信息物理系统攻击威胁的防御策略综述

文成林[2], 杨　力[1,3†]

(1. 湖州师范学院 工学院, 浙江 湖州 313000; 2. 广东石油化工学院 自动化学院, 广东 茂名 525000;

3. 湖州市工业系统智能感知与优化控制重点实验室, 湖州师范学院 工学院, 浙江 湖州 313000)

摘要: 信息物理系统是一种通过网络空间将物理对象和计算单元相连接的智能系统, 其构建了“感知–传输–决策–控制”的一体化框架. 由于信息物理系统应用于许多基础设施中, 因此其安全问题引起了研究者的兴趣. 首先, 阐述典型的信息物理系统建模方法, 以满足性能分析的需求; 然后, 从数学表示的角度构建3种代表性的网络攻击模型(DoS攻击、欺骗攻击以及重放攻击), 为防御方法的研究奠定基础; 接着, 从特定防御方法和通用防御方法两个方面总结针对信息物理系统的防御手段及最新研究进展; 最后, 从4个不同的角度指出现存问题, 并且探讨了其未来的研究方向.

关键词: 信息物理系统; 特定防御方法; 通用防御方法; 系统建模

引用格式: 文成林, 杨力. 信息物理系统攻击威胁的防御策略综述. 控制理论与应用, 2024, 41(12): 2224 – 2236

DOI: 10.7641/CTA.2023.30195

Research survey on defense strategy of attack threat in cyber physical systems

WEN Cheng-lin[2], YANG Li[1,3†]

(1. School of Engineering, Huzhou University, Huzhou Zhejiang 313000, China;
2. School of Automation, Guangdong University of Petrochemical Technology, Maoming Guangdong 525000, China;
3. Huzhou Key Laboratory of Intelligent Sensing and Optimal Control for Industrial Systems,
School of Engineering, Huzhou University, Huzhou Zhejiang 313000, China)

Abstract: Cyber-physical systems are intelligent system that connect physical objects and computational units through cyberspace, forming an integrated framework of “perception-transmission-decision-control”. As cyber-physical systems are applied to many critical infrastructures, their security issues have attracted researchers’ interest. Firstly, typical modeling methods for cyber-physical systems are presented to meet the needs of performance analysis. Then, three representative network attack models (denial of service attack, spoofing attack and replay attack) are constructed from a mathematical representation perspective, laying the foundation for the study of defense methods. Next, both specific and general defense methods are summarized for cyber-physical systems, and the latest research progress is reviewed. Finally, existing problems are identified from four different perspectives, and future research directions are discussed.

Key words: cyber-physical system; specific defense methods; common defense methods; system modeling

Citation: WEN Chenglin, YANG Li. Research survey on defense strategy of attack threat in cyber physical systems. *Control Theory & Applications*, 2024, 41(12): 2224 – 2236

1　引言

近年来, 随着互联网技术快速发展, “万物互联”的愿景被进一步推动实现[1]. 物理端采集数据量的增加以及云端处理数据能力的提升, 将自动化控制理论、物理端数据采集以及信息层数据处理相结合, 形成信息物理系统. 信息物理系统是计算单元和物理对象在网络环境中高度集成交互而成的智能系统[2], 其构建了“感知–传输–控制” 的一体化框架[3]. 信息物理系统被广泛应用在智能电网、智能交通、智能制造业等[4–9].

目前, 网络空间与物理空间紧密联系, 不断交换信息, 最终成为一个整体[10]. 网络、数据、计算、智能将

收稿日期: 2023−04−07; 录用日期: 2023−12−18.

†通信作者. E-mail: yangli@zjhu.edu.cn.

本文责任编委: 谭永红.

国家自然科学基金项目(U22A2046, 62125307), 湖州市自然科学资金项目(2023YZ47), 湖州市工业系统智能感知与优化控制重点实验室项目(2022–17)资助.

Supported by the National Natural Science Foundation of China (U22A2046, 62125307), the Natural Science Foundation of Huzhou (2023YZ47) and the Huzhou Key Laboratory of Intelligent Sensing and Optimal Control for Industrial Systems (2022–17).

无所不在. 由于网络的开放性和互联性, 以及协议的安全漏洞, 导致了多种、多层次的网络攻击. 网络攻击将导致设备–设备、设备–平台以及设备–计算单元之间基于数据流的交互变得异常. 信息物理系统中的关键设备被不可信的设备更改或替换, 造成系统做出错误决策, 引发非法者获取系统控制权, 进而导致人们的生命和财产安全受到威胁. 保障信息物理系统安全运行成为了一项重要挑战. 美国研究院表明网络安全应具有3个要素: 保密性、完整性以及可用性. 其中, 保密性指的是信息的获取仅限于具有权限的用户或组织; 完整性指的是保证数据或信息的精确性和一致性; 可用性指的是信息能够在任何时刻被授权者访问[11]. 因此, 破坏以上3个要素的行为均被视为网络攻击, 如DoS(denial of service)攻击、黑洞攻击、中间人攻击、恶意代码注入、数据欺诈等. 近年来, 针对信息物理系统的攻击事件频频发生. 例如: 乌克兰电网遭受了突发性停电事故, 造成了70万户居民停电数小时. 事后信息安全公司表示, 这是一起由Black Energy恶意代码导致的蓄意网络攻击事件, 其伪装成了Office 文档的宏入侵了监控与数据采集系统(supervisory control and data acquisition, SCADA) 工作站和服务器, 获取了远程管理权限, 篡改了日志, 破坏了存储数据, 使得变电站自动化系统瘫痪并与调度中心失去联系, 引发了大面积停电[12]; 美国俄亥俄州核工厂遭受蠕虫攻击, 其通过渗透获取了系统的控制权, 破坏了可编程逻辑控制器 (programmable logic controller, PLC)设备, 导致离心机异常故障[13].

本文总结了近些年有关信息物理系统攻击威胁综述性探讨并提出未来方向[3, 14–19], 如表1所示. 从表1中可以得出, 文献[15]从分析现有安全事件出发, 以时间、空间关联性角度对信息物理系统的攻击和防御进行分类和论述. 文献[3]分析了感知、传输、控制一体化面临的问题, 并且论述了分布式状态感知、协同控制等技术的研究进展. 文献[14]论述了在信息系统中的物理层、传输层以及应用层可能遭受的攻击方式, 并且分析了身份认证技术等研究现状. 文献[17]论述了网络漏洞、攻击策略以及攻击检测的最新研究进展. 文献[16]从两个实际案例出发, 综述信息物理系统相关的7个技术的研究进展. 文献[18]从基于时间驱动和基于事件驱动的角度综述了可用性攻击和完整性攻击的原理和防御策略.

与以上所述相异, 基于控制理论的角度, 本文从主动攻击防御和被动窃听防御两个角度对信息物理系统的防御方法进行综述, 并提出了现存问题和挑战. 首先, 本文介绍了信息物理系统模型、常见的3种攻击威胁模型以及被动窃听威胁模型; 然后, 基于对攻击威胁的认知, 本文分别综述了针对信息物理系统的主动攻击和被动窃听的防御方法的最新研究进展; 最后, 本文指出了现存问题及挑战并总结了全文.

文章余下部分的结构如下: 第2节介绍了系统模型和攻击模型; 第3节从主动攻击和被动窃听介绍了安全防御方法的相关研究进展; 第4节介绍了现存问题与挑战; 第5节总结全文, 并且分析了当前信息物理系统的网络安全技术面临的问题与挑战, 并指出潜在研究方向. 如图1所示.

2　信息物理系统模型和攻击模型介绍

本节将分别介绍信息物理系统模型和常见的3种攻击手段(DoS攻击、欺骗攻击和重放攻击)的数学建模方法.

2.1　信息物理系统模型

信息物理系统(cyber-physical system, CPS)将物理层与信息层相连接, 其构建了基于数据流动的状态感知、实时分析、科学决策、精准执行的闭环体系[20], 如图2所示. 信息物理系统的数学建模能够准确的了解其工作机理, 并且对防御方法的设计起到了重要的作用. 下面将分别从物理层和信息层对信息物理系统进行简单的建模阐述.

2.1.1　物理层

基于控制论的角度, 信息物理系统的物理层主要包括传感器设备和控制单元等. 物理层实现状态感知和精准执行的目的. 本文以离散时间线性时不变系统为例[21], 构建信息物理系统中的物理设备的系统方程和观测方程如下:

$$\begin{cases} x(k+1) = Ax(k) + Bu(k) + w(k), \\ y(k) = Hx(k) + v(k), \end{cases} \tag{1}$$

其中: $k \in \mathbb{Z}$为离散时间序列; $x(k) \in \mathbb{R}^n$为系统的状态向量, 假设系统的初始状态向量为$x(0)$; $y(k) \in \mathbb{R}^m$为传感器的测量向量; $u(k)$为系统的输入向量; $A \in \mathbb{R}^n$, $H \in \mathbb{R}^{m\times n}$; $w(k) \in \mathbb{R}^n$为过程噪声, 假设其为高斯白噪声, 均值为0, 方差为$Q \geqslant 0$; $v(k) \in \mathbb{R}^m$为测量噪声, 假设其为高斯白噪声, 均值为0, 方差$R \geqslant 0$. $x(k)$, $w(k)$以及$v(k)$之间是相互独立.

