由于无线通信的广播性质,其信息传输过程容易受到非法窃听. 窃听攻击可以在通信双方都不知情的情况下介入他们的交互过程,伪装成二者正确的通讯对象窃听通信信息[17]. 当攻击者对系统中的控制指令和测量输出等数据进行窃听时,可以通过适当分析推断出物理系统参数及运行状态等隐私信息,进而对CPS实施更具破坏性的攻击方式. 窃听攻击通常需要借助特殊的设备或软件来监听系统通信,捕获其中的传输数据. 例如,在医疗系统中,病人的敏感数据(如性别或健康状况)可能会被第三方利用,以达到有针对性的广告或其他目的. 在智能电网中,窃听攻击可以从智能电表提供的耗电数据中获得居民的私人信息,甚至进一步推断出日程安排,严重危害国民安全[18]. 文献[19]建立了窃听攻击和主动破坏传输数据的交替攻击模型,研究了窃听性能和攻击隐蔽性之间的制衡关系,并通过求解马尔可夫决策过程得到了最优的攻击策略. 文献[20]考虑攻击者以一定概率成功窃听各传感器数据的情况,通过求解组合优化问题得到了具有阈值结构的最优传感器调度策略,使窃听攻击获取的状态估计误差最大化.

1.3 重放攻击研究现状

重放攻击不需要具体的系统模型信息,通过信道入侵、窃听等相关手段在一段时间内记录发送者和接收者之间的通信数据,然后在某个时刻之后将记录的数据重新发送给接收者[21]. 文献[22]研究了线性二次高斯控制系统在重放攻击下的安全性问题,并给出了重放攻击的不可检测条件. 由于重放信号和真实观测值的统计相似性使得重放攻击难以被发现. 为了解决这一问题,文献[23]通过在控制输入中添加水印实现重放攻击检测. 在只增加固定控制成本的情况下,得到了最优水印方案,使攻击前后新息的相对熵最大. 文献[24]针对不连续的重放攻击,设计了一类周期性的水印调度,在减少控制成本的同时获得良好的攻击检测性能. 文献[25]假设重放攻击可以记录并覆盖传感器的传输数据,提出了一种随机编码方案,保证了在不牺牲正常系统任何性能的情况下有效检测重放攻击. 文献[26]关注重放攻击下具有状态和输入约束的CPS弹性控制问题,通过一种滚动时域控制方法来处理重放攻击导致的系统性能下降. 文献[27]利用博弈方法研究了控制系统性能与重放攻击检测率之间的权衡,通过最小化控制和检测成本,得到重放攻击下的最优控制策略.

1.4 FDI攻击研究现状

当攻击者充分掌握系统模型参数和运行数据等知识时,可以精心篡改CPS的传感器和执行器信道的传输数据,从而形成更具破坏力的FDI攻击. 不同于DoS攻击,FDI攻击可以在对检测器保持隐蔽的同时使CPS的运行状态产生尽可能大的偏差. 因此,精心设计的FDI攻击往往会对CPS的可靠稳定运行造成严重威胁. 由于FDI攻击通常需要借助于系统的模型参数,实时数据等信息,其设计方法也更加多样,例如数据驱动攻击[28-29],多信道联合攻击[30],以及切换攻击方法[31]等. 文献[28-29]在不需要任何系统动力学矩阵知识的情况下,仅依赖系统的输入输出数据,提出了一类FDI攻击设计方法,进而影响系统性能. 文献[30]将一组人工生成的高斯噪声作为FDI攻击信号,考虑了多传感器系统的最优攻击调度问题. 文献[32]针对传感器信道和执行器信道同时遭受FDI攻击的情况,给出了有限时间范围内的最优攻击调度方案. 为了避免攻击信号过大而被系统识别,针对检测器的隐蔽性通常是FDI攻击的目标之一. 文献[33]讨论了FDI攻击破坏能力与隐蔽性的制衡关系,其中攻击的隐蔽性由受攻击前后新息数据的相对熵描述. 文献[34-35]介绍了一种基于新息数据的FDI攻击并给出了最优攻击的具体结构. 相比基于高斯噪声的FDI攻击,这类FDI攻击能够导致更加严重的系统性能下降[36]. 文献[37]通过历史新息数据进一步改进FDI攻击,使CPS产生更大的系统性能下降.

上述FDI攻击仅能使系统状态产生有界偏差以便恶化系统性能,但难以威胁CPS的稳定性. 针对可以使系统状态发散并维持隐蔽性的FDI攻击,文献[38]利用输出矩阵的零空间和状态可达性给出了这类攻击存在的充要条件. 文献[39]介绍了一种具有完全隐蔽性的FDI攻击,在使CPS状态发散的同时,可以渐近地消除对系统残差的影响. 不同于单独入侵传感器或执行器信道的FDI攻击,对多种信道进行联合入侵的FDI攻击更容易在维持隐蔽性的前提下使CPS失稳. 文献[40-41]提出了一种同时入侵传感器和执行器信道的FDI攻击,相比于文献[38-39]中的FDI攻击,该攻击的存在性条件更加宽松. 文献[42]研究了同时篡改估计器和传感器数据的FDI攻击,并讨论了该攻击存在的充要条件.

CPS利用通信网络为不同子系统提供信息交互平台,通过分布式估计和控制技术实现子系统间的协同运行. 然而,子系统间的通信信道也为网络攻击提供了更多的入侵空间. 文献[43]基于能观矩阵的零空间,对一类入侵子系统间通信信道的FDI攻击进行

研究. 文献[44]分析了FDI攻击通过篡改子系统间通信信道使分布式估计过程失稳的情况,并在此基础上制定了相应的防御策略. 文献[45]为了进一步揭示分布式估计不同于集中式估计的互联脆弱性,提出了一种分散FDI攻击,在保持完全隐蔽性的同时使所有观测器节点的估计误差发散.

