计算机科学
COMPUTER SCIENCE

信息物理系统的传感器攻击抵御策略综述

陈彦峰, 冯智伟, 邓庆绪, 王妍

引用本文

陈彦峰, 冯智伟, 邓庆绪, 王妍. 信息物理系统的传感器攻击抵御策略综述[J]. 计算机科学, 2025, 52(4): 4-13.

CHEN Yanfeng, FENG Zhiwei, DENG Qingxu, WANG Yan. Survey of Sensor Attack Defense Strategies for Cyber Physical Systems [J]. Computer Science, 2025, 52(4): 4-13.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.241000138

信息物理系统的传感器攻击抵御策略综述

陈彦峰[1]　冯智伟[2]　邓庆绪[2]　王　妍[1]
1 辽宁大学网络与信息安全学院　沈阳 110036
2 东北大学计算机科学与工程学院　沈阳 110167
(yfchen@lnu.edu.cn)

摘　要　信息物理系统(Cyber Physical System,CPS)作为融合了计算、通信和控制的智能系统,在诸多领域,如智能交通、智能健康等方面发挥着越来越重要的作用。传感器在CPS中扮演着重要角色,但也常成为攻击者的目标。首先,明确了传感器攻击抵御的研究范围,按照攻击发生时间点,将传感器攻击的相关研究分为了攻击防御、攻击抵御和攻击恢复。然后,回顾了常见传感器攻击的类型和影响,包括拒绝服务攻击、重放攻击、欺骗攻击等。接着,总结了基于多源一致性、历史一致性和响应一致性的传感器攻击检测方法。随后,论述了攻击检测后的数据融合方法,包括基于卡尔曼滤波和基于间隔的数据融合方法。最后,探讨了未来可能的研究方向,以进一步加强CPS中传感器攻击的防御能力。

关键词:信息物理系统;传感器攻击;攻击抵御;攻击检测;数据融合;数据安全
中图分类号　TP399

Survey of Sensor Attack Defense Strategies for Cyber Physical Systems

CHEN Yanfeng[1],FENG Zhiwei[2],DENG Qingxu[2] and WANG Yan[1]
1 School of Cyber Science and Engineering,Liaoning University,Shenyang 110036,China
2 College of Computer Science and Engineering,Northeastern University,Shenyang 110167,China

Abstract　Cyber-physical system(CPS),as an intelligent system integrating computation,communication and control,plays an increasingly important role in various fields such as intelligent transportation and healthcare. Sensors play a crucial role in CPS but are also commonly targeted by attackers. Firstly,the scope of research on sensor attack defense is clarified,and the relevant studies on sensor attacks are categorized into attack prevention,defense and recovery according to the timing of attack occurrence. Next,the types and impacts of sensor attacks are reviewed,including DoS attacks,replay attacks and deception attacks. Then,sensor attack detection methods based on multi-source consistency,historical consistency and response consistency are summarized. Subsequently,data fusion methods after attack detection are discussed,including Kalman filter-based and interval-based data fusion methods. Finally,potential future research directions are explored to further enhance the defense capabilities against sensor attacks in CPS.

Keywords　Cyber physical system,Sensor attack,Attack defense,Attack detection,Data fusion,Data security

1　引言

信息物理系统(CPS)融合了计算、网络、控制,实现了物理世界与信息世界的感知、控制与服务,广泛应用于军事、工业、生活等领域。为实现物理世界与信息世界的交互,大量传感器被部署用于测量相关物理状态。传感器测量值是CPS感知物理状态的基础数据,经过网络传输到控制器,再由特定算法实现各种功能。准确测量,是CPS做出正确决策与控制的关键。控制器一旦接收到错误的传感器数据,就可能做出错误决策,威胁到安全。恶意传感器攻击可能直接篡改控制器接收的数据,导致系统性能下降,甚至威胁到生命财产安全。例如,若电力设施、军事无人机、自动驾驶汽车等典型CPS受到传感器攻击,将造成灾难性后果。CPS中信息安全、网络安全、功能安全和人的安全是深度交织和偶合的,这四者共同保障着系统的整体安全性。在这个系统中,信息安全和网络安全相互作用,信息安全主要保护传感器数据和控制指令的完整性与保密性,而网络安全则防止数据传输过程中被篡改或遭受拒绝服务等攻击。例如,在智能驾驶汽车场景中,网络攻击可能通过车载网络入侵,篡改传感器数据,导致系统错误决策,进而威胁到功能安全和人的安全。功能安全在此扮演着关键角色,确保系统即使在传感器或控制模块发生故障的情况下仍能安全运行,而人的安全则关乎驾驶员与乘客的生命安全。在实际场景中,如高速公路驾驶或复杂城市环境下的自动驾驶,传感器的数据采集与融合直接依赖于这些

到稿日期:2024-10-28　返修日期:2025-02-14
基金项目:辽宁省科技计划联合计划(自然科学基金-博士科研启动项目)(2024-BSLH-108)
This work was supported by the Liaoning Province Science and Technology Plan Joint Plan(2024-BSLH-108).
通信作者:王妍(wang_yan@lnu.edu.cn)

安全保障机制的协同工作。若发生传感器欺骗或数据丢失，系统的决策可能受到影响，进而威胁到驾驶员的安全。因此，智能驾驶系统必须在多层次的安全防护中考虑这 4 个安全维度的深度交织，确保各个层面的安全机制能够在实际应用中共同发挥作用，从而全面保障系统的安全。因此，准确的传感器测量对于 CPS 的正常运行至关重要，而传感器攻击则直接威胁到测量的准确性。传感器攻击抵御策略通过多传感器冗余测量同一物理状态，并结合先进的攻击检测算法，有效识别和处理受到攻击的传感器数据，从而精确估测系统的真实状态，确保系统的稳健性和安全性。本文对传感器攻击抵御策略进行了系统综述，旨在为学术界指明清晰的研究方向，为进一步推动该领域的创新与应用奠定基础，并为实际场景中的智能系统提供有价值的思路和方案。