注 1　线性时不变系统是指系统的输入和输出具有线性关系, 其满足叠加原理, 并且系统的参数不随时间而变化[22]. 本文以离散时间线性时不变系统为例从控制的角度阐述信息物理系统中物理层的简单建模形式.

2.1.2　信息层

信息物理系统的信息层主要包括远程状态估计器等. 信息层实现实时分析和科学决策的目的. 远程状态估计器是信息物理系统中的计算单元. 该组件接收物理层传输的数据, 并基于算法产生控制命令传输至执行器. 本文以目前研究广泛采用的基于Kalman滤波的远程状态估计器为例, 阐述其工作原理[23]如下:

$$\bar{x}(k|k-1) = A\bar{x}(k-1|k-1) + Bu(k), \tag{2}$$

$$\bar{P}(k|k-1) = A\bar{P}(k-1|k-1)A^{\mathrm{T}} + Q, \tag{3}$$

$$K(k)=\bar{P}(k|k-1)H^{\mathrm{T}}[H\bar{P}(k|k-1)H^{\mathrm{T}}+L]^{-1}, \tag{4}$$

$$\bar{x}(k|k)=\bar{x}(k|k-1)+K(k)(y(k)-H\bar{x}(k|k-1)), \tag{5}$$

$$\bar{P}(k|k)=\bar{P}(k|k-1)-K(k)H\bar{P}(k|k-1), \tag{6}$$

其中: $\bar{x}(k|k)$为估计值; $\bar{x}(k|k-1)$为预测值; $\bar{P}(k|k-1)$是$\bar{x}(k|k-1)$的协方差; $\bar{P}(k|k)$是$\bar{x}(k|k)$的协方差; $K(k)$为Kalman滤波器的增益.

注 2 在上述讨论中, 将物理设备的状态方程和观测方程均建模为线性方程, 因此, 远程状态估计器采用了Kalman滤波方法. 本文只是以线性系统作为例子以说明信息物理系统的结构. 在实际工程中, CPS的物理层常为非线性系统, 而远程状态估计器采用非线性Kalman滤波算法, 例如: 扩展卡尔曼滤波(extended Kalman filter, EKF)、无迹Kalman滤波(unscented Kalman filter, UKF)以及特征函数滤波等[24–26].

表 1 综述性文章的主要贡献和未来方向

Table 1 Main contributions and future directions of research paper

文献(发表年)	主要贡献	未来方向
[14](2016)	* 阐述了信息层、物理层以及信息和物理交互的安全挑战 * 介绍了针对物理层和传输层的攻击 * 综述了基于传统IT系统、入侵检测系统、身份认证技术以及隐私保护技术的抗攻击方法	• 解决安全机制保护物理层密钥的研究问题 • 解决系统漏洞的全面性分析的研究问题 • 解决一体化的系统安全架构的研究问题
[15](2019)	* 提出了针对信息物理系统的安全威胁模型(通用型模型) * 全面介绍了针对信息物理系统的攻击手段(空间隐蔽型、时间隐蔽型、空间–时间隐蔽型、非隐蔽型攻击) * 综述了针对信息物理系统的防御方法(信息层防御、物理层防御、基于信息物理融合的通用防御方法)	• 解决由人类嵌入信息物理系统中带来的信息安全和人类社会安全相结合的研究问题 • 解决信息层的防御方法和物理层的防御方法相结合的研究问题
[3](2019)	* 阐述了基于“感知–传输–控制”的工业网络一体化设计和面临的挑战 * 综述了非理想通信下异构网络分布式融合估计研究进展 * 综述了面向感知和控制的适变传输研究进展 * 综述了网络环境下的复杂系统协同控制研究进展	• 在感知层, 解决估计算法的测量预测误差的更新和信息交互的研究问题 • 在传输层, 解决有限资源下信息实时传输交互的安全性研究问题 • 在控制层, 解决因控制对象的性质与结构发生变化而改进反馈控制算法的研究问题
[16](2019)	* 综述了CPS感知设计、CPS信息处理、CPS建模与认知、CPS决策与控制、CPS集成设计技术、数字孪生技术、CPS安全性技术 * 介绍了CPS的两个实际案例: 基于Internet的网络化三容水箱系统和智能船舶运行与维护系统	• 解决开放空间下保证CPS服务的持续性、正确性、安全性的研究问题 • 解决数字孪生建模的准确性、实时性等技术的研究问题 • 解决缺少面向CPS复杂层级应用的新型架构设计的研究问题
[17](2020)	* 介绍了智能电网系统的网络安全目标、要求以及关键组件 * 综述了针对智能电网系统的完整性攻击及防御方法、可用性攻击及防御方法、应用层攻击及防御方法	• 解决针对不断发展的零日攻击的防御方法研究问题 • 解决开发系统的“自愈”能力(例如: 信息层的计算恢复能力)的研究问题 • 解决智能电网广域态势感知和新技术和新指标的研究问题
[18](2022)	* 综述了基于时间驱动系统的可用性攻击(DoS攻击)的原理和防御策略 * 综述了基于时间驱动系统和基于事件驱动系统的完整性攻击(欺骗攻击)的原理和防御策略	• 解决高级攻击(以随机方式发起的攻击)的有效防御的研究问题 • 解决机密性攻击、隐身攻击的有效防御的研究问题 • 解决参数设计的合理性的研究问题
[19](2018)	* 总结CPS的典型系统模型 * 揭示了3种典型的网络攻击的原理, CPS攻击检测的研究进展	• 解决CPS同时受到多种攻击下系统的自适应补偿策略的研究问题 • 解决提高检测率的研究问题, 通信网络不完美的情况下(存在丢包和延迟)新的检测方法和补偿策略的研究问题

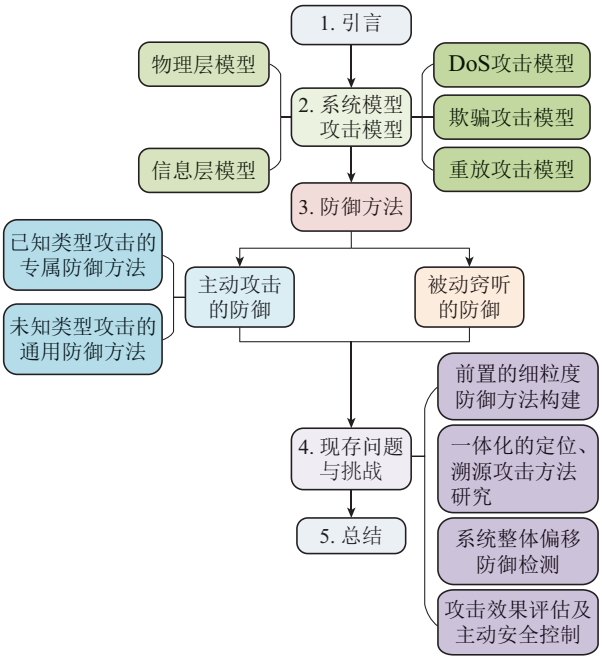

图 1　文章结构图

Fig. 1　Paper structure chart

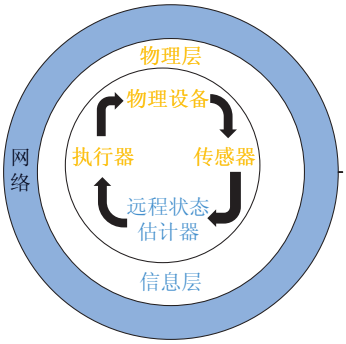

图 2　信息物理系统模型

Fig. 2　Cyber physical system

2.2　攻击模型

不懂攻击, 就不知道如何防御. 对恶意攻击进行防御之前, 需要认识和了解攻击威胁. 攻击威胁分为主动攻击和被动窃听. 下面将进行简单介绍.

2.2.1　主动攻击

主动攻击手段丰富多样, 本文仅讨论常见的3种主动攻击场景, 即: DoS攻击、欺骗攻击以及重放攻击. DoS攻击是一种典型的网络攻击, 其主要通过发射强干扰信号阻止设备之间的数据包传输, 达到限制访问服务的目的[27], 如图3所示. 在信息物理系统中, 攻击者通过对元器件之间传输数据包的完整性进行修改的攻击被称为欺骗攻击[28], 如图4所示. 在重放攻击中, 攻击者发动攻击主要分为两步: 首先在攻击发动前一段时间内记录系统传输数据; 然后在攻击发动时, 将之前记录的传输数据重放入系统中[29], 如图5所示.

在本文中, 采用如下表达式对主动攻击行为进行建模[30]:

$$\begin{cases} x(k+1) = Ax(k) + Bu(k) + w(k), \\ y(k) = Hx(k) + v(k), \\ \tilde{y}(k) = \beta(k)(y(k)) + \lambda(k)a(k), \end{cases} \tag{7}$$

其中: $x(k)$, $u(k)$, $w(k)$, $v(k)$, A, B以及H与式(1)中定义相同; $y(k)$表示在k时刻物理层设备传输的测量值; $\tilde{y}(k)$表示在k时刻远程状态估计器接收到的测量值; $a(k)$表示攻击者篡改的数据值.