2 网络攻击下信息物理系统的防御策略

从防御者的角度出发,控制领域的专家和学者研究了如何在网络攻击下对系统异常状态进行有效监测并通过控制技术维持CPS的安全运行. 本文将从安全状态估计、攻击检测和安全控制3个角度出发介绍基于控制理论的CPS防御技术.

2.1 网络攻击下信息物理系统的安全状态估计

安全状态估计使CPS在网络攻击下依然能够通过传感器测量信息对系统运行状态进行准确估计,为CPS防御策略的建立提供可靠的信息保障[46]. 现有的安全估计方法主要分为最小二乘估计和基于观测器的状态估计两类.

2.1.1 基于最小二乘法的安全状态估计

设状态变量为x,对其进行k次测量,则测量值可以表示为

$$y_i = H_i x + \nu_i,\ i = 1, 2, \dots, k.$$

其中:y_i和ν_i分别表示第i次测量时的测量值和测量噪声,H_i为测量矩阵. 记

$$Y = \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_k \end{bmatrix},\ H = \begin{bmatrix} H_1 \\ H_2 \\ \vdots \\ H_k \end{bmatrix},\ \nu = \begin{bmatrix} \nu_1 \\ \nu_2 \\ \vdots \\ \nu_k \end{bmatrix},$$

设x的估计值为$\hat{x}$,则测量值Y与估计值$H\hat{x}$的估计误差为

$$e = Y - H\hat{x}.$$

最小二乘估计的目标是找到$\hat{x}$使误差的平方和

$$J(\hat{x}) = (Y - H\hat{x})^{\mathrm{T}}(Y - H\hat{x})$$

最小,则对$\hat{x}$求偏导并令之为零,可得

$$\frac{\partial J(\hat{x})}{\partial \hat{x}} = -2H^{\mathrm{T}}(Y - H\hat{x}) = 0.$$

当$(H^{\mathrm{T}}H)^{-1}$存在时,可得$\hat{x}$的最小二乘估计为

$$\hat{x} = (H^{\mathrm{T}}H)^{-1}H^{\mathrm{T}}Y.$$

最小二乘估计作为一种简单、灵活的参数估计方法,被广泛应用于控制系统的状态估计. 文献[47]将稀疏FDI攻击信号作为增广系统状态,通过事件触发的投影梯度下降算法实现了系统状态的最小二乘安全估计. 文献[48]提出了一类基于L_0范数优化的最小二乘安全估计算法以减少稀疏FDI攻击的影响,并证明了最大估计误差的有界性. 文献[49]通过引入正交补矩阵的概念,提供了稀疏FDI攻击下状态可观的充要条件,并利用最小平方技术和投影算子从一组连续的测量值中重构系统状态. 文献[50]表明若超过一半的传感器信道受到攻击则无法准确地重构系统状态. 当攻击数量小于某个阈值时,文献[50]提出了一种基于压缩感知技术的最小二乘估计算法以实现系统状态的安全估计. 文献[51]针对任意形式的攻击信号,通过测量矩阵及系统矩阵的特征向量给出了传感器攻击的可检测性条件,并利用L_0/L_1范数优化和n步连续测量数据实现系统状态的最小二乘估计. 针对发生在分布式网络中的拜占庭攻击,文献[52]提出了一种高效的梯度下降算法,将收到的邻居信息以坐标修剪的方式进行汇总,保证了健康节点对拜占庭节点的鲁棒性. 文献[53]针对由恶意攻击造成的拜占庭链路/节点,提出了一种分布式最小二乘状态估计算法. 通过采用局部最小切换决策来对抗拜占庭链路/节点的影响,保证了所有正常节点状态的渐近收敛.

2.1.2 基于观测器的安全状态估计

根据CPS的未知外部输入类型(攻击、噪声和扰动等),基于观测器的安全状态估计包括如下两种实现方法.

1)通过卡尔曼滤波器实现安全状态估计. 卡尔曼滤波适用于离散时间的线性高斯随机系统. 卡尔曼滤波考虑过程噪声和测量噪声的统计特性,在多次迭代过程中得到使均方误差最小的状态估计值. 考虑如下离散时间的线性高斯随机系统:

$$\begin{aligned} x_{k+1} &= Ax_k + B(u_k + a_k^u) + \omega_k, \\ y_k &= Cx_k + a_k^y + \nu_k. \end{aligned}$$

其中:$x_k \in \boldsymbol{R}^n, u_k \in \boldsymbol{R}^l$和$y_k \in \boldsymbol{R}^m$分别表示系统状态、控制输入和测量输出;$\omega_k \in \boldsymbol{R}^n$和$\nu_k \in \boldsymbol{R}^m$分别表示服从高斯分布的系统过程噪声和测量噪声,即$\omega_k \sim \mathcal{N}(0, Q)$和$\nu_k \sim \mathcal{N}(0, R)$;$a_k^u \in \boldsymbol{R}^l$和$a_k^y \in \boldsymbol{R}^m$分别表示执行器和传感器攻击信号. 标准卡尔曼滤波设计如下:

$$\begin{aligned} \hat{x}_{k+1}^- &= A\hat{x}_k + Bu_k, \\ P_{k+1}^- &= AP_kA^{\mathrm{T}} + Q, \\ K_{k+1} &= P_{k+1}^- C(CP_{k+1}^- C^{\mathrm{T}} + R)^{-1}, \\ \hat{x}_{k+1} &= \hat{x}_{k+1}^- + K_{k+1}(y_{k+1} - C\hat{x}_{k+1}^-), \\ P_{k+1} &= (I - K_{k+1}C)P_{k+1}^-. \end{aligned}$$

其中: $\hat{x}_k^-$ 和 $\hat{x}_k$ 分别为 k 时刻的先验估计和后验估计, K_k 为滤波增益.