2 CPS 传感器攻击概述

典型 CPS 包含物理层的物理系统和信息层的传感器、通信网络、控制器、执行器。传感器数据通过传感器设备对物理系统的测量生成，再经由通信网络传输到控制器，其数据链路经过物理系统、传感器设备和通信网络，如图 1 所示。在此过程中发生的所有 CPS 攻击都可能造成控制器接收到的传感器数据被篡改，从而生成错误的控制指令[1-2]。本文中所指的传感器攻击包含所有可以影响传感器数据的攻击。目前其他综述文章[3-7]侧重于对具体的攻击实现方式进行划分和论述，然而系统的安全隐患存在于各个地方，攻击方式多种多样，很难全面地对所有具体攻击方式进行概括；同时，这些综述文章也没有从攻击发生的时间轴角度进行划分。

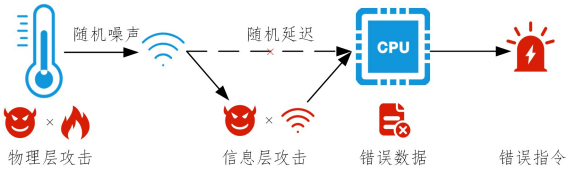

图 1 CPS 传感器攻击示意图

Fig. 1 Schematic diagram of CPS sensor attack

本文按照攻击发生的位置，将 CPS 传感器攻击分为以下几类。

1）物理层攻击。以声、光、热和电力等物理方式直接改变现实世界中的物理量，干扰、篡改传感器生成的测量值[3]。此类攻击无法在信息层面通过算法进行防御[4-5]。

2）信息层攻击。通过代码植入等方式影响传感器的工作过程，篡改生成的传感器数据[6-7]；或者在网络通信过程中拦截原始传感器数据，伪造身份发送篡改数据到控制器。此类攻击可以在信息层面通过代码防御[8]、信息加密[9]、身份认证[10]等技术进行防御，但是会在一定程度上增加 CPS 的计算负担。

传感器所处的物理环境、设备硬件、软件、网络上都可能发生不同种类的攻击，它们都可以划分到信息物理系统中的物理层或者信息层。比如，设备硬件本身可能发生代码植入、篡改等攻击，最终结果是导致信息层的数据被窃取、篡改。传感网络中发生被破解通信密钥、侧信道等攻击，同样会导致信息层数据受影响。以上两类都属于本文所定义的信息层攻击。而攻击者可以直接对物理世界产生影响，比如在智能驾驶汽车这个场景中，攻击者直接产生设计好的同频率的超声波信号，让超声波传感器对前方障碍物产生误判。这类攻击则属于本文所定义的物理层攻击。

按照传感器攻击发生的时间顺序，将相关的技术划分为防御、抵御和恢复，如图 2 所示。防御技术旨在攻击发生前，通过加密算法、身份认证等措施预防攻击事件的发生[11-12]；抵御技术是在传感器攻击发生后，检测攻击数据，降低其损害，并通过冗余传感器数据确保系统正常运行[13]；恢复技术是在系统受传感器攻击崩溃后，通过读取日志、备份回滚等方式使系统恢复到正常状态[14-15]。除介绍本文所做的攻击抵御相关研究外，对攻击防御和攻击恢复相关技术做如下简要介绍。

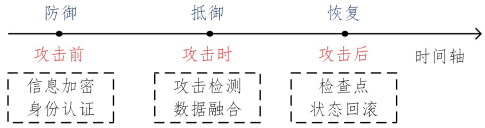

图 2 传感器攻击相关技术的时间轴分布

Fig. 2 Time distribution of sensor attack-related technologies

1）攻击防御。在攻击防御阶段，有传统的信息安全技术防止攻击者监听、窃取或篡改数据，如身份验证和访问控制机制[16]、网络入侵检测系统[17]、补丁管理和安全认证[18]。例如，在信息加密方向，Sodhroa 等提出了一种线性加密方案，以减小潜在隐蔽攻击的影响。针对任意线性加密，推导出产生最大估计误差的最坏线性攻击。基于斯塔克伯格博弈分析设计了最优线性加密，以减小最坏情况下的估计误差[19]。在身份认证和访问控制方向，针对车-车中确保安全消息实时性传输的问题，Bai 等提出 MC-Safe 多通道通信框架，监视所有可用通道，并动态选择最佳通道进行安全消息传输，允许所有潜在事故涉及的车辆以分布式的方式合作，以确定满足延迟要求的通信通道[20]。Shang 团队介绍了多种 5G 智慧医疗系统中的身份认证方案，利用训练的 AI 模型对用户进行认证并允许访问资源，其决策可以输入到专家系统中[21]。然而，上述攻击防御技术均不能完全保证系统安全，所有防御技术中始终存在一些技术或者机制漏洞让攻击者有机会对系统成功实施攻击[22-23]。

2）攻击恢复。攻击恢复旨在攻击防御和攻击抵御技术均失效后，通过状态回滚、数据恢复的方式使 CPS 恢复到正常工作状态。Lian 等提出了一种基于形式化的传感器攻击恢复方法，通过在线计算一个恢复控制序列，将正在受到传感器攻击的系统从当前状态引导到目标状态，以确保在此过程中不会到达任何不安全状态。为缩短其计算时间，首先基于线性规划限制给定到达-避免问题的安全和目标规范，然后使用线性规划求解器找到解决方案[15]。该学者还提出了一种适用于非线性系统的数据预测恢复方法，利用未受损的传感器来减轻不确定性积累，用于保护 CPS 免受传感器攻击。恢复系统保证 CPS 不会遇到不安全状态，并能在保守的截止期限内平稳恢复到目标集，保证 CPS 将在指定时间内保持在目标集内[16]。