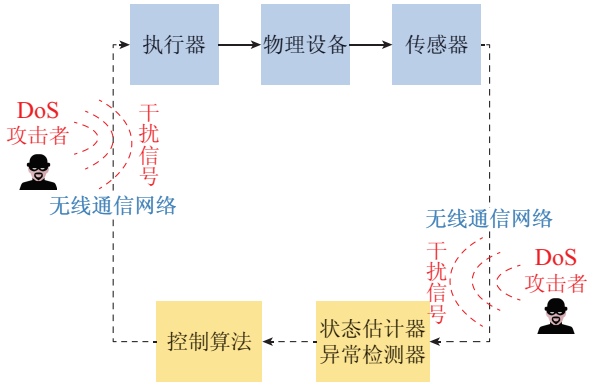

图 3　DoS攻击

Fig. 3　DoS attack

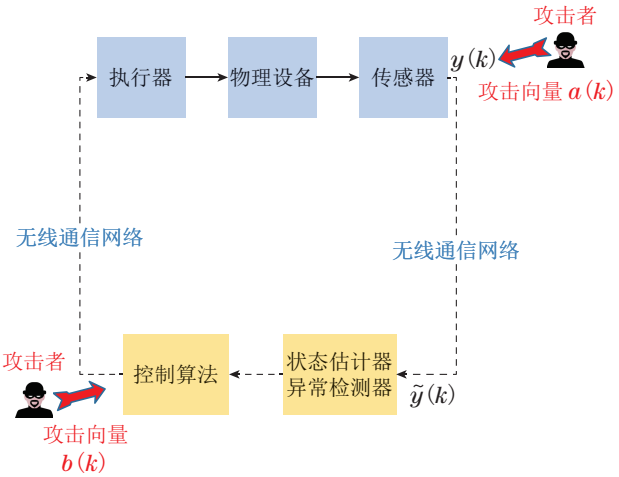

图 4　欺骗攻击

Fig. 4　Spoofing attack

对式(7)进行讨论: 如果$\beta(k) = 0, \lambda(k) = 0$, 则$\tilde{y}(k) = 0$意味着DoS攻击(即: 远程状态估计器无法接收测量值)的发生. 如果$\beta(k) = I, \lambda(k) = I$, 则$\tilde{y}(k) = y(k) + a(k)$ 意味着欺骗攻击(即: 远程状态估计器接收篡改之后的测量值)的发生. 如果$\beta(k) = I, \lambda(k) = I, a(k) = y(k-n) - y(k), n = 1, 2, \cdots, k-1$, 则$\tilde{y}(k)$意味着重放攻击(即: k时刻的状态值对应$k-n$时刻的测量值)的发生. 如果$\beta(k) = I, \lambda(k) = 0$意味着没有攻击发生[31].

注 3　本文只介绍了常见的3种攻击手段. 这3种攻击手段是基础的攻击方法, 其容易发动且对系统具有大的破坏效果. 各种类型的攻击手段实质可以归纳于该3种之一.

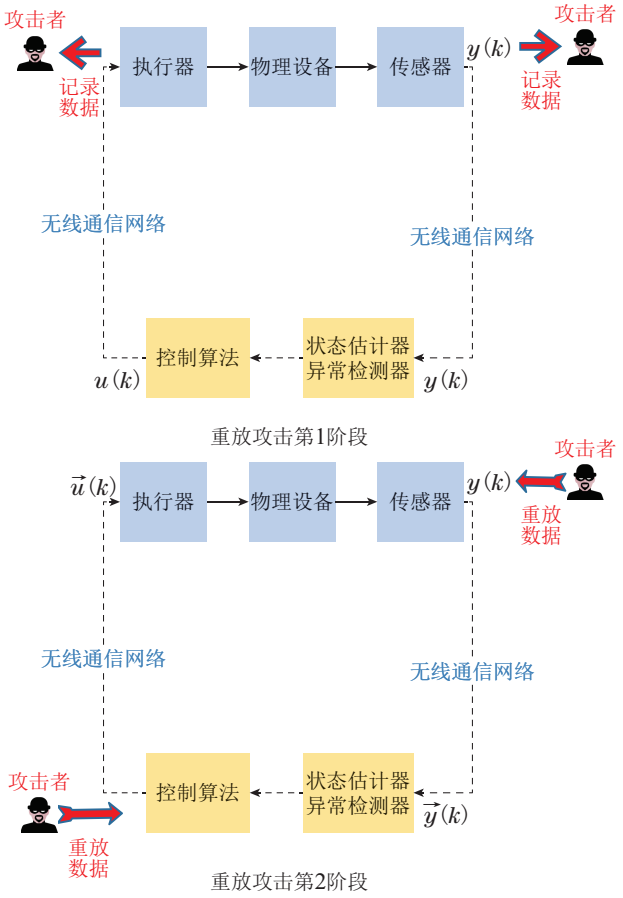

图 5 重放攻击

Fig. 5 Replay attack

2.2.2 被动窃听

被动窃听是一种异于主动攻击的攻击方法. 窃听者对无线通信潜伏以窃取传输数据. 窃听攻击和主动攻击不同, 主动攻击会造成信息的丢包或者篡改, 但是被动窃听只会造成信息的泄露. 如图6所示. 本文采用如下表达式对被动窃听进行建模:

$$\vec{y}(k) = \theta(k)y(k), \tag{8}$$

其中: $\vec{y}(k)$表示窃听者窃取的信息; $y(k)$表示在k时刻物理层设备传输的测量值; $\theta(k) = 1$表示成功地窃听信息; $\theta(k) = 0$表示失败地窃听信息.

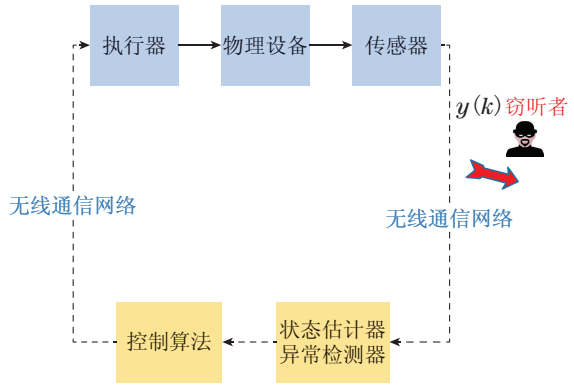

图 6 被动窃听

Fig. 6 Passive eavesdropping

3 信息物理系统的网络安全防御方法

在计算技术、控制技术以及通信技术的相关领域, 分别从主动攻击威胁的安全防御和被动窃听威胁的安全防御两个方面, 研究者们持续推动着对CPS安全问题的相关研究. 在本小节中, 将综述针对信息物理系统的网络安全防御方法的最新研究进展.

3.1 针对主动攻击的防御方法

3.1.1 已知攻击类型的特定防御方法

针对已知类型的主动攻击, 研究者们提出了特定的防御方法. 典型的主动攻击威胁包括DoS攻击、欺骗攻击和重放攻击.

针对DoS攻击的防御方法[32–41], 如表2所示. 方法1: 研究者们提出了事件触发机制来抵御DoS攻击, 例如文献[32–33, 42]等. 事件触发机制的优点在于能够节约系统资源. 不同的事件触发机制代表了研究者针对DoS攻击不同的防御思想. 方法2: 研究者们提出了DoS攻击下改进的滤波器算法, 例如文献[34–35]等. 改进的滤波器算法的本质是加强系统抵抗攻击的鲁棒性. 方法3: 研究者们提出了以补偿算法来抵御DoS攻击, 例如文献[37–38, 43]等. DoS攻击的本质是导致传输信息的丢失, 而补偿算法能够为系统弥补丢失的信息. 方法4: 研究者们提出了弹性的防御策略以防御DoS攻击, 例如文献[39–41]等. 由于攻击者的能量有限, 因此通过物理层的弹性传输策略是保证系统免受DoS攻击的重要方法.

针对欺骗攻击的防御方法[28, 44–52], 如表3所示. 方法1: 研究者们对基于Kalman滤波残差的卡方检测器进行改进得到新型的检测器. 例如文献[44–46]等. 研究者们运用了类似于KL散度(Kullback-Leibler divergence)、欧式距离度量等度量方式用于检测欺骗攻击行为. 方法2: 与DoS攻击相似, 研究者们同样也提出了欺骗攻击下改进的滤波算法和补偿算法, 例如文献[49–50, 53]等. 加强系统的鲁棒性实现容忍攻击是防御攻击的重要方法. 方法3: 研究者们从两个方面对欺骗攻击进行防御, 即提出了基于事件触发机制, 并且同时设计观测器和执行器的控制算法, 例如文献[44, 47–48]等. 方法4: 研究者们提出了基于零和博弈的思想的防御方法, 例如文献[51]等. 从攻击者和防御者相互博弈的过程中实现对系统的保护. 方法5: 研究者们从能量变换的角度提出了防御方法, 例如文献[52]等. 基于能量变换的检测手段是一种新型的防御方法.