作为一种最优滤波方法, 卡尔曼滤波可以在过程噪声和测量噪声满足一定假设条件的情况下, 得到最优的状态估计结果. 因此吸引了众多学者采用卡尔曼滤波对CPS进行安全状态估计. 文献[54]利用Holt双参数指数平滑技术和改进的卡尔曼滤波技术, 提出了一种新型的状态估计算法以增强电力系统在连续DoS攻击下的状态估计精度. 文献[55]考虑了两个不同电力子系统在DoS攻击下的融合状态估计问题, 并通过一种基于新息的切换律分析了两个子系统在估计精度、收敛速度和计算时间方面的制衡关系. 文献[56]假设DoS攻击通过发出噪声功率来干扰无线信道, 利用零和博弈和马尔可夫博弈研究了不同网络环境下的最优攻防策略, 以保证DoS攻击下的卡尔曼滤波估计性能. 文献[57]建立了一类发生在传感器信道的DoS和FDI混合攻击模型, 通过自适应分布式卡尔曼滤波估计减轻了攻击对大规模电力系统性能的影响.

2) 利用龙伯格观测器实现CPS的安全状态估计. 针对平方可积和幅值有界的外部扰动/未知输入, 龙伯格观测器可以有效估计系统状态, 并通过预设系统估计性能抑制攻击和扰动等未知外部输入. 考虑如下线性时不变CPS模型:

$$\delta(x(t)) = Ax(t) + B_u(u(t) + f_a^u(t)) + B_d d(t),$$
$$y(t) = Cx(t) + Df_a^y(t).$$

其中: $\delta(x(t))$ 对于连续时间和离散时间系统分别表示 $\dot{x}(t)$ 和 $x(t+1)$; $x(t) \in \boldsymbol{R}^n$, $u(t) \in \boldsymbol{R}^l$ 和 $y(t) \in \boldsymbol{R}^m$ 分别表示系统状态、控制输入和传感器输出; $d(t) \in \boldsymbol{R}^{l_d}$ 表示外部扰动, 满足 $d(t) \in L_2(0, \infty)$; $f_a^u(t) \in \boldsymbol{R}^l$ 和 $f_a^y(t) \in \boldsymbol{R}^h$ 分别表示发生执行器和传感器信道中的攻击信号. 针对上述CPS, 龙伯格状态观测器设计如下:

$$\delta(\hat{x}(t)) = A\hat{x}(t) + B_u u(t) + L(y(t) - \hat{y}(t)),$$
$$\hat{y}(t) = C\hat{x}(t).$$

其中: $\hat{x}(t)$ 和 $\hat{y}(t)$ 分别表示 $x(t)$ 和 $y(t)$ 的估计, L 为观测器增益且满足 $\rho(A - LC) < 1$.

龙伯格观测器针对非高斯系统具有更好的适用性, 因此被国内外学者广泛应用于CPS的安全状态估计. 针对一类非线性系统, 文献[58]在能量受限DoS攻击的最坏情况下构建了一个基于神经网络的龙伯格状态观测器, 分析了估计误差动态和神经网络权重的关系. 文献[59]假设遭受稀疏FDI攻击的传感器信道数量上限已知, 提出了一种多模龙伯格观测器, 并基于可满足性模理论选出未被攻击的传感器信道. 文献[60]针对稀疏FDI攻击下的CPS提出了一种自适应切换龙伯格状态观测器, 筛选安全传感器数据估计系统状态.

相比于集中式估计, 分布式估计可以进一步提高对CPS运行状态的感知能力, 并因此受到控制领域学者的广泛关注. 文献[61]针对稀疏FDI攻击, 提出了分布式的测量数据预选器以确保CPS能够利用健康传感器数据实现安全状态估计. 文献[62]建立了FDI攻击下的分布式电力系统模型, 并通过设计龙伯格观测器和 H_∞ 检测器以估计系统状态并检测攻击. 文献[63]利用排序修剪后的邻居信息设计局部龙伯格观测器, 克服了拜占庭攻击对系统分布式估计性能的影响, 并通过引入网络拓扑“强鲁棒性”概念, 给出了估计算法的有效性条件.

2.2 信息物理系统的攻击检测

攻击检测通过安全状态估计提供的可靠数据, 实时判断CPS是否遭受网络攻击, 是主动防御策略有效实施的信息基础, 近年来受到科研工作者的广泛关注. 针对网络攻击的检测方法主要分为以下几类:

1) 卡方检测器.

卡方检测器是一个基于残差的检测器, 并被广泛地用于检测高斯随机系统中出现的异常情况. 卡方检测器的检测原理是利用残差的统计特性设计检测器阈值, 并区分CPS的正常与异常工况, 从而达到检测网络攻击的目的. 卡方检测器的检测机制如下:

$$H_0 : g_k = \sum_{i=k-J+1}^{k} z_i^{\mathrm{T}} \Sigma^{-1} z_i \leqslant J_{\mathrm{th}},$$
$$H_1 : g_k = \sum_{i=k-J+1}^{k} z_i^{\mathrm{T}} \Sigma^{-1} z_i > J_{\mathrm{th}}.$$

其中: $z_i = y_i - C\hat{x}_i$, 表示 i 时刻的系统残差; Σ 表示残差向量在稳态时刻的协方差矩阵; J 表示检测窗口大小; J_{th} 表示阈值; H_0 表示系统未检测到攻击, 未触发警报; H_1 表示检测器触发警报, 系统可能遭受攻击. 卡方检测器通过期望的误警率设置检测阈值, 阈值越小, CPS正常工况下的误警率越小, 但对网络攻击的检测能力越差.