3 常见 CPS 传感器攻击

3.1 物理层攻击

1）基于物理信号的干扰攻击

传感器的物理层攻击通过对传感器接收的物理信号进行

干扰，扰乱其正常测量功能。常见的攻击对象包括超声波、雷达、激光雷达等。这些传感器依赖于声波、光波、激光等物理量来感知环境或检测物体。以雷达为例，雷达传感器通过发射电磁波并接收反射信号来测量物体的距离和速度，通常用于自动驾驶中的碰撞预警。攻击者可以利用频率相近的电磁波对雷达信号进行干扰，使雷达无法准确探测物体，甚至引发误判，影响系统的判断[3]。类似地，激光雷达(LiDAR)也对外部光源尤其是强光极为敏感，攻击者可以通过强激光干扰激光雷达的探测功能，导致测量失真或出现盲区，从而影响自动驾驶系统的环境感知能力。此外，超声波传感器被广泛应用于车辆倒车辅助系统，攻击者可以通过向超声波信号路径中引入噪音或反射物来破坏正常测距，导致系统无法正确识别障碍物位置，增加碰撞风险[4]。

2)基于物理信号的欺骗攻击

物理信号欺骗攻击利用传感器对声、光、热、电等物理量的敏感性，设计并实施干扰手段，干扰传感器的正常工作。常见的攻击对象包括超声波、雷达、激光雷达等传感器。超声波传感器通常通过主动发射脉冲探测周围障碍物，在低速行驶时用于停车辅助，在高速行驶时用于盲区监测。攻击者可以通过发射与车辆传感器相同频率的超声波，欺骗传感器误判障碍物位置，从而影响安全决策。文献[5]提到，针对 Tesla Model S 汽车的超声波传感器攻击中，攻击者通过精确设计的超声波发射装置，制造与车辆传感器相同频率的信号，导致对障碍物的错误判断。类似地，攻击者也可能通过改变交通标志的外观(如贴上反光贴纸、海报或涂画)来误导传感器，尤其是相机系统会受到影响[6-8]，但对激光雷达的影响较小。相反，激光雷达系统则可能受到激光射击的欺骗，攻击者通过激光发射器干扰激光雷达的测距功能，从而使自动驾驶系统无法准确识别环境物体。

3.2 信息层攻击

1)面向网络的拒绝服务攻击

DoS 攻击(或干扰攻击)是攻击者经常使用的策略，其通过占用网络资源阻止测量或控制信号的传输，从而尽可能地降低系统性能。在数据特征上，DoS 攻击下的传感器数据在该时间段内的数值为空。实际上，DoS 攻击的数据特征使其容易被时间戳对比、数据更新检测等方法检测出来。一般来说，对 DoS 攻击研究的重点不在检测而是防御[17]。现有研究对各种场景下可能的 DoS 攻击进行了设计和防御。Lian 等通过破坏互联电力系统中单个控制中心的通信基础设施，设计了一种针对分布式状态估计的 DoS 攻击[22]。这种攻击可以使每个地区的系统操作员变得盲目。Zhang 等通过在每个采样时间点决定攻击者是否干扰通信信道，来干扰通过无线信道进行状态估计的远程估计器[23]。Aghili 等提出了一种针对干扰攻击的最优防御机制，以攻击者和传感器的发射器之间的随机博弈理论为基础，将二次状态估计误差作为成本函数中的一项进行考虑[8]。

2)面向网络的重放攻击

实际上，重放攻击对于不了解系统动态的攻击者来说是容易实现的攻击方式。通过记录来自受损传感器和执行器的读数并在一段时间后进行重复，攻击者可以注入外部控制输入而不被检测，从而干扰系统的性能。此类攻击可以绕过一般的身份认证或数据加密等机制，避免被检测。关于此类攻击的相关研究主要为在不同应用场景下进行攻击的设计和检测。Tahoun 等提出了在重放攻击下的递减视界控制的变体，该变体导出了无限视界成本、计算和攻击视界之间的简单而明确的关系，并提供了一组充分条件，以确保系统的渐近指数稳定性[24]。Zaman 等针对离散时间线性定常高斯系统，设计了在重放攻击下的无限视界线性二次高斯控制器，同时根据已获得的关于重放攻击可行性的条件，提出了一种在折衷控制精度下降和控制努力增加之间以保证期望检测概率的对策[25]。

3)面向网络的欺骗攻击

欺骗攻击(或虚假数据注入攻击)是更一般的攻击行为，被认为是对 CPS 最危险的网络攻击，因为攻击者可以注入恶意数据以降低甚至恶化系统的性能。基于单个传感器的传统错误数据检测对于这种攻击策略没有检测效果，需要引入冗余传感器数据进行攻击检测[26-28]。在此类攻击研究领域，众多学者对不同条件下的欺骗攻击进行了设计和检测。Khare 等首次构建了一种攻击向量，这些攻击向量可以通过使用现有的虚警算法更敏感地改变状态估计性能而不被检测到[26]。Gheitasi 等针对能够观察所有仪表和网络数据的攻击者，获得了一个不可检测攻击存在的充分必要条件，并且还考虑了防止这些不可检测攻击的对策[28]。有关电力系统在欺骗攻击下的过滤或状态估计问题引起了广泛的研究。传统的状态估计方法一直被假定能够容忍和检测随机的错误测量值。然而，最近的研究显示这些方法容易受到故意的虚假数据注入攻击的影响[28]。Jorjani 等提出了一种用图形方法进行电力系统状态估计的虚假数据注入攻击的防御机制，该方法通过保护所选仪表测量值，可以防止虚假数据注入攻击造成的状态估计的准确性降低[29-30]。Aoufi 等构建了一种新型的虚假数据注入攻击，称为可容忍的虚假数据注入。该攻击可以规避传统的错误数据检测[31]。为了抵御这种攻击，Sengan 等提出了一种基于扩展分布式状态估计的方法和数据框架攻击，然后将理想状态估计器的设计问题定义为约束二次规划问题[32]。对于电网中不可观测的稀疏数据注入攻击，Shinoharat 等提出了在性能和虚警之间的灵活权衡的设计，攻击者可以访问所有网络信息并添加恶意节点[33]。此外，集中式情况已经扩展到分布式框架，用于状态估计和攻击问题。值得一提的是，到目前为止，关于 CPS 在欺骗攻击下的控制结果还很少见。Fawzi 等在一些传感器或执行器受到攻击时，对线性系统的状态估计和控制问题进行了处理[34]。