针对重放攻击的防御方法[38, 54–59], 如表4所示. 方法1: 研究者们采用随机编码的方案对重放攻击进行防御, 例如文献[54, 60]等. 不同编码的形式代表了研究者不同的防御思想, 例如: 基于随机编码的方式防御重放攻击、基于特定规则的编码方式防御重放攻击

等. 方法2: 研究者们提出了重放攻击下系统的控制算法和补偿算法作为防御手段, 例如文献[57–58, 61]等. 该方法与DoS攻击和欺骗攻击的思想相类似, 不同的是设计的算法相异. 方法3: 研究者们提出了水印的防御方法, 例如文献[55–56, 62]等. 利用水印方法检测重放攻击是当前防御者使用最频繁的措施, 许多改进的水印的方法被研究者们提出. 基于物理水印的主动防御方法的本质是在控制系统的输入中添加攻击者未知的信号, 基于输出检测系统是否存在攻击. 方法4: 研究者们采用了时间戳机制防御重放攻击, 例如文献[59, 63]等. 基于时间戳机制防御重放攻击是简单的防御方法.

表 2 DoS攻击防御方法

Table 2 DoS attack defense methods

防御策略	文献(发表年)
事件触发机制防御DoS攻击:	
利用弹性事件触发机制产生的触发状态消除DoS攻击对系统性能的影响	[32](2019)
设计了一种事件触发通信策略(预测的估计误差协方差超过阈值时观测值传输)以保护DoS攻击下的CPS	[33](2022)
基于鲁棒的改进滤波算法防御DoS攻击:	
提出适用DoS攻击下的改进无迹Kalman滤波方法	[34](2019)
DoS攻击多传输通道场景下, 利用协方差交集融合方法和矩阵全等变换秩设计状态估计	[35](2022)
构建了自适应观测器, 从而提高了远程估计器的估计精度	[36](2021)
DoS攻击威胁下控制策略防御DoS攻击:	
借助了李雅普诺夫函数理论, 针对非线性信息物理系统, 设计了一种DoS攻击下的补偿控制方案	[37](2019)
提出了基于李雅普诺夫理论的自适应方法来实现闭环系统在DoS攻击下的有界稳定性	[38](2020)
弹性策略防御DoS攻击:	
提出了CPS的网络层和物理层的组合设计, 其中包含了弹性控制器的设计和弹性防御策略的设计	[39](2017)
提出了两个观测机制, 其中一个通过引入缓冲机制来消除通信延迟, 另一个引入弹性机制来抵抗DoS攻击	[40](2020)
基于通信网络建模提出了一种新颖的多通道传输框架以降低被DoS攻击的可能性	[41](2018)

表 3 欺骗攻击防御方法

Table 3 Spoofing attack defense methods

防御策略	文献(发表年)
改进卡方检测器防御欺骗攻击:	
对非线性系统提出了一种针对欺骗攻击的攻击缓解的控制算法, 其利用了李雅普诺夫稳定性定理	[44](2021)
提出了基于欧氏距离度量改进卡方检测器的攻击检测方法	[45](2014)
提出了基于改进卡方检测器的KL散度检测器	[46](2021)
基于事件触发机制防御欺骗攻击:	
设计了事件触发的自适应控制器和自适应控制率, 以补偿在欺骗攻击和执行器故障下非线性系统性能损失	[47](2021)
提出了一种基于事件触发机制的自适应滑膜控制方法	[48](2022)
欺骗攻击威胁下控制策略防御欺骗攻击:	
提出了欺骗攻击下一种具有事件触发方案的状态估计算法	[49](2017)
提出了一种针对欺骗攻击的不安全系统保护方法, 并且应用于飞行器状态估计系统中	[50](2018)
设计了一种互联的自适应观测器在线估计攻击效果, 并基于攻击效果, 提出了具有弹性的安全控制方案	[28](2022)
基于零和博弈和能量转换的方法防御欺骗攻击:	
提出了在执行器虚假数据注入攻击情形下信息物理系统基于零和博弈的安全控制器	[51](2021)
基于能量转换的角度建立一种针对欺骗攻击的防御框架, 通过设计能量控制器动态调整攻击引起的系统能量变化	[52](2021)

3.1.2 未知攻击类型的通用防御方法

针对未知的攻击类型, 研究者们提出了通用的防御方法[64–70]. 如表5所示.

基于传统计算机网络安全, 研究者提出了入侵检测器. 其中分为基于数据包的入侵检测方法和基于网络流量的入侵检测方法, 例如文献[64–66]等. 机器学习算法的快速发展促进了入侵检测系统准确率的提升/误报率的下降, 近些年研究者们也提出了诸多改进机器学习算法的方法. 但是, 该方法对于数据样本的依赖程度大, 对于训练数据样本中的完整性和质量性有很高的要求.

基于密码学的贡献, 研究者们将加密/解密用于防

御攻击, 例如文献[67–68]. 物理层中传感器的计算能力和能耗有限, 复杂的加密算法难以应用于实际工程中, 为此, 轻量级加密的方法被研究者们所关注. 同样, 研究者们也提出了许多有关加密的状态估计算法, 使得信息层中远程状态估计器能够直接使用加密的数据而不影响状态估计的误差.

表 4 重放攻击防御方法

Table 4 Replay attack defense methods

防御策略	文献(发表年)
基于随机编码防御重放攻击:	
提出了随机编码方案, 使CPS在正常数据和受损数据之间产生协方差差异以检测重放攻击	[54](2019)
基于水印防御重放攻击:	
利用伪随机数作为水印对传输的数据进行加密和解密	[55](2020)
提出了一种周期性水印策略防御重放攻击检测	[56](2020)
重放攻击威胁下控制策略防御重放攻击:	
研究者提出了在重放攻击下非线性系统的自适应控制方法, 保证即使存在重放攻击, 控制系统也不会崩溃	[57](2020)
在系统中独立的设置了一个观测器估算每个信号的输出, 用于补偿因受到重放攻击损失的性能	[38](2019)
系统在重放攻击场景下恢复能力提供了可行条件	[58](2019)
时间戳机制防御重放攻击:	
提出了一种基于时间戳的远程用户认证方案, 该方案使用椭圆曲线密码机制	[59](2013)

表 5 通用防御方法

Table 5 General defense methods

防御策略	文献(发表年)
入侵检测器技术防御:	
开发了基于深度学习的异常检测系统	[64](2022)
设计了基于双自动编码器无监督深度学习模型用于CPS的异常检测	[65](2022)
基于机器学习算法提出了纵深防御概念的网络攻击检测系统	[66](2019)
密码学技术防御:	
使用部分同态加密设计了一种基于加密的状态估计	[67](2020)
设计了基于压缩感知的轻量级加密方案	[68](2020)
身份认证技术防御:	
提出了基于过程噪声为指纹的身份认证方法	[69](2021)
提出了去中心化身份认证方法	[70](2022)

身份认证是一种辅助系统防御体系的方法. 研究者们对此方法也做了相关研究, 例如文献[69–71]. 身份认证能够保证设备单元接收数据的合法性, 基于此类方法, 对于能够证明数据唯一性的身份(特征)显得尤为重要. 同样, 认证的方法在目前的研究中未被重视, 其存在很大的研究前景.

3.2 针对被动窃听的防御方法

被动窃听攻击是指窃听者基于潜伏行为而获取系统信息. 本文总结了常见的被动窃听攻击的防御方法[72–78], 如表6所示. 差分隐私技术被研究者们用于防御信息物理系统的被动窃听攻击, 例如: 文献[72, 79–80]等. 差分隐私是近些年被广泛用于保护信息隐私安全的方法. 其主要分为: 基于拉普拉斯机制、基于高斯机制、基于指数机制和基于混合机制等. 其次, 研究者们提出基于轻量级信息加密的方法, 例如: 文献[73–74, 81]等. 与第3.1节中阐述的相类似, 加密方法可以保护数据的完整性和保密性.

研究者们采用噪声扰动的策略以实现被动窃听威胁的防御, 例如: 文献[75–76]等. 噪声扰动技术使得窃听者从窃取的数据中难以获取有用的信息. 当然, 如何保证所加噪声的扰动不会影响接收端数据的可用性成为了具有争议性的问题. 以不破坏系统性能为前提, 如何选择适当的噪声扰动以保护信息的传输. 同样, 基于噪声扰动的策略对于窃听者的“惩罚”效果有限(惩罚是指窃听者使用添加了噪声的信息对其的影响程度).

基于编码机制的被动窃听防御方法被研究者们所提出, 例如: 文献[77, 82–83]等. 基于编码机制的本质是找寻一种方法对原始数据进行变换. 将编码机制应用于信息物理系统中存在许多挑战, 例如: 在系统正常工作下, 编码之后的信息如何不牺牲系统的估计性能, 编码之后的信息如何不增加传输网络的繁重性, 以及评估每个时刻是否需要编码操作(编码的收益和代价之比)等.