2) 基于 H_∞/H_- 指标的攻击检测器.

该检测器围绕平方可积和幅值有界的攻击信号, 通过 H_∞/H_- 指标使残差对攻击信号敏感, 对扰动和模型不确定性具有一定的鲁棒性. 令龙伯格观测器增益 L 满足 H_∞ 和 H_- 性能, 即

$$\int_0^\infty r^{\mathrm{T}}(t) r(t) \mathrm{d}t \leqslant \gamma^2 \int_0^\infty d^{\mathrm{T}}(t) d(t) \mathrm{d}t,$$
$$\int_0^\infty r^{\mathrm{T}}(t) r(t) \mathrm{d}t > \beta^2 \int_0^\infty f_a^{\mathrm{T}}(t) f_a(t) \mathrm{d}t.$$

其中: $r(t)=y(t)-C\hat{x}(t)$, 表示系统残差; γ 和 β 为预设的性能指标常数; $f_a(t)$ 为执行器攻击和传感器攻击的整合形式, 即

$$f_a(t)=[(f_a^u(t))^{\mathrm{T}}\ \ (f_a^y(t))^{\mathrm{T}}]^{\mathrm{T}}.$$

检测机制设计如下:

$$H_0: g(t)=r^{\mathrm{T}}(t)r(t)\leqslant J_{\mathrm{th}},$$
$$H_1: g(t)=r^{\mathrm{T}}(t)r(t)>J_{\mathrm{th}}.$$

其中检测器阈值 J_{th} 选为在最坏扰动且系统正常情况下的 $g_{\max}=r_{\max}^{\mathrm{T}}r_{\max}$.

现有研究在上述两类检测方法的基础上, 进一步通过数据融合和编解码等方法提高CPS对网络攻击的检测能力. 例如, 文献[64]提出了一种具有随机检测阈值的改进卡方检测器以积极防御FDI攻击, 并将此类随机FDI攻击检测方法扩展至具有多传感器的CPS. 文献[65]研究了一种利用当前信息和所有历史信息的累加卡方检测器以验证传输数据的真实性, 通过选择适当的阈值可以将误报率限制在给定值之下. 文献[29,44,66]在卡方检测器的基础上, 利用水印技术和编解码技术提出了一些有效的FDI攻击检测方案. 此类通过编解码技术的攻击检测方法不仅可以应用于高斯系统, 对于非高斯系统同样有效. 由于编解码改变了测量矩阵的零空间, 可以有效检测基于矩阵零空间设计的隐蔽FDI攻击[38-42]. 文献[67]通过构造一个包含演化-决策两阶段的分布式攻击检测器, 以提供局部可靠的状态估计并检测FDI攻击. 文献[68]将平方可积的FDI攻击建模为系统的未知输入信号, 通过给定的 H_∞ 性能指标抑制攻击影响, 并利用分布式融合方法提高对攻击的预警速度. 文献[69]针对CPS系统矩阵未知的情况, 提出了一种基于数据驱动的攻击检测方案, 并通过 H_∞/H_- 性能指标来提高残差信息对测量噪声的鲁棒性和对攻击的敏感性.

2.3 网络攻击下信息物理系统的安全控制

CPS安全控制的目标是当网络攻击发生时维持系统的可靠稳定运行, 并主动抑制攻击者对系统运行状态的影响. CPS安全控制包括如下几类典型方法:

1) 切换控制方法.

当CPS受到网络攻击时, 切换控制可以根据不同的攻击方式和攻击目标自动调整控制策略, 从而应对攻击者引起的CPS信道变化并保证系统的安全运行. 例如, 当DoS攻击通过阻断CPS的通信信道使得闭环反馈结构受到影响时, 切换控制技术可以根据受攻击信道实时调整控制参数, 从而优化DoS攻击下的系统性能. 近年来, 控制领域学者围绕间歇DoS攻击建立安全切换控制策略, 给出容许的DoS攻击持续时间和攻击频率以保证CPS的稳定性[70]. 文献[71]研究了间歇性DoS攻击下闭环系统的输入状态稳定性, 并通过切换系统理论给出了系统性能和通信资源之间的制衡关系. 文献[72]将这类安全控制器拓展至多传感器系统中, 将CPS在DoS攻击下的稳定性分析转化为切换控制下的稳定性分析, 讨论了系统对DoS攻击的容忍能力. 文献[73]建立了可同时阻断多智能体系统间通信的单模式DoS攻击模型, 并通过切换控制调整控制器参数实现各智能体状态的一致性. 文献[74]考虑针对多智能体系统通信信道的多模式DoS攻击, 提出了一种安全模式策略使系统在攻击发生时切换到安全模式, 从而降低攻击者对多智能体一致性的负面影响. 针对稀疏FDI攻击, 文献[75-76]将原系统分解为具有多个控制模式的切换系统, 并利用切换控制原理实现系统的安全控制. 其中: 文献[75]利用移动目标策略和强化学习分别给出了主动和被动的攻击防御措施; 文献[76]利用线性二次性能指标设计了一个自适应切换律, 以选择适当的系统运行模式.

2) 预测控制方法.