3.3 对比分析

在传感器网络中，拒绝服务攻击、重放攻击和欺骗攻击是 3 种主要的攻击形式，各具独特特征与潜在影响。拒绝服务攻击旨在通过过载网络和耗尽资源，使系统无法处理合法请求，从而直接影响可用性，导致经济损失和用户信任度下降。防御此类攻击需实施流量监控、负载均衡和冗余设计，以提高系统的弹性和可用性。重放攻击则通过截获并重新发送合法消息来误导系统执行错误操作，可能导致重复交易和数据不一致。为此，可在消息中添加时间戳和序列号，并使用一次性令牌，增强对重复消息的检测能力。欺骗攻击通过伪装成合法用户或设备，获取未授权访问权限，导致敏感信息泄露和数据篡改。有效的身份验证机制和严格的访问控制策略是防止

此类攻击的关键。综上所述，保护传感器网络需要综合多层次的防御机制，包括实时监控与响应、身份验证与访问控制，以及系统冗余与弹性设计，以应对这些攻击，确保网络安全。3 种典型攻击类型的对比结果如表 1 所列。

表 1 典型攻击类型对比

Table 1 Comparison of typical attack types

位置	攻击类别	定义	目的	影响	防御措施
物理层	干扰攻击	外部信号干扰传感器信号接收	破坏传感器测量功能	传感器无法准确感知环境	提升抗干扰能力，多传感器融合
	欺骗攻击	模拟或篡改传感器信号	误导传感器判断环境	错误判断障碍物位置和距离	引入信号验证，多传感器一致性检查
信息层	拒绝服务攻击	使系统无法处理合法请求	阻止合法用户访问服务	服务中断、经济损失、用户信任下降	流量监控、负载均衡、冗余设计
	重放攻击	截获并重发合法消息	误导系统执行重复操作	重复数据、状态不一致	时间戳、序列号、一次性令牌
	欺骗攻击	伪装成合法用户或设备	获取未授权访问权限	敏感信息泄露、系统滥用、数据篡改	身份验证机制、数字签名、访问控制

4 传感器攻击抵御的两个阶段

在传感器网络的安全性研究中，传感器攻击抵御策略通常分为两个关键阶段：传感器攻击检测和传感器数据融合。首先，传感器攻击检测阶段的主要任务是识别和定位潜在的攻击行为。通过应用多种检测算法和策略，这一阶段能够实时监控传感器数据，分析其一致性和可靠性，从而及时发现异常模式。这些检测方法包括基于多源一致性、历史一致性和响应一致性的技术，旨在提供对不同攻击类型（如拒绝服务攻击、重放攻击和欺骗攻击）的防护。

在成功检测到攻击后，接下来的传感器数据融合阶段则聚焦于处理和整合来自多个传感器的数据，以生成更准确和可靠的信息。这一阶段的关键在于通过数据融合算法，综合各个传感器的测量结果，以减轻单一传感器数据异常对整体系统性能的影响。采用如卡尔曼滤波、加权平均或多传感器融合技术，可以有效提高数据的鲁棒性和抗攻击能力。

综上所述，这两个阶段相辅相成，形成了一套完整的传感器攻击抵御策略体系。在检测阶段确保及时发现攻击，融合阶段则通过优化数据输出增强系统的稳定性和可靠性，从而提升整个传感器网络的安全性和应对能力。

5 传感器攻击检测

传感器攻击检测是传感器攻击抵御技术的首要环节，是实现物理状态高精度估测的基础。目前的攻击检测算法均通过冗余数据间的一致性实现，一致性按照不同维度可分为多源一致性[35-37]、历史一致性[38]和响应一致性[39]。

5.1 定义和介绍

假设物理状态真实值为 θ，第 $i(i\in[1,N])$ 个传感器在 k 时刻的测量值为 z_k^i，第 i 个传感器的最大误差为 ε^i。3 个一致性的定义如下。

定义 1（多源一致性） 来自不同传感器或数据源的测量结果在相同时间点或相同事件下应当保持一致或相近的状态 $|z_k^i-\theta|<\varepsilon^i, i\in[1,N]$，即每个传感器的测量误差均小于其最大误差。这种一致性确保了不同数据源所提供的信息能够相互验证，从而提升数据的可靠性。

定义 2（历史一致性） 当前传感器数据与其历史数据之间的一致性 $|z_k^i-\theta|<\varepsilon^i, k\in[j,j+1,\cdots]$，即每个传感器不同时刻的测量误差均小于其最大误差。在特定时间段内，传感器的输出应该与过去的输出保持合理的相关性和趋势。

定义 3（响应一致性） 在接收到请求或触发事件后，传感器或系统的反应应当是一致的，$\{z_k^i, z_{k+1}^i, \cdots\}(i\in[1,N])$ 具有相同的变化趋势，即相同条件下的相同输入应产生相似趋势的输出。

3 种方法与不同攻击类型的关系如下：基于多源一致性的抵御策略，通过利用多源数据进行投票和加权融合，能够有效应对拒绝服务攻击，确保在少于一半的传感器被攻击时仍能提供准确的测量结果。此外，该策略还可通过历史数据对比，识别和排除重放攻击。基于历史一致性的策略则采用时间窗累积检测算法，监测传感器数据的历史趋势，从而及时识别逐渐变化的攻击模式，如虚假数据注入，保障系统在攻击发生时的安全运行区域不被突破。响应一致性的检测策略通过主动激励和动态水印算法，实时监控系统对特定激励的响应，帮助快速识别重放攻击或其他伪装攻击。这些多层次的抵御策略在面对各种攻击时相辅相成，使得传感器网络更加安全可靠。综上所述，本章详细分析了攻击方法与抵御策略之间的关联，强调了综合应用不同策略的重要性，为传感器网络的整体安全性和可靠性提供了有力保障。表 2 按照 3 种一致性对攻击检测方法进行分类，下文将分别进行详细论述。