表 6 被动窃听的防御方法

Table 6 Defense methods for passive eavesdropping

防御策略	文献(发表年)
差分隐私技术防御:	
针对智能车辆信息物理系统的车辆位置和轨迹隐私问题, 提出了具有差分隐私保护的估计器	[72] (2021)
轻量级身份加密技术防御:	
提出了一种轻量级数据加密方案, 保护工业数据在网络传输过程中不被窃听	[73](2021)
提出了一种双去噪自动编码器对传输的数据进行加密, 在接收端由残差生产器判断数据是否可信	[74](2021)
噪声扰动技术防御:	
提出了一种隐形人工噪声策略以防御窃听攻击	[75](2022)
提出了一种将线性变换和人工噪声相结合的编码机制	[76](2020)
编码机制技术防御:	
在传感器处设计一种编码方案, 对状态信息进行编码	[77](2019)
区块链技术防御:	
针对无人机的信息物理系统, 提出了一种基于区块链的安全机制, 其中将深度学习融入区块链中	[78](2020)

随着近些年区块链技术被提出, 研究者们将其应用于信息物理系统中, 例如文献[78, 84–85]等. 区块链技术由数据节点组成. 数据节点之间的通信采用哈希算法进行加密. 所有参与的节点都知道区块链中的每笔交易信息. 区块链技术包含有以下特性: 不可变性(采用哈希算法加密)、透明性(将账本进行广播)、真实性(交易各方拥有准确的数据)、去中心化(没有单一的控制实体)、分布性(记录账本的计算机分布在不同地点)、无中介(智能合约)以及匿名(非对称算法)[86–87]. 信息物理系统的特点包括: 网络的高效连接、智能决策系统以及设备间的互动性等. 将区块链技术应用于信息物理系统中, 存在许多挑战, 例如: 哈希算法和传输网络带宽受限、账本广播和数据隐私以及决策系统和匿名相互之间的矛盾等.

3.3 讨论

3.3.1 针对主动攻击的防御方法的讨论

1) 针对已知攻击类型的特定防御方法的讨论.

针对DoS攻击的检测方法所述. 对于事件触发机制的方法, 事件触发器需要嵌入传感器中. 在实际工程中, 由于环境的复杂性导致事件触发方法存在不确定性. 并且, 基于事件触发机制对于系统性能的损失是需要持续关注的问题. 同样, 信息物理系统部署在恶劣的外部环境中, 无线通信网络存在丢包和延迟. 因此, 检测器需要区分丢包和DoS攻击是需要持续关注的问题. 对于网络攻击的防御方法包括攻击检测和安全控制. 对于改进滤波算法和性能补偿方法, 当前的研究建立在物理层建模为线性系统的基础上, 对于实际工程建模为非线性系统的DoS攻击安全控制研究是需要持续关注的问题.

针对欺骗攻击的检测方法所述. 欺骗攻击包括有虚假数据注入攻击, 其与干扰噪声、故障相类似但又相异. 相似点在于均会对系统性能造成损失, 相异点在于其原理不同, 攻击威胁的发动者更加智慧. 因此, 如何提高检测器对于虚假数据注入攻击、干扰噪声以及故障的区别, 提高攻击的检测率和降低攻击的误报率是需要持续关注的问题. 同样, 随着攻击者对系统结构和参数的了解以及先验知识的不断丰富, 精心设计的虚假数据矩阵能够绕过现有检测器的检测, 例如文献[88]. 因此, 随着攻击者所设计的虚假数据矩阵更加隐蔽性, 检测器的通用性和不断的更新是需要持续关注的问题.

针对重放攻击的检测方法所述. 对于添加水印的方法, 需要持续研究添加的水印信号对系统性能的影响小而带来优异的检测性能. 对于基于编码的防御方法, 编码矩阵的设计显得十分重要. 轻量级的编码矩阵是该方法需要持续关注的问题. 同样, 对于不存在重放攻击的时间段内, 添加水印对系统所引发的代价以及编码、水印所需要的额外成本是需要持续关注的问题.

2) 针对未知攻击类型的通用防御方法的讨论.

针对入侵检测器的方法所述. 基于数据包的入侵检测器技术依赖于大量的训练数据集. 训练数据集可能未包含完整的攻击数据, 并且获取具有丰富且准确标签的代表性数据集代价大(Ring等人在文献[89]中也提出了相同的观点), 因此基于数据包的入侵检测器无法检测未知的攻击行为. 由于物理层数据的篡改不会引起网络流量的异常改变, 因此, 基于网络流量的入侵检测器针对物理层的数据篡改行为无法检测.

针对密码学的方法所述, 对数据进行加密和解密. 加密方法对无线传输通道的带宽有很高要求, 并且传统的基于密码学的方法在处理大数据方面效率不高.

针对身份认证的方法所述. 基于过程噪声的指纹身份认证方法对微小数据篡改(尤其是将攻击向量隐

藏在噪声中)的攻击行为难以检测. 并且, 以噪声和残差作为指纹的身份认证方法的前提是建立准确的过程动力学模型, 这是一件很困难的事情. “身份”在辅助防御系统中相当于是独有特征的提取. 目前, 研究者们专注于“身份”的讨论, 并没有提及“认证”的方法. “认证”在辅助防御系统中相当于是特征的匹配, 涉及到度量单位的讨论. 在手机端的身份认证技术: 伴随着从指纹认证发展到人脸认证(人脸的身份认证相比指纹的身份认证, 其能够提取的特征更加的多样性, 包括: 眼睛、鼻子、嘴巴、脸型等). 受此启发, 设备–设备、设备–平台以及设备–计算单元之间的身份认证技术进度缓慢, 值得研究者进一步研究.

3.3.2 针对被动窃听的防御方法的讨论

针对加密的防窃听攻击方法, 其加密过程过重, 造成系统资源消耗、信息延迟等问题. 针对噪声编码的方法, 其研究者采用的编码机制是对信息添加高斯噪声或者非高斯噪声. 当然, 近些年研究者们提出了一些基于高斯噪声或者非高斯噪声的改进编码机制, 这些机制从防御者角度添加了节约传输能量等目标函数, 以实现编码传输信息的目的. 如果窃取者在不知情的状况下窃取信息并将其使用, 基于噪声编码机制的方法仅能有限的破坏窃取者系统性能. 至今研究者们没有从惩罚窃听者的角度提出编码机制. 基于同态加密的方法在处理大数据方面效率不高. 文献[90]通过调度以防御窃听威胁. 这本身并不能作为针对窃听威胁的主要防御手段. 研究者在文献[91]中表明, 攻击者无法每时刻监听全部无线通信信道. 基于能量受限的传感器/能量受限的噪声发射机, 每个时刻均对传输的信息加密/编码是不现实的事情. 当然, 单一的防御手段不能完全的保证窃听攻击的防御. 多层次的防御能够有效的降低窃听者成功的概率. 由于计算能力的代价昂贵, 采用基于物理层的调度方法能够不需要任何计算能力为代价的保护系统免受窃听攻击.

4 现存问题与挑战

随着计算技术、通信技术、感知技术以及控制技术的快速发展, 信息物理系统被应用于许多关键设施中. 网络的开放性和攻击手段的丰富性给信息物理系统的安全带来了极大的挑战. 以下讨论针对信息物理系统安全防御方法现存问题与挑战:

1) 前置的细粒度防御方法构建.

由于攻击方式的隐蔽性和破坏性日益增强, 因此, 必须在攻击者渗透网络防御之前阻止攻击, 同时影响攻击者的行为方式. 依据攻击的演化分为: 攻击的征兆→隐式的攻击→微小的攻击显现→显式的攻击出现→显著的攻击涌现. 针对显著和显示的攻击, 如何提高攻击检测的准确率和降低攻击检测的误报率是当前存在的问题, 估计系统受攻击程度是亟待解决的问题. 针对微小和隐式的攻击, 攻击行为被噪声所参杂/覆盖, 如何分离攻击和噪声是当前存在的问题, 如何从混杂攻击和噪声中检测出攻击是亟待解决的问题. 对不同层次的攻击过程构建改进的检测算法、全面的防御策略以及深层次的防御体系将是未来研究的挑战.

完备的特征提取是提高攻击检测的准确率的前提. 将特征提取的精细程度划分为粗粒度特征提取和细粒度特征提取. 细粒度特征与粗粒度特征是相对的, 例如在使用多维泰勒网对特征提取时, 视泰勒展开的1次系数作为粗粒度特征, 泰勒展开的2次系数作为细粒度特征(2次系数展开式相对1次系数展开式, 其包含的信息更加丰富). 目前, 粗粒度的防御方法需要更加的精细化、多样化和不断“学习”化(更新). 防御不是一蹴而就, 不同层次的攻击需要不同粒度、多类型的检测手段. 对微小的攻击, 本文提出基于设备指纹的多级身份认证思想: 一种基于真实数据的身份认证方法, 该方法以多级数学表示、多粒度特征提取和多尺度匹配为一体化防御框架[71]. 特别地, 在攻击的前置时期, 准确的防御对系统的安全运行显得十分重要. 前置防御时期, 对重要性大的单元组件部署更多的防御资源. 因此, 对单元组件的重要性评估显得尤为重要. 本文提出思想: 平均影响度 (mean impact value, MIV)算法是评估神经网络中神经元节点重要性的方法. 将MIV与集中式Kalman滤波算法相结合, 用于评估系统中单元组件的重要性[23].