预测控制通过分析系统模型以及历史信息推断未来的系统状态, 可以有效应对网络攻击对CPS传输数据的篡改和拦截. 文献[77-79]针对CPS中发生的DoS攻击, 提出了相应的模型预测控制方案以减少攻击对系统性能的不利影响. 文献[77]利用最近的状态数据设计预测控制器以补偿DoS攻击对CPS性能的影响. 文献[78]表明模型预测控制的性能与DoS攻击的持续时间以及控制参数有关, 在保证闭环系统的指数稳定性下得到了DoS攻击的最大允许持续时间. 文献[79]在系统状态不可测的情况下, 通过优化给定时间段内的一系列反馈控制律来合成多步模型预测控制器, 以保证网络攻击下的控制性能. 文献[80]针对范数有界的FDI攻击, 提出了一种基于输出反馈的鲁棒模型预测控制策略, 保证了系统的安全性.

3) 自适应控制方法.

自适应控制能够使被控系统随着环境变化和未知扰动等因素自动调整运行状态, 优化控制性能. 因此, 这类技术在应对CPS中网络攻击问题上具有独特的优势, 并受到国内外学者的关注. 针对一类发生在传感器信道的非周期性DoS攻击, 文献[81]设计了一种基于学习的无模型自适应控制方案, 该方法可以在DoS攻击再次发生时自适应地调整控制输入的衰减系数以提高系统的性能. 文献[82-83]研究了多智能

体系统内部通讯链路遭受DoS攻击时的一致性控制问题. 其中: 文献[82]设计了一种自适应输出反馈控制策略使各智能体的状态趋于一致; 文献[83]提出了一种无模型自适应控制算法, 使各智能体能够在DoS攻击下只利用本地信息跟踪参考信号. 文献[84]通过设计自适应律和补偿机制处理由FDI攻击引起的不确定性问题, 并将其应用于非自主性移动机器人的分布式编队控制. 文献[85]针对执行器信道遭受FDI攻击的情况, 设计了一种自适应安全控制方案以缓解FDI攻击的影响. 文献[86-87]提出了一种自适应控制器补偿同时入侵执行器和传感器的网络攻击, 分别实现了多智能体系统的状态一致和跟踪任务. 文献[88]介绍了一种基于自适应机制的分布式估计和控制联合设计方法, 维持FDI攻击下多智能体系统的跟踪一致性.

3 总结与展望

本文从攻击者和防御者角度出发总结了近年来与CPS安全性相关的研究工作. 从攻击者角度梳理了CPS中典型的网络攻击及其对系统安全性造成的潜在威胁, 从防御者角度介绍了现有工作中应对典型网络攻击的CPS安全状态估计、攻击检测和安全控制技术. CPS的建设和发展为传统产业转型提供了新的机遇, 但也使许多重要基础设施受到网络攻击的安全威胁, 特别是在CPS规模日益庞大的背景下, 网络攻击的影响更加复杂, 使得安全控制技术面临着如下挑战:

1) 现有研究所建立的CPS安全控制技术主要以被动容忍网络攻击的影响为目标. 如何进一步通过攻击检测技术对攻击位置和类型进行区分, 并在此基础上进一步构建主动安全控制方案对于CPS安全性具有重要科学价值.

2) 子系统间的通信结构对于CPS的安全运行具有重要影响. 然而, 网络攻击却可以通过子系统的互联耦合造成更恶劣的影响. 因此, 分析通信结构与网络攻击智能化行为间的关系, 对于进一步研究CPS的脆弱性具有重要意义.

3) CPS不仅时刻受到网络攻击的威胁, 其物理元件更会因长时间运行而发生故障. 网络攻击和物理故障的交叉耦合作用使CPS的安全性面临更大挑战. 因此, 如何对攻击和故障的影响进行解耦补偿, 是CPS安全控制的难题.

参考文献(References)

[1] Li R F, Xie Y, Li R, et al. Survey of cyber-physical systems[J]. Journal of Computer Research and Development, 2012, 49(6): 1149-1161.

[2] Zhang S Q, Che W W, Deng C. Observer-based event-triggered control for linear MASs under a directed graph and DoS attacks[J]. Journal of Control and Decision, 2022, 9(3): 384-396.

[3] Sun Z W, Zhang Y Q. Research on attack modeling of industrial cyber physical systems[J]. Control and Decision, 2019, 34(11): 2323-2329.

[4] Xia Y Q, Yan C, Wang X J, et al. Intelligent transportation cyber-physical cloud control systems[J]. Acta Automatica Sinica, 2019, 45(1): 132-142.

[5] Ding D R, Han Q L, Wang Z D, et al. A survey on model-based distributed control and filtering for industrial cyber-physical systems[J]. IEEE Transactions on Industrial Informatics, 2019, 15(5): 2483-2499.

[6] Zhou C J, Hu B W, Shi Y, et al. A unified architectural approach for cyberattack-resilient industrial control systems[J]. Proceedings of the IEEE, 2021, 109(4): 517-541.

[7] Svetlana K. SQL slammer worm lessons learned for consideration by the electricity sector[J]. North American Electric Reliability Council, 2003, 1(2): 5.

[8] Farwell J P, Rohozinski R. Stuxnet and the future of cyber war[J]. Survival, 2011, 53(1): 23-40.

[9] Yang H J, Ye D. Observer-based fixed-time secure tracking consensus for networked high-order multiagent systems against DoS attacks[J]. IEEE Transactions on Cybernetics, 2022, 52(4): 2018-2031.