5.2 基于多源一致性的攻击检测

以 Marzullo 为代表的学者对传感器数据进行最差情况分析，构造出表示所有测量值可能范围的传感器间隔（Interval[38]），通过多数投票法的方式确定最终融合值并检测可能受攻击的传感器数据，属于被动方式的攻击检测[35-38]。该方法不受限于特定的噪声概率分布特征，在获取了传感器测量噪声和网络延迟的限定范围后，即可获得最终融合值的限定范围，能够直接应用于攻击造成数据异常的情况。只要异常数据少于所有传感器数据的一半，该方法就能正常工作。在传感器间隔算法基础上，Lu 等构造了虚拟传感器，并引入到传感器融合中，增强了数据间的物理约束，获得了更好的抗攻击性[40]。Park 等提出了传感器的瞬态攻击和永久攻击模型。首先，在给定每个传感器的瞬态故障模型的情况下，分析传感器融合随时间变化的最坏情况下的性能，并开发一个过滤的融合间隔。该间隔保证包含真实值，并且大小有界。其次，针对不符合传感器瞬态故障模型的攻击，提出了一种基于传感器测量值之间成对不一致的攻击检测算法[41]。Zhang 等研究了基于系统动态平衡的传感器攻击检测算法，通过构造

一个时间窗内的滚动预测状态空间来判断物理状态是否在预定平衡点上，进而判断期间是否存在传感器攻击[42]。Akowuah 等提出了一个实时自适应传感器攻击检测框架。该框架可以根据不同的系统状态来动态调整检测延迟和虚警率，以满足检测期限，提高系统的可用性。该框架的核心组件是一个攻击检测器，其基于 Cumulative Sum(CUSUM)算法，通过监控传感器观测值和期望值之间的差异累计和来辨识异常情况[43]。Zhu 在线性矩阵不等式可行的假设下，设计了一种类 Luenberger 的 H 值观测器，其在 H 值性能指标上对扰动体现出了强鲁棒性。此外，构造了残差并给出了残差的间隔估计，并在此基础上提出了一种基于残差间隔估计的 Finite Difference(FD)算法，用以检测异常数据[44]。Degue 等在存在未知但有界的噪声和扰动的情况下，设计了能够克服线性时不变控制系统的隐身攻击的方法，该系统使用间隔观测器估计其状态；同时，分析了恶意代理使用附加攻击信号来危害系统的传感器和执行器的场景，其将状态估计控制在了间隔观测提供的界限之外，并据此提出了一种使用半定规划来确定最佳观测器增益的计算方法，用于计算未知攻击信号界限[45]。

5.3 基于历史一致性的攻击检测

Radoslav 等在基于间隔算法的基础上提出了时间窗累积检测算法，当在时间窗口内被识别为攻击的次数超过设定的阈值时，确定传感器受到攻击[46]。Bai 等分析了卡尔曼滤波框架下的攻击行为，评估了攻击可以造成的最坏影响，给出了最优攻击策略[20]。Dorigoni 等利用一个滚动时间窗对一段时间内的估测值的方差进行监测，可以监测不符合高斯分布的攻击行为[47]。Koley 等提出一种基于强化学习的攻击检测框架，其根据攻击场景所学习的经验自适应地设置攻击检测算法的参数，为检测系统提供一个合适的训练环境，学习如何在实现最高检测率的同时将误报降到最低[48]。针对具有足够和有限能量的隐蔽攻击，有学者提出了基于分布式估计器的新型检测器。Lv 等在部分传感器存在虚假数据注入攻击的情况下，通过最小化估计误差协方差的最优卡尔曼增益来分析估计误差协方差收敛的充分条件[49]。隐藏攻击向传感器测量中注入了极小的恶意信号，以至于它们可以保持不被检测，但最终会导致结果出现显著偏差。Liu 等针对隐藏攻击，根据历史传感器数据，以离线方式划定系统安全运行区域，在该区域内即便隐藏攻击不被检测出来，依然能够保证系统安全运行，超过该区域则说明检测出了隐藏攻击，然后发出黄色等级的报警[50]。

5.4 基于响应一致性的攻击检测

在主动方式的攻击检测方面，针对传感器攻击检测的研究较少。在无线传感网络、汽车自动驾驶视觉识别等领域，已有应用水纹原理进行攻击检测的研究。基于响应一致性的攻击检测直接在 CPS 中的某一节点施加主动激励，在系统中的不同传感节点观察激励产生的响应，如 X^2 校验。通过在网络中某一节点施加特定的主动激励，观测特定节点的数据变化特征，可以对系统的特性进行评估[38]。Kumar 团队针对自适应巡航控制系统和无人车跟踪给定轨迹系统，提出了动态水印算法，在执行器中注入特定激励并与期望激励作对比，对重放攻击进行检测[51-52]。Rubio-Hernan 等分析了假设攻击者能够推断系统动力学，并且能够以高频率躲避检测器情况下的检测率，并提出了一种采用几种非平稳水印的检测方案，能够应对非参数方法攻击[53]。Fang 等针对不连续重放攻击，建立了一次性攻击持续时间模型，然后利用该攻击模型提出了一种周期水印策略，以降低控制的时间成本[54]。Liu 等提出了一种新的混合主动检测方案，将水印和运动目标相结合来检测隐蔽攻击，所设计的异常检测器基于小带观测器的残差，可以用来估计有未知有界噪声的系统状态[55-56]。然而，上述攻击检测方法仅通过最差情况分析或卡尔曼滤波算法处理随机噪声和随机延迟，难以准确区分这些干扰与传感器攻击。最差情况分析的精度不高，因为它未有效利用随机延迟的概率分布信息；卡尔曼滤波算法只能处理零均值高斯噪声，而随机延迟不符合此条件。常规攻击检测算法对随机噪声和随机延迟的处理能力不足，必须准确处理非零均值的随机延迟，才能满足传感器防御的功能要求。