2) 一体化的定位、溯源攻击方法研究.

随着科学技术的快速发展, 嵌入信息物理系统中的设备单元数量繁多、复杂且异构. 确认受攻击设备单元之后的定位攻击漏洞是目前存在的问题. 定位攻击之后的攻击类型辨识和溯源攻击是亟待解决的问题. 溯源攻击分为溯源攻击的首次发动时间和溯源攻击的路线. 溯源机制问题可分为建模为线性溯源问题和建模为非线性溯源问题. 针对建模为线性溯源问题, Kalman滤波算法可以实现平滑估计. 因此, 针对建模为非线性溯源问题, 以高斯和非高斯噪声场景下, 如何实现首次攻击时间溯源和攻击路线溯源是未来研究的挑战.

将确认受攻击的设备单元、定位攻击、辨识攻击和溯源攻击分解建模为多个数学问题. 本文提出的思想: 构建设备单元健康管理系统, 在线监控设备状态; 基于机器学习方法对受攻击系统实时检测和分类, 依据攻击者最大化破坏系统性能的原则, 构建攻击对系统性能影响的趋势分析和预测模型; 依据攻击行为特征和类型数据库, 建立攻击模型的参数在线辨识方法; 依据非线性滤波器解决非线性溯源建模问题, 以输出纠偏原则逆向重构攻击路线图[92–94].

3) 系统整体偏移防御检测.

针对复杂信息物理系统, 攻击者采用新型的集成式微弱攻击手段场景. 集成式微弱攻击是指攻击者针对系统中多个单元组件发动微弱的攻击. 单个单元组件的性能破坏效果弱, 但是整个系统性能却受到强的破坏效果. 为此, 基于部署的单个单元组件的检测方法无法预警, 需要部署系统整体性能偏移检测方法将是未来研究的挑战.

微弱攻击的发生可能是绝对变化量很小, 但是相对变化率较大. 例如, 数据从1篡改到2, 其绝对变化量为1, 相对变化率为100%, 而数据从1000篡改到1001, 其绝对变化量也为1, 但是相对变化率为0.1%. 因此, 本文提出的思想: 以系统整体性能输出为对象, 基于空间域转换(数据低维空间投影转换数据高维空间投影), 构建数据变换率的攻击检测方法[95–96].

4) 攻击效果评估及主动安全控制.

基于攻击下系统运行是保证系统安全性的最后一道防线. 滤波器的改进及性能补偿算法是目前研究者们常依赖的技术. 基于系统攻击受损的评估结果, 建立及时且自适应的鲁棒、容错的主动安全控制方法是亟待解决的问题. 对于真实的信息物理系统, 其物理单元通常为非线性系统. 当系统建模为非线性系统时, 如何对其进行线性逼近其参数是当前研究的挑战性问题[97–98]. 物理单元建模为非线性系统时, 远程状态估计器采用基于非线性系统的多项式容侵滤波算法以及系统基于自适应滑模技术将是未来研究的挑战.

本文提出的思想: 依据评估系统受到不同程度的攻击效果, 建立系统自适应的性能补偿算法. 同时, 将拟态防御[99](邬江兴院士提出)融入系统安全防御体系中, 构建基于拟态防御的信息物理系统防御方法, 不仅加强信息物理系统的容侵能力, 而且增强防御方法的容侵能力(例如, 针对基于机器学习的入侵检测器中机器学习模型的容侵能力), 实现主动安全控制.

5 总结

随着5G技术的快速发展, 信息物理系统被广泛应用于各个行业. 由于网络攻击手段的不断丰富, 针对信息物理系统的网络攻击事件逐年增加, 并且引起了研究者高度的兴趣. 本文在介绍信息物理系统的组件的建模方式的基础上, 阐述了针对信息物理系统的丰富的攻击类型, 并且综述了常见的网络攻击防御手段及最新研究进展, 最后给出了当前研究存在的问题和未来的挑战. 对于文中给出的当前存在的问题和挑战性问题, 如果部分得到解决, 那么在实际工程中将有重大的意义.

[0]在现存问题与挑战中, 所提出的思想均为本课题组独立提出.

参考文献:

[1] FAN Lingjun, YANG Fei, ZHENG Weicheng, et al. Constructing Internet plus new infrastructure in cities. *Chinese Engineering Science*, 2020, 22(4): 106 – 113.
(范灵俊, 杨菲, 郑卫城, 等. 构建城市“互联网+”新型基础设施发展战略研究. 中国工程科学, 2020, 22(4): 106 – 113.)

[2] GRIFFOR E R, GREER C, WOLLMAN D, et al. *Framework for Cyber-Physical Systems*. Volume 2, Working Group Reports. Gaithersburg, MD: National Institute of Standards and Technology, 2017.

[3] GUAN Xinping, CHEN Cailian, YANG Bo, et al. Towards the integration of sensing, transmission and control for industrial network systems: Challenges and recent developments. *Acta Automatica Sinica*, 2019, 45(1): 25 – 36.
(关新平, 陈彩莲, 杨博, 等. 工业网络系统的感知–传输–控制一体化: 挑战和进展. 自动化学报, 2019, 45(1): 25 – 36.)

[4] TATTIA M, SENOUCI S M, SEDJELMACI H, et al. An efficient intrusion detection system against cyber-physical attacks in the smart grid. *Computers and Electrical Engineering*, 2018, 68: 499 – 512.

[5] CINTUGLU M H, MOHAMMED O A, AKKAYA K, et al. A survey on smart grid cyber-physical system testbeds. *IEEE Communications Surveys and Tutorials*, 2017, 19(1): 446 – 464.

[6] XIE G, ZENG G, LI Z, et al. Adaptive dynamic scheduling on multifunctional mixed-criticality automotive cyber-physical systems. *IEEE Transactions on Vehicular Technology*, 2017, 66(8): 6676 – 6692.

[7] ZHOU Z, WANG B, DONG M, et al. Secure and efficient vehicle-to-grid energy trading in cyber physical systems: Integration of blockchain and edge computing. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2020, 50(1): 43 – 57.

[8] SINHA D, ROY R. Deadline-aware scheduling for maximizing information freshness in industrial cyber-physical system. *IEEE Sensors Journal*, 2021, 21(1): 381 – 393.

[9] FRANCO J, ARIS A, CANBERK B, et al. A survey of honeypots and honeynets for internet of things, industrial internet of things, and cyber-physical systems. *IEEE Communications Surveys and Tutorials*, 2021, 23(4): 2351 – 2383.

[10] TALAT R, OBAIDAT M S, MUZAMMAL M, et al. A decentralised approach to privacy preserving trajectory mining. *Future Generation Computer Systems*, 2020, 102: 382 – 392.

[11] TANG Yi, CHEN Qian, LI Mengya, et al. Overview on cyber-attacks against cyber physical power system. *Automation of Electric Power Systems*, 2016, 40(17): 59 – 69.
(汤奕, 陈倩, 李梦雅, 等. 电力信息物理融合系统环境中的网络攻击研究综述. 电力系统自动化, 2016, 40(17): 59 – 69.)

[12] WANG R X. *Random Process*. Xi'an: Xi'an Jiaotong University Press, 1993.

[13] HAYKIN S, BROCKETT R W. Adaptive filtering theory. *Essays in Control*. New York: Prentice Hall, 1996.

[14] PENG Kunlun, PENG Wei, WANG Dongxia, et al. Research survey on security issues in cyber-physical systems. *Information Network Security*, 2016(7): 20 – 28.
(彭昆仑, 彭伟, 王东霞, 等. 信息物理融合系统安全问题研究综述. 信息网络安全, 2016(7): 20 – 28.)

[15] LIU Ting, TIAN Jue, WANG Jiazhou, et al. Integrated security threats and defense of cyber-physical systems. *Acta Automatica*

Sinica, 2019, 45(1): 7 – 26.
(刘烃, 田决, 王稼舟, 等. 信息物理融合系统综合安全威胁与防御研究. 自动化学报, 2019, 45(1): 7 – 26.)

[16] LI Hongyang, WEI Muheng, HUANG Jie, et al. A survey of cyber-physical systems technology. *Acta Automatica Sinica*, 2019, 45(1): 37 – 50.
(李洪阳, 魏慕恒, 黄洁, 等. 信息物理系统技术综述. 自动化学报, 2019, 45(1): 37 – 50.)

[17] MUHAMMED Z G, RESUL D. Cyber-security on smart grid: Threats and potential solutions. *Computer Networks*, 2020, 169: 107094.