[10] Zhang H, Cheng P, Shi L, et al. Optimal denial-of-service attack scheduling with energy constraint[J]. IEEE Transactions on Automatic Control, 2015, 60(11): 3023-3028.

[11] Qin J H, Li M L, Shi L, et al. Optimal denial-of-service attack scheduling with energy constraint over packet-dropping networks[J]. IEEE Transactions on Automatic Control, 2018, 63(6): 1648-1663.

[12] Peng L H, Shi L, Cao X H, et al. Optimal attack energy allocation against remote state estimation[J]. IEEE Transactions on Automatic Control, 2018, 63(7): 2199-2205.

[13] Xu Y H, Yang H, Jiang B, et al. Multiplayer pursuit-evasion differential games with malicious pursuers[J]. IEEE Transactions on Automatic Control, 2022, 67(9): 4939-4946.

[14] 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.

[15] 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.

[16] Ding K M, Ren X Q, Quevedo D E, et al. DoS attacks on remote state estimation with asymmetric information[J]. IEEE Transactions on Control of Network Systems, 2019, 6(2): 653-666.

[17] Zou L, Wang Z D, Shen B, et al. Encrypted finite-horizon energy-to-peak state estimation for time-varying systems under eavesdropping attacks: Tackling secrecy capacity[J]. IEEE/CAA Journal of Automatica Sinica, 2023, 10(4): 985-996.

[18] Rouf I, Mustafa H, Xu M, et al. Neighborhood watch: Security and privacy analysis of automatic meter reading systems[C]. Proceedings of the 2012 ACM Conference on Computer and Communications Security. Raleigh, 2012: 462-473.

[19] Ding K M, Ren X Q, Leong A S, et al. Remote state estimation in the presence of an active eavesdropper[J]. IEEE Transactions on Automatic Control, 2021, 66(1): 229-244.

[20] Leong A S, Quevedo D E, Dolz D, et al. Transmission scheduling for remote state estimation over packet dropping links in the presence of an eavesdropper[J]. IEEE Transactions on Automatic Control, 2019, 64(9): 3732-3739.

[21] Su L, Fang S N, Liu Z J, et al. Secure control for discrete-time hidden Markov jump systems subject to replay attacks via output feedback[J]. Journal of Control and Decision, DOI: 10.1080/23307706.2022.2127948.

[22] Mo Y L, Sinopoli B. Secure control against replay attacks[C]. The 47th Annual Allerton Conference on Communication, Control, and Computing (Allerton). Monticello, 2010: 911-918.

[23] Naha A, Teixeira A, Ahlén A, et al. Sequential detection of replay attacks[J]. IEEE Transactions on Automatic Control, 2023, 68(3): 1941-1948.

[24] Fang C R, Qi Y F, Cheng P, et al. Optimal periodic watermarking schedule for replay attack detection in cyber——Physical systems[J]. Automatica, 2020, 112: 108698.

[25] Ye D, Zhang T Y, Guo G. Stochastic coding detection scheme in cyber-physical systems against replay attack[J]. Information Sciences, 2019, 481: 432-444.

[26] 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.

[27] Miao F, Pajic M, Pappas G J. Stochastic game approach for replay attack detection[C]. The 52nd IEEE Conference on Decision and Control. Firenze, 2014: 1854-1859.

[28] Wang J S, Yang G H. Data-driven methods for stealthy attacks on TCP/IP-based networked control systems equipped with attack detectors[J]. IEEE Transactions on Cybernetics, 2019, 49(8): 3020-3031.

[29] Zhao Z G, Huang Y M, Zhen Z Y, et al. Data-driven false data-injection attack design and detection in cyber-physical systems[J]. IEEE Transactions on Cybernetics, 2021, 51(12): 6179-6187.

[30] Li F F, Tang Y. False data injection attack for cyber-physical systems with resource constraint[J]. IEEE Transactions on Cybernetics, 2020, 50(2): 729-738.

[31] 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.

[32] Guo L, Yu H, Hao F. Optimal allocation of false data injection attacks for networked control systems with two communication channels[J]. IEEE Transactions on Control of Network Systems, 2021, 8(1): 2-14.

[33] Bai C Z, Gupta V, Pasqualetti F. On Kalman filtering with compromised sensors: Attack stealthiness and performance bounds[J]. IEEE Transactions on Automatic Control, 2017, 62(12): 6641-6648.

[34] Guo Z Y, Shi D W, Johansson K H, et al. Worst-case stealthy innovation-based linear attack on remote state estimation[J]. Automatica, 2018, 89: 117-124.

[35] Shang J, Yu H, Chen T W. Worst-case stealthy innovation-based linear attacks on remote state estimation under Kullback-Leibler divergence[J]. IEEE Transactions on Automatic Control, 2022, 67(11): 6082-6089.

[36] Jin K J, Ye D. Optimal innovation-based stealthy attacks in networked LQG systems with attack cost[J]. IEEE Transactions on Cybernetics, DOI: 10.1109/TCYB.2022.3229430.

[37] Ren X X, Yang G H, Zhang X G. Optimal stealthy attack with historical data on cyber-physical systems[J]. Automatica, 2023, 151: 110895.

[38] Mo Y , Sinopoli B. False data injection attacks in control systems[C]. Preprints of the 1st Workshop on Secure Control Systems. 2010: 1-7.

[39] Zhang T Y, Ye D. False data injection attacks with complete stealthiness in cyber-physical systems: A self-generated approach[J]. Automatica, 2020, 120: 109117.

[40] Pang Z H, Liu G P, Zhou D, et al. Two-channel false data injection attacks against output tracking control of networked systems[J]. IEEE Transactions on Industrial Electronics, 2016, 63(5): 3242-3251.