表 2 相关工作对比

Table 2 Comparison of related works

研究方向	学者/团队	方法/算法	优点	不足
基于多源一致性的攻击检测	Marzullo 等	最差情况分析与多数投票法	不受限于噪声概率分布，能直接应用于异常数据	被动检测，可能无法及时发现快速变化的攻击
	Lu 等	虚拟传感器构造	增强了数据的一致性和可靠性	复杂度增加，实施难度提升
	Park 等	瞬态攻击与永久攻击模型	适应性强，能处理不同类型的攻击	需要较强的模型假设，可能不适用于所有场景
	Zhang 等	基于系统动态平衡的检测算法	通过动态平衡判断提高检测的准确性	可能对传感器的动态变化敏感，需精确建模
	Akowuah 等	实时自适应攻击检测框架	可根据系统状态调整，提升系统可用性	复杂性高，需持续监控系统状态
	Zhu	类 Luenberger 的 H 观测器	鲁棒性强，适应各种干扰情况	实施较为复杂，对模型参数敏感
	Degue 等	间隔观测器与半定规划	能有效处理未知攻击信号，适应性强	可能对模型假设有较高要求
基于历史一致性的攻击检测	Radoslav 等	时间窗累积检测算法	简单易实现，适用于长期监控	对短期攻击敏感性不足，可能出现误报
	Bai 等	卡尔曼滤波框架下的攻击分析	能够有效评估攻击影响，适用于动态环境	依赖于系统模型，可能不适用于所有类型的攻击
	Basiri 等	滚动时间窗方差监测	能够及时发现不符合分布的异常	适应性不足，对分布假设敏感
	Koley 等	基于强化学习的攻击检测	适应性强，能自动优化检测算法参数	训练数据需求大，实施成本高
	Lv 等	分布式估计器与最优卡尔曼	能够处理复杂场景，提高估计精度	需要较强的假设条件和精确建模
	Liu 等	离线系统安全运行区域划定	能够有效防范隐藏攻击，保障系统稳定性	对于动态环境适应性不足，可能造成误报警
基于响应一致性的攻击检测	Kumar 团队	动态水印算法	能有效检测重放攻击，提高响应安全性	需精确控制激励信号，实施复杂度较高
	Rubio-Hernan 等	非平稳水印检测方案	能应对多种攻击，增强检测能力	需考虑多种攻击模型，复杂性高
	Fang 等	周期水印策略	降低成本，提高检测效率	对攻击模式假设要求较高，可能对多种攻击不敏感
	Liu 等	混合主动检测方案	结合多种方法，增强检测的鲁棒性	需精确建模和参数设定，实施复杂度增加

6 传感器数据融合

在检测出受攻击的传感器后，通过传感器数据融合算法对物理状态实现高精度估测。攻击传感器数据的处理可以分为两大类：一类是直接丢弃被攻击数据[37]；另一类是在丢弃源数据的基础上，利用对应传感器的历史数据进行基于物理模型的预测补偿[38]。在攻击传感器数据处理的基础上，影响传感器数据融合精度的主要因素是传感器自身测量的随机噪声和传感器数据传输过程中的随机延迟。在多数实际系统中，高斯噪声是随机噪声最为广泛的分布形式，可以通过适当的滤波算法进行处理；而随机延迟受到通信协议、网络状态、外部干扰等因素的影响，不同系统间的延迟存在较大差异，不服从零均值高斯分布[57-58]。

6.1 基于卡尔曼滤波的数据融合算法

卡尔曼滤波是当前应用最广泛的随机噪声处理算法，在此基础上衍生出了适应不同场景的数据融合算法。Pu 等提出了一种有效的块坐标下降算法来解决异步多传感器注册问题[59-63]。他们利用一个以几乎恒定的速度移动的参考目标来获得局部估计器和交叉协方差矩阵。基于这些估计器，他们提出了一个分布式最优融合估计器，其采用基于线性最小方差的矩阵加权融合估计算法[64-65]。该方法旨在通过有效地融合来自多个传感器的异步数据，提高状态估计的准确性和可靠性。Corrales 等介绍了一个多传感器融合框架，解决了测量中的未知时间偏移的补偿问题。他们开发了一种连续时间解来估计状态变量，以适应传感器之间的时间偏移变化。这种自适应融合技术通过有效地对齐不同传感器的异步测量，实现了更准确的状态估计[66-67]。Huang 等提出了一种基于改进的反向传播神经网络并经由粒子群优化算法优化的多传感器数据融合算法[68]。通过使用粒子群优化算法优化网络输入，该算法提高了数据融合性能，并基于多传感器的异步数据实现了对雪车状态的高准确性估计。这种方法利用了神经网络和优化技术的优势，应对了异步数据融合的挑战。Li 等提出了集中式顺序处理的方法，利用顺序方法来预测和更新基于测量集到达时间序列的后验概率。通过考虑异步传感器数据的时间顺序，该方法提高了雪车状态的融合精度和实时性能[69]。Tang 等针对智能电网的数据融合问题，利用系统数学模型设计了一个预测误差评估值，并在此基础上提出了结合卡尔曼滤波和安全估计的数据融合算法[70]。将超宽带定位与惯性测量单元相结合的融合方法，在无人机室内定位方面取得了较高的定位精度[71-72]。这些方法通常采用特征层融合，主要依赖于扩展卡尔曼滤波器，以获取更高精度的定位信息。