[18] DUO W, ZHOU M, ABUSORRAH A. A survey of cyber attacks on cyber physical systems: Recent advances and challenges. *IEEE/CAA Journal of Automatica Sinica*, 2022, 9(5): 784 – 800.

[19] DING D, HAN Q L, XIANG Y, et al. A survey on security control and attack detection for industrial cyber-physical systems. *Neurocomputing*, 2018, 275: 1674 – 1683.

[20] GUO Nan, JIA Chao. Interpretation of "cyber-physical systems whitepaper (2017)" (Part One). *Information Technology and Standardization*, 2017, (4): 36 – 40.
(郭楠, 贾超.《信息物理系统白皮书(2017)》解读(上). 信息技术与标准化, 2017, (4): 36 – 40.)

[21] NEGI N, CHAKRABORTTY A. Sparsity-promoting optimal control of cyber-physical systems over shared communication networks. *Automatica*, 2020, 122: 109217.

[22] MO L, YOU P, CAO X, et al. Event-driven joint mobile actuators scheduling and control in cyber-physical systems. *IEEE Transactions on Industrial Informatics*, 2019, 15(11): 5877 – 5891.

[23] YANG L, WEN C. Optimal jamming attack system against remote state estimation in wireless network control systems. *IEEE Access*, 2021, 9: 51679 – 51688.

[24] LUO J, HUANG Q, DAI H, et al. Adaptively adjusted ekf-based magnet tracking method for fast-moving object. *IEEE Transactions on Instrumentation and Measurement*, 2023, 72: 7502309.

[25] WEN C, CHENG X, XU D, et al. Filter design based on characteristic functions for one class of multi-dimensional nonlinear non-Gaussian systems. *Automatica*, 2017, 82: 171 – 180.

[26] GE Q, SHAO T, DUAN Z, et al. Performance analysis of the Kalman filter with mismatched noise covariances. *IEEE Access*, 2016, 61(12): 4014 – 4019.

[27] ZHANG Y, WU Z G. Asynchronous control of markov jump systems under aperiodic dos attacks. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 2023, 70(2): 685 – 689.

[28] MUKHERJEE D. Data-driven false data injection attack: A low-rank approach. *IEEE Transactions on Smart Grid*, 2022, 13(3): 2479 – 2482.

[29] YU Y, YANG W, DING W, et al. Reinforcement learning solution for cyber-physical systems security against replay attacks. *IEEE Transactions on Information Forensics and Security*, 2023, 18: 2583 – 2595.

[30] GAO Y, MA J, WANG J, et al. Event-triggered adaptive fixed-time secure control for nonlinear cyber-physical system with false data-injection attacks. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 2023, 70(1): 316 – 320.

[31] SONG W, WANG Z, WANG J, et al. Particle filtering for a class of cyber-physical systems under round-robin protocol subject to randomly occurring deception attacks. *Information Sciences*, 2021, 544: 298 – 307.

[32] YANG Feisheng, WANG Jing, PAN Quan, et al. Elastic event-triggered control of cyber-physical fusion power system under network attack. *Acta Automatica Sinica*, 2019, 45(1): 110 – 119.
(杨飞生, 汪璟, 潘泉, 等. 网络攻击下信息物理融合电力系统的弹性事件触发控制. 自动化学报, 2019, 45(1): 110 – 119.)

[33] SUN Y C, YANG G H. Event-triggered remote state estimation for cyber-physical systems under malicious DoS attacks. *Information Sciences*, 2022, 602: 43 – 56.

[34] LI Xue, LI Wenting, DU Dajun, et al. Research on dynamic state estimation of smart grid based on UKF under denial of service attack. *Acta Automatica Sinica*, 2019, 45(1): 120 – 131.
(李雪, 李雯婷, 杜大军, 等. 拒绝服务攻击下基于UKF的智能电网动态状态估计研究. 自动化学报, 2019, 45(1): 120 – 131.)

[35] LIU Y, YANG G H. Event-triggered distributed state estimation for cyber-physical systems under dos attacks. *IEEE Transactions on Cybernetics*, 2022, 52(5): 3620 – 3631.

[36] YAN J J, YANG G H. Adaptive fault estimation for cyber-physical systems with intermittent DoS attacks. *Information Sciences*, 2021, 547: 746 – 762.

[37] ZHANG M, SHEN C, HAN S. A compensation control scheme against dos attack for nonlinear cyber-physical systems. *The 38th Chinese Control Conference (CCC)*. Guangzhou, China: IEEE, 2019: 144 – 149.

[38] LÜ S Y, JIN X Z. Robust adaptive control for a class of disturbed cyber-physical systems with denial of service. *The 39th Chinese Control Conference (CCC)*. Shenyang, China: IEEE, 2020: 4313 – 4317.

[39] LIU S, XU B, LI S, et al. Resilient control strategy of cyber-physical system under DoS attacks. *The 36th Chinese Control Conference (CCC)*. Dalian, China: IEEE, 2017: 7760 – 7765.

[40] DENG C, WEN C. Mas-based distributed resilient control for a class of cyber-physical systems with communication delays under dos attacks. *IEEE Transactions on Cybernetics*, 2021, 51(5): 2347 – 2358.

[41] YUAN H, XIA Y. Resilient strategy design for cyber-physical system under DoS attack over a multi-channel framework. *Information Sciences*, 2018, 454: 312 – 327.

[42] SUN Y C, YANG G H. Periodic event-triggered resilient control for cyber-physical systems under denial-of-service attacks. *Journal of the Franklin Institute*, 2018, 355(13): 5613 – 5631.

[43] ZHAO L, LI W, LI Y. Research on dual security control for a nonlinear CPS with multi-objective constraints under DoS attack and actuator fault: An active-passive attack-tolerant approach. *Journal of Control Science and Engineering*, 2022, DOI: 10.1155/2022/1734593.

[44] SARGOLZAEI A. A secure control design for networked control system with nonlinear dynamics under false-data-injection attacks. *American Control Conference (ACC)*. New Orleans, Louisiana, USA: IEEE, 2021: 2693 – 2699.

[45] MANANDHAR K, CAO X, HU F, et al. Detection of faults and attacks including false data injection attack in smart grid using Kalman filter. *IEEE Transactions on Control of Network Systems*, 2014, 1(4): 370 – 379.

[46] WANG Caiyun. *Fraud attack analysis and security defense strategy of cyber-physical system*. Shanghai: East China University of Science and Technology, 2021.
(王彩云. 信息物理系统的欺诈攻击分析及安全防御策略. 上海: 华东理工大学, 2021.)

[47] WANG P, REN X, HU S, et al. Event-based adaptive compensation control of nonlinear cyber-physical systems under actuator failure and false data injection attack. *The 40th Chinese Control Conference (CCC)*. Shanghai: IEEE, 2021: 509 – 514.

[48] XUE Y, REN W, ZHENG B C, et al. Event-triggered adaptive sliding mode control of cyber-physical systems under false data injection attack. *Applied Mathematics and Computation*, 2022, 433: 127403.

[49] YANG W, LEI L, YANG C. Event-based distributed state estimation under deception attack. *Neurocomputing*, 2017, 270: 145 – 151.

[50] HU L, WANG Z, HAN Q L, et al. State estimation under false data injection attacks: Security analysis and system protection. *Automatica*, 2018, 87: 176 – 183.

[51] ZOU T, BRETAS A S, RUBEN C, et al. Smart grids cyber-physical security: Parameter correction model against unbalanced false data injection attacks. *Electric Power Systems Research*, 2020, 187: 106490.

[52] ZHAO Y, CHEN Z, ZHOU C, et al. Passivity-based robust control against quantified false data injection attacks in cyber-physical systems. *IEEE/CAA Journal of Automatica Sinica*, 2021, 8(8): 1440 – 1450.

[53] YE D, ZHANG T Y, GUO G. Stochastic coding detection scheme in cyber-physical systems against replay attack. *Information Sciences*, 2019, 481: 432 – 444.

[54] XIE G, YANG K, XU C, et al. Digital twinning based adaptive development environment for automotive cyber-physical systems. *IEEE Transactions on Industrial Informatics*, 2021, 18(2): 1387 – 1396.

[55] HUANG J, HO D W C, LI F, et al. Secure remote state estimation against linear man-in-the-middle attacks using watermarking. *Automatica*, 2020, 121: 109182.

[56] FANG C, QI Y, CHENG P, et al. Optimal periodic watermarking schedule for replay attack detection in cyber-physical systems. *Automatica*, 2020, 112: 108698.

[57] HUANG J, ZHAO L, WANG Q G. Adaptive control of a class of strict feedback nonlinear systems under replay attacks. *ISA Transactions*, 2020, 107: 134 – 142.

[58] HOSSEINZADEH M, SINOPOLI B, GARONE E. Feasibility and detection of replay attack in networked constrained cyber-physical systems. *The 57th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*. Monticello, IL, USA: IEEE, 2019: 712 – 717.

[59] TANG H, LIU X, JIANG L. A robust and efficient timestamp-based remote user authentication scheme with smart card lost attack resistance. *International Journal of Network Security*, 2013, 15(6): 446 – 454.