[41] Sui T J, Mo Y L, Marelli D, et al. The vulnerability of cyber-physical system under stealthy attacks[J]. IEEE Transactions on Automatic Control, 2021, 66(2): 637-650.

[42] Xu W Y, Wang Z D, Hu L, et al. State estimation under joint false data injection attacks: Dealing with constraints and insecurity[J]. IEEE Transactions on Automatic Control, 2022, 67(12): 6745-6753.

[43] Lu A Y, Yang G H. Malicious attacks on state estimation against distributed control systems[J]. IEEE Transactions on Automatic Control, 2020, 65(9): 3911-3918.

[44] Zhou J Y, Yang W, Ding W J, et al. Watermarking-based protection strategy against stealthy integrity attack on distributed state estimation[J]. IEEE Transactions on Automatic Control, 2023, 68(1): 628-635.

[45] Zhang T Y, Ye D, Shi Y. Decentralized false-data injection attacks against state omniscience: Existence and security analysis[J]. IEEE Transactions on Automatic Control, DOI: 10.1109/TAC.2022.3209396.

[46] Ma R J, Shi P, Wu L G. Sparse false injection attacks reconstruction via descriptor sliding mode observers[J].

IEEE Transactions on Automatic Control, 2021, 66(11): 5369-5376.

[47] Shoukry Y, Tabuada P. Event-triggered state observers for sparse sensor noise/attacks[J]. IEEE Transactions on Automatic Control, 2016, 61(8): 2079-2091.

[48] Pajic M, Weimer J, Bezzo N, et al. Robustness of attack-resilient state estimators[C]. 2014 ACM/IEEE International Conference on Cyber-Physical Systems. Berlin, 2014: 163-174.

[49] Lu A Y, Yang G H. Switched projected gradient descent algorithms for secure state estimation under sparse sensor attacks[J]. Automatica, 2019, 103: 503-514.

[50] Fawzi H, Tabuada P, Diggavi S. Secure estimation and control for cyber-physical systems under adversarial attacks[J]. IEEE Transactions on Automatic Control, 2014, 59(6): 1454-1467.

[51] Pajic M, Lee I, Pappas G J. Attack-resilient state estimation for noisy dynamical systems[J]. IEEE Transactions on Control of Network Systems, 2017, 4(1): 82-92.

[52] Su L L, Shahrampour S. Finite-time guarantees for Byzantine-resilient distributed state estimation with noisy measurements[J]. IEEE Transactions on Automatic Control, 2020, 65(9): 3758-3771.

[53] An L W, Yang G H. Byzantine-resilient distributed state estimation: A min-switching approach[J]. Automatica, 2021, 129: 109664.

[54] Li X, Jiang C, Du D J, et al. A novel state estimation method for smart grid under consecutive denial of service attacks[J]. IEEE Systems Journal, 2023, 17(1): 513-524.

[55] Chen J, Dou C X, Xiao L, et al. Fusion state estimation for power systems under DoS attacks: A switched system approach[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2019, 49(8): 1679-1687.

[56] Yuan H H, Xia Y Q, Yang H J. Resilient state estimation of cyber-physical system with multichannel transmission under DoS attack[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2021, 51(11): 6926-6937.

[57] Yang J, Zhang W A, Guo F H. Adaptive distributed Kalman-like filter for power system with cyber attacks[J]. Automatica, 2022, 137: 110091.

[58] Zhang Y H, Wang Z D, Zou L, et al. Neural-network-based secure state estimation under energy-constrained denial-of-service attacks: An encoding-decoding scheme[J]. IEEE Transactions on Network Science and Engineering, DOI: 10.1109/TNSE.2023.3237639.

[59] Shoukry Y, Chong M, Wakaiki M, et al. SMT-based observer design for cyber-physical systems under sensor attacks[C]. The 7th International Conference on Cyber-Physical Systems. Vienna, 2016: 1-10.

[60] An L W, Yang G H. Secure state estimation against sparse sensor attacks with adaptive switching mechanism[J]. IEEE Transactions on Automatic Control, 2018, 63(8): 2596-2603.

[61] Ao W, Song Y D, Wen C Y. Distributed secure state estimation and control for CPSs under sensor attacks[J]. IEEE Transactions on Cybernetics, 2020, 50(1): 259-269.

[62] Wu J, Li Y N, Li S Y. State estimation for distributed cyber-physical power systems under data attacks[J]. Control and Decision, 2016, 31(2):331-336.

[63] Mitra A, Sundaram S. Byzantine-resilient distributed observers for LTI systems[J]. Automatica, 2019, 108: 108487.

[64] 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.

[65] Ye D, Zhang T Y. Summation detector for false data-injection attack in cyber-physical systems[J]. IEEE Transactions on Cybernetics, 2020, 50(6): 2338-2345.

[66] Liu C S, Deng R L, He W L, et al. Optimal coding schemes for detecting false data injection attacks in power system state estimation[J]. IEEE Transactions on Smart Grid, 2022, 13(1): 738-749.

[67] Ge X H, Han Q L, Zhong M Y, et al. Distributed Krein space-based attack detection over sensor networks under deception attacks[J]. Automatica, 2019, 109: 108557.

[68] Shen J H, Weng P D, Chen B, et al. A fast detection method of FDI attack signal based on distributed fusion[J]. Control and Decision, 2022, 37(12): 3259-3266.

[69] Li X J, Shen X Y. A data-driven attack detection approach for DC servo motor systems based on mixed optimization strategy[J]. IEEE Transactions on Industrial Informatics, 2020, 16(9): 5806-5813.