6.2 基于间隔的数据融合算法

在基于多源一致性的攻击检测算法的基础上，众多学者提出了相应的基于间隔的数据融合算法。Tang 等研究了离散线性时不变系统的间隔估计方法，提出了一种新的间隔估计方法，将鲁棒观测器设计与可达性分析相结合。通过在间隔估计中引入 H∞设计，该方法有效地提高了间隔估计的精度[73]。Huang 等研究了含扰动的离散时间切换广义系统的基于函数间隔观测器的估计方法，提出了一个采用 H∞形式的函数观测器，然后利用基于分区拓扑的方法来估计其边界，减少了观测器设计约束[74]。Guo 等研究了离散时间 Takagi-Sugeno 模糊系统的间隔估计方法，集成了基于 H∞技术和可达性分析的鲁棒观测器，从而获得了精确的估计结果，同时抑制了系统中的干扰和噪声[75]。Tang 等提出了一种基于广义系统观测器和观测器误差界的分区估计器的集员估计方法。为了最小化包围所有允许状态轨迹的窄带节点的大小，对观察器参数进行优化[76]。以图 3 为例，假设对 5 个传感器数据进行融合，S_1-S_5（从上到下）的初始间隔分别为[14,19]，[11,17]，[13,18]，[12,15]及[10,13]，每个传感器的间隔都表示真实测量值的可能范围。在少于半数传感器受攻击的条件下，真实被测值一定落在所有或多数传感器的重叠范围内。在获取了 5 个传感器的间隔后，计算不同范围内传感器间隔重叠的个数，其表征了真实值落在该范围内的可能性大小。在[10,11]，[11,12]，[12,13]，[13,14]，[14,15]，[15,17]，[17,18]和[18,19]这 8 段范围内，分别有 1,2,3,3,4,3,2,1 个重叠间隔。采用多数投票法进行融合，则间隔[14,15]有 4 个传感器（S_1-S_4）有共同重叠，具有最高的投票权重，因此选取该间隔作为最终融合间隔，S_5 数据被丢弃。

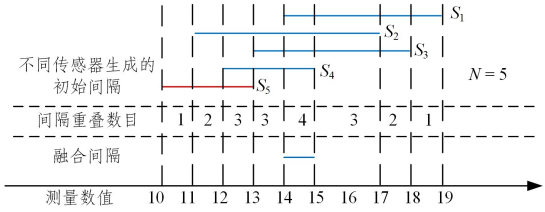

图 3 基于间隔的数据融合方法

Fig. 3 Data fusion based on interval

目前已有许多方法可以融合具有不同频率和时间戳的异步数据。对于多个采样率，数据融合控制器可以通过同步器预处理原始数据，选择最新的数据对，但会舍弃一些高频数据，例如，Apollo Cyber RT 的数据同步器[77]。为了避免丢弃数据，可以多阶段融合关联不同采样率传感器的最新数据，以充分利用原始数据[78-80]。此外，可以通过零阶/一阶保持等数学方法重建低速数据，并将其作为高速数据[81-82]。处理异步时间戳时，可以引入中点来获得同步状态预测[83-84]。针对通信网络的随机延迟问题，众多学者对传统卡尔曼滤波算法进行了改进，以减小随机延迟的影响。通过物理模型预测补偿通信延迟的影响是其中一个重点方向。Li 等在无线网络中，利用历史数据和通信延迟估测值对传感器数据进行动态补偿[78]。Nesti 等将传统卡尔曼滤波器扩展到 2 维空间，建立了 2 维正则化最小二乘估测模型，利用历史方差对随机延迟产生的误差进行最小化处理[85]。Wang 等在多采样频率和通信延迟条件下，利用被控系统的数学模型，对传感器测量值进行了不确定补偿[86]。Muhammad 等研究了不同采样频率和通信延迟下的状态估测算法，通过一段时间内滚动预测的方式实现了对状态量的平滑估测[87]。Sun 等对一个时间窗内的卡尔曼滤波矩阵进行观测，在状态估测中引入系统不确定性来缓解随机延迟的影响[88]。

结束语 本文综述了信息物理系统（CPS）中传感器攻击的类型、影响及其防御策略。传感器作为 CPS 的关键组件，

其安全性对整个系统的稳定运行至关重要。当前研究主要集中在攻击检测和数据融合等方面的传感器攻击防御方法，这些方法在一定程度上提升了 CPS 的安全性，但仍面临诸多挑战。

未来，传感器攻击防御策略的发展方向包括以下几个方面。1)智能化防御系统：结合人工智能和机器学习技术，构建更为智能的攻击检测和防御系统，以自适应地识别和应对新型攻击手段。2)分布式防御机制：发展分布式防御架构，利用多传感器的协同工作提高系统的鲁棒性和安全性，避免单点故障。3)区块链技术应用：探索区块链技术在传感器数据验证和溯源中的应用，增强数据传输过程中的安全性和可信性。4)动态安全策略：研究动态调整防御策略的方法，根据实时威胁情报和系统状态，灵活调整防御措施，提高系统的响应速度和防御效果。5)标准化与规范化：推动传感器安全标准和规范的制定，建立统一的安全评估和认证体系，促进 CPS 安全防护技术的广泛应用和普及。

综上所述，随着信息物理系统在各个领域的广泛应用，传感器攻击防御将成为保障系统安全的核心问题。未来需要持续关注新技术的发展和新型攻击手段的出现，通过不断创新和完善防御策略，构建更加安全可靠的信息物理系统。

参 考 文 献

[1] KONG F, XU M, WEIMER J, et al. Cyber-physical system checkpointing and recovery [C]// 2018 ACM/IEEE 9th International Conference on Cyber-Physical Systems (ICCPS). IEEE, 2018: 22-31.

[2] KONG F, SOKOLSKY O, WEIMER J, et al. State consistencies for cyber-physical system recovery [C]// the 2nd Workshop on Cyber-Physical Systems Security and Resilience (CPSSR). 2019: 3-7.

[3] GIRALDO J, URBINA D, CARDENAS A, et al. A survey of physics-based attack detection in cyber-physical systems [J]. ACM Computing Surveys (CSUR), 2018, 51(4): 1-36.

[4] FENG S, LI X, ZHANG S, et al. A review: State estimation based on hybrid models of Kalman filter and neural network [J]. Systems Science & Control Engineering, 2023, 11(1): 2173682.