[60] GUO H, PANG Z H, SUN J, et al. An output-coding-based detection scheme against replay attacks in cyber-physical systems. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 2021, 68(10): 3306 – 3310.

[61] TRAPIELLO C, ROTONDO D, SANCHEZ H, et al. Detection of replay attacks in CPSs using observer-based signature compensation. *The 6th International Conference on Control, Decision and Information Technologies (CoDIT)*. Paris, France: IEEE, 2019: 1 – 6.

[62] MA L, CHU Z, YANG C, et al. Recursive watermarking-based transient covert attack detection for the industrial cps. *IEEE Transactions on Information Forensics and Security*, 2023, 18: 1709 – 1719.

[63] FARHA F, NING H. Enhanced timestamp scheme for mitigating replay attacks in secure zigbee networks. *International Conference on Smart Internet of Things (SmartIoT)*. Tianjin: IEEE, 2019: 469 – 473.

[64] NAGARAJAN S M, DEVERAJAN G G, BASHIR A K, et al. IADF-CPS: Intelligent anomaly detection framework towards cyber physical systems. *Computer Communications*, 2022, 188: 81 – 89.

[65] XI L, WANG R, HAAS Z J. Data-correlation-aware unsupervised deep-learning model for anomaly detection in cyber-physical systems. *IEEE Internet of Things Journal*, 2022, 9(22): 22410 – 22421.

[66] ZHANG F, KODITUWAKKU H A D E, HINES J W, et al. Multilayer data-driven cyber-attack detection system for industrial control systems based on network, system, and process data. *IEEE Transactions on Industrial Informatics*, 2019, 15(7): 4362 – 4369.

[67] ZHANG Z, CHENG P, WU J, et al. Secure state estimation using hybrid homomorphic encryption scheme. *IEEE Transactions on Control Systems Technology*, 2020, 29(4): 1704 – 1720.

[68] XUE W, LUO C, SHEN Y, et al. Towards a compressive-sensing-based lightweight encryption scheme for the internet of things. *IEEE Transactions on Mobile Computing*, 2020, 20(10): 3049 – 3065.

[69] HONG Z, YANG C, YU L. *R*-Print: A system residuals-based fingerprinting for attack detection in industrial cyber-physical systems. *IEEE Transactions on Industrial Electronics*, 2020, 68(11): 11458 – 11469.

[70] ADIL M, KHAN M K, JADOON M M, et al. An ai-enabled hybrid lightweight authentication scheme for intelligent iomt based cyber-physical systems. *IEEE Transactions on Network Science and Engineering*, 2022, 10(5): 2719 – 2730.

[71] YANG L, WEN C, WEN T. Multilevel fine fingerprint authentication method for key operating equipment identification in cyber-physical systems. *IEEE Transactions on Industrial Informatics*, 2023, 19(2): 1217 – 1226.

[72] SUN Y E, HUANG H, YANG W, et al. Toward differential privacy for traffic measurement in vehicular cyber-physical systems. *IEEE Transactions on Industrial Informatics*, 2021, 18(6): 4078 – 4087.

[73] JIANG Y, WU S, ZHAO X, et al. A lightweight defense scheme for industrial data transmission against eavesdropping attacks and integrity attacks. *The 4th IEEE International Conference on Industrial Cyber-Physical Systems (ICPS)*. Victoria, BC, Canada: IEEE, 2021: 461 – 466.

[74] WU S, JIANG Y, LUO H, et al. Deep learning-based defense and detection scheme against eavesdropping and typical cyber-physical attacks. *CAA Symposium on Fault Detection, Supervision, and Safety for Technical Processes (SAFEPROCESS)*. Chengdu: IEEE, 2021: 1 – 6.

[75] CHEN G, SUN L, ZHANG Y. A stealthy artificial noise strategy against eavesdropping for remote estimation sensor networks. *Journal of the Franklin Institute*, 2022, 359(18): 10726 – 10740.

[76] YANG W, LI D, ZHANG H, et al. An encoding mechanism for secrecy of remote state estimation. *Automatica*, 2020, 120: 109116.

[77] TSIAMIS A, GATSIS K, PAPPAS G J. State-secrecy codes for networked linear systems. *IEEE Transactions on Automatic Control*, 2019, 65(5): 2001 – 2015.

[78] SINGH M, AUJLA G S, BALI R S. A deep learning-based blockchain mechanism for secure internet of drones environment. *IEEE Transactions on Intelligent Transportation Systems*, 2020, 22(7): 4404 – 4413.

[79] JIANG B, LI J, YUE G, et al. Differential privacy for industrial internet of things: Opportunities, applications, and challenges. *IEEE Internet of Things Journal*, 2021, 8(13): 10430 – 10451.

[80] CANONNE C L, KAMATH G, STEINKE T. The discrete gaussian for differential privacy. *Advances in Neural Information Processing Systems*, 2020, 33: 15676 – 15688.

[81] MORIAI S. Privacy-preserving deep learning via additively homomorphic encryption. *The 26th Symposium on Computer Arithmetic (ARITH)*. Kyoto, Japan: IEEE, 2019: 198.

[82] YANG L, WEI X K, WEN C L. A security defense method against eavesdroppers in the communication-based train control system. *Chinese Journal of Electronics*, 2023, 32(5): 992 – 1001.

[83] HAY M, SAEED B, LUNG C H, et al. Co-located physical-layer network coding to mitigate passive eavesdropping. *The 8th International Conference on Privacy, Security and Trust*. Auckland, New Zealand: IEEE, 2010: 1 – 2.

[84] YANG Z, YANG K, LEI L, et al. Blockchain-based decentralized trust management in vehicular networks. *IEEE Internet of Things Journal*, 2018, 6(2): 1495 – 1505.

[85] LU Y, HUANG X, DAI Y, et al. Blockchain and federated learning for privacy-preserved data sharing in industrial IoT. *IEEE Transactions on Industrial Informatics*, 2019, 16(6): 4177 – 4186.

[86] LEE J, AZAMFAR M, SINGH J. A blockchain enabled cyber-physical system architecture for industry 4.0 manufacturing systems. *Manufacturing Letters*, 2019, 20: 34 – 39.

[87] WANG S, OUYANG L, YUAN Y, et al. Blockchain-enabled smart contracts: Architecture, applications, and future trends. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2019, 49(11): 2266 – 2277.

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

[89] RING M, WUNDERLICH S, SCHEURING D, et al. A survey of network-based intrusion detection data sets. *Computers Security*, 2019, 86: 147 – 167.

[90] WANG L, CAO X, SUN B, et al. Optimal schedule of secure transmissions for remote state estimation against eavesdropping. *IEEE Transactions on Industrial Informatics*, 2020, 17(3): 1987 – 1997.

[91] PENG L, CAO X, SUN C, et al. Energy efficient jamming attack schedule against remote state estimation in wireless cyber-physical systems. *Neurocomputing*, 2018, 272: 571 – 583.

[92] SUN X, WEN T, WEN C, et al. High order extended strong tracking filter. *Chinese Journal of Electronics*, 2021, 30(6): 1152 – 1158.

[93] WENG X, XU X, FENG J, et al. A correlation analysis-based multivariate alarm method with maximum likelihood evidential reasoning. *IEEE Transactions on Automation Science and Engineering*, 2023, DOI: 10.1109/TASE.2023.3305524.

[94] ZHOU Z, WEN C L, YANG C J. Fault isolation based on k-nearest neighbour rule for industrial processes. *IEEE Transactions on Industrial Electronics*, 2016, 63(4): 2578 – 2586.

[95] BAO Zhongxin, WEN Chenglin, MA Xue. Data preprocessing and pca fault diagnosis method based on rate of change transformation. *Acta Electronica Sinica*, 2021, 49(11): 2234 – 2240.
(鲍中新, 文成林, 马雪. 一种基于数据变化率的预处理及主元分析故障诊断方法. 电子学报, 2021, 49(11): 2234 – 2240.)

[96] MA X, WEN C, WEN T. An asynchronous and real-time update paradigm of federated learning for fault diagnosis. *IEEE Transactions on Industrial Informatics*, 2021, 17(12): 8531 – 8540.

[97] SUN X, WEN C, WEN T. Maximum correntropy high order extended Kalman filter. *Chinese Journal of Electronics*, 2022, 31(1): 190 – 198.

[98] ZHOU F, YANG S, FUJITA H, et al. Deep learning fault diagnosis method based on global optimization GAN for unbalanced data. *Knowledge-Based Systems*, 2020, 187: 104837.

[99] WU Jiangxing. Research on mimic defense in cyberspace. *Journal of Information Security*, 2016, 1(4): 1 – 10.
(邬江兴. 网络空间拟态防御研究. 信息安全学报, 2016, 1(4): 1 – 10.)

作者简介:

文成林 教授, 目前研究方向为故障诊断与主动安全控制、隐写检测与定位、多目标跟踪、信息融合等, E-mail: wencl@hdu.edu.cn;

杨 力 讲师, 目前研究方向为复杂工业系统的网络攻击、信息物理系统的网络安全等, E-mail: yangli@zjhu.edu.cn.