[70] Deng C, Zhang D, Feng G. Resilient practical cooperative output regulation for MASs with unknown switching exosystem dynamics under DoS attacks[J]. Automatica, 2022, 139: 110172.

[71] De Persis C, Tesi P. Input-to-state stabilizing control under denial-of-service[J]. IEEE Transactions on Automatic Control, 2015, 60(11): 2930-2944.

[72] Lu A Y, Yang G H. Input-to-state stabilizing control for cyber-physical systems with multiple transmission channels under denial of service[J]. IEEE Transactions on Automatic Control, 2018, 63(6): 1813-1820.

[73] Wen G H, Wang P J, Huang T W, et al. Distributed consensus of layered multi-agent systems subject to attacks on edges[J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2020, 67(9): 3152-3162.

[74] Zhang T Y, Ye D, Guo G. Distributed event-triggered control for multiagent systems under denial-of-service attacked topology: Secure mode strategy[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2022, 52(10): 6534-6544.

[75] Wu C W, Yao W R, Pan W, et al. Secure control for cyber-physical systems under malicious attacks[J]. IEEE Transactions on Control of Network Systems, 2022, 9(2): 775-788.

[76] An L W, Yang G H. LQ secure control for cyber-physical systems against sparse sensor and actuator attacks[J]. IEEE Transactions on Control of Network Systems, 2019,

6(2): 833-841.

[77] Sun H T, Peng C, Wang Z W. Event-triggered predictive control of cyber-physical systems under DoS attacks[J]. Control and Decision, 2019, 34(11): 2303-2309.

[78] Sun Q, Zhang K W, Shi Y. Resilient model predictive control of cyber-physical systems under DoS attacks[J]. IEEE Transactions on Industrial Informatics, 2020, 16(7): 4920-4927.

[79] Tang X M, Wu M Y, Li M Y, et al. On designing the event-triggered multistep model predictive control for nonlinear system over networks with packet dropouts and cyber attacks[J]. IEEE Transactions on Cybernetics, 2022, 52(10): 11200-11212.

[80] Wang J, Ding B C, Hu J C. Security control for LPV system with deception attacks via model predictive control: A dynamic output feedback approach[J]. IEEE Transactions on Automatic Control, 2021, 66(2): 760-767.

[81] Li F H, Hou Z S. Learning-based model-free adaptive control for nonlinear discrete-time networked control systems under hybrid cyber attacks[J]. IEEE Transactions on Cybernetics, DOI: 10.1109/TCYB.2022.3225203.

[82] Zhang Y H, Wang G, Sun J, et al. Distributed observer-based adaptive fuzzy consensus of nonlinear multiagent systems under DoS attacks and output disturbance[J]. IEEE Transactions on Cybernetics, 2023, 53(3): 1994-2004.

[83] Deng C, Jin X Z, Wu Z G, et al. Data-driven-based cooperative resilient learning method for nonlinear MASs under DoS attacks[J]. IEEE Transactions on Neural Networks and Learning Systems, DOI: 10.1109/TNNLS.2023.3252080.

[84] Wang W, Han Z, Liu K X, et al. Distributed adaptive resilient formation control of uncertain nonholonomic mobile robots under deception attacks[J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2021, 68(9): 3822-3835.

[85] Wang Y M, Li Y X. Adaptive security control of time-varying constraints nonlinear cyber-physical systems with false data injection attacks[J]. Journal of Control and Decision, DOI: 10.1080/23307706.2022.2136274.

[86] Meng M, Xiao G X, Li B B. Adaptive consensus for heterogeneous multi-agent systems under sensor and actuator attacks[J]. Automatica, 2020, 122: 109242.

[87] Jin X, Haddad W M, Yucelen T. An adaptive control architecture for mitigating sensor and actuator attacks in cyber-physical systems[J]. IEEE Transactions on Automatic Control, 2017, 62(11): 6058-6064.

[88] Huang X, Dong J X. Reliable leader-to-follower formation control of multiagent systems under communication quantization and attacks[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2020, 50(1): 89-99.

作者简介

叶丹 (1979–), 女, 教授, 博士生导师, 从事容错控制、自适应控制等研究, E-mail: yedan@ise.neu.edu.cn;

靳凯净 (1995–), 女, 博士生, 从事信息物理系统安全性的研究, E-mail: jinkaijing11@163.com;

张天予 (1994–), 男, 博士后, 从事信息物理系统安全性、分布式估计和控制等研究, E-mail: zhangtianyu@ise.neu.edu.cn.

特邀专家 叶丹, 2001年和2004年于东北师范大学数学系获得学士和硕士学位、2008年于东北大学信息科学与工程学院获得博士学位. 2006年留东北大学任教, 并分别于2008年和2010年被评为讲师和教授. 目前是东北大学教授、博士生导师, 主要从事信息物理系统安全性、容错控制、智能电网及人工智能等研究工作. 曾获得国家自然科学优秀青年科学基金、辽宁省杰出青年基金, 入选教育部新世纪优秀人才、辽宁省“兴辽英才”计划、辽宁省百千万人才工程百人层次. 现为IEEE高级会员、中国自动化学会信息物理系统控制与决策专委会秘书长、控制理论专委会委员等. 以第1(通讯)作者发表期刊论文100余篇、出版学术专著1部; 获全国百篇优秀博士学位论文、教育部自然科学二等奖.

专家寄语 饮水思源, 作为校友, 也作为学校教师, 我深切感谢母校的栽培. 忆往昔, 桃李不言, 自有风雨话沧桑, 看今朝, 厚德载物, 祝母校的未来更加美好, 桃李满天下.