[5] WEI H, TANG H, JIA X, et al. Physical adversarial attack meets computer vision: A decade survey [J]. arXiv: 2209.15179v3, 2022.

[6] JU Z, ZHANG H, LI X, et al. A survey on attack detection and resilience for connected and automated vehicles: From vehicle dynamics and control perspective [J]. IEEE Transactions on Intelligent Vehicles, 2022, 7(4): 815-837.

[7] PARK P, COLERI ERGEN S, FISCHIONE C, et al. Wireless network design for control systems: A survey [J]. IEEE Communications Surveys & Tutorials, 2018, 20(2): 978-1013.

[8] AGHILI S F, ASHOURI-TALOUKI M, MALA H. Dos, impersonation and desynchronization attacks against an ultra-lightweight rfid mutual authentication protocol for iot [J]. The Journal of Supercomputing, 2018, 74(1): 509-525.

[9] SHANG J, CHEN M, CHEN T. Optimal linear encryption against stealthy attacks on remote state estimation [J]. IEEE Transactions on Automatic Control, 2020, 66(8): 3592-3607.

[10] SHOUKRY Y, MARTIN P, YONA Y, et al. Pycra: Physical challenge-response authentication for active sensors under spoofing attacks [C]// Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. 2015: 1004-1015.

[11] XIONG W, LAGERSTRÖM R. Threat modeling—a systematic literature review [J]. Computers & Security, 2019, 84: 53-69.

[12] 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.

[13] PAJIC M, WEIMER J, BEZZO N, et al. Robustness of attack-resilient state estimators [C]// 2014 ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS). 2014.

[14] ZHANG L, CHEN X, KONG F, et al. Real-time attack-recovery for cyber-physical systems using linear approximations [C]// 2020 IEEE Real-Time Systems Symposium (RTSS). IEEE, 2020: 205-217.

[15] ZHANG L, SRIDHAR K, LIU M, et al. Real-time data-predictive attack-recovery for complex cyber-physical systems [C]// 2023 IEEE 29th Real-Time and Embedded Technology and Applications Symposium (RTAS). IEEE, 2023: 209-222.

[16] KHAN M A, ULLAH I, ALKHALIFAH A, et al. A provable and privacy-preserving authentication scheme for uav-enabled intelligent transportation systems [J]. IEEE Transactions on Industrial Informatics, 2021, 18(5): 3416-3425.

[17] AGHILI S F, ASHOURI-TALOUKI M, MALA H. Dos, impersonation and desynchronization attacks against an ultra-lightweight rfid mutual authentication protocol for iot [J]. The Journal of Supercomputing, 2018, 74(1): 509-525.

[18] SHOUKRY Y, MARTIN P, YONA Y, et al. Pycra: Physical challenge-response authentication for active sensors under spoofing attacks [C]// Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. 2015: 1004-1015.

[19] SODHROA H, AWADA I, VAN DE BEEK J, et al. Intelligent authentication of 5g healthcare devices: A survey [J]. Internet of Things, 2022, 20: 100610.

[20] BAI Y, ZHENG K, WANG Z, et al. Dynamic channel selection for real-time safety message communication in vehicular networks [C] // 2018 IEEE Real-Time Systems Symposium (RTSS). IEEE, 2018: 56-66.

[21] SHANG J, CHEN M, CHEN T. Optimal linear encryption against stealthy attacks on remote state estimation [J]. IEEE Transactions on Automatic Control, 2020, 66(8): 3592-3607.

[22] LIAN J, HUANG X. Resilient control of networked switched systems against dos attack [J]. IEEE Transactions on Industrial Informatics, 2021, 18(4): 2354-2363.

[23] ZHANG J, SUN J, LIN H. Optimal dos attack schedules on remote state estimation under multi-sensor round-robin protocol [J]. Automatica, 2021, 127: 109517.

[24] TAHOUN A H, ARAFA M. Cooperative control for cyber-

physical multi-agent networked control systems with unknown false data-injection and replay cyber-attacks[J]. ISA transactions, 2021, 110: 1-14.

[25] ZAMAN A, SAFARINEJADIAN B, BIRK W. Security analysis and fault detection against stealthy replay attacks[J]. International Journal of Control, 2022, 95(6): 1562-1575.

[26] KHARE G, MOHAPATRA A, SINGH S N. State vulnerability assessment against false data injection attacks in ac state estimators[J]. Energy Conversion and Economics, 2022, 3(5): 319-332.

[27] REDA H T, ANWAR A, MAHMOOD A N, et al. A taxonomy of cyber defence strategies against false data attacks in smart grids[J]. ACM Computing Surveys, 2023, 55(14s): 1-37.

[28] GHEITASI K, LUCIA W. Undetectable finite-time covert attack on constrained cyberphysical systems[J]. IEEE Transactions on Control of Network Systems, 2022, 9(2): 1040-1048.

[29] JORJANI M, SEIFI H, VARJANI A Y. A graph theory-based approach to detect false data injection attacks in power system ac state estimation[J]. IEEE Transactions on Industrial Informatics, 2020, 17(4): 2465-2475.

[30] TIAN J, WANG B, WANG Z, et al. Joint adversarial example and false data injection attacks for state estimation in power systems[J]. IEEE Transactions on Cybernetics, 2021, 52(12): 13699-13713.

[31] AOUFI S, DERHAB A, GUERROUMI M. Survey of false data injection in smart power grid: Attacks, countermeasures and challenges[J]. Journal of Information Security and Applications, 2020, 54: 102518.

[32] SENGAN S, SUBRAMANIYASWAMY V, INDRAGANDHI V, et al. Detection of false data cyber-attacks for the assessment of security in smart grid using deep learning[J]. Computers & Electrical Engineering, 2021, 93: 107211.

[33] SHINOHARA T, NAMERIKAWA T. Distributed secure state estimation with a priori sparsity information[J]. IET Control Theory & Applications, 2022, 16(11): 1086-1097.

[34] FAWZI H, TABUADAP, DIGGAVI S. Security for control systems under sensor and actuator attacks[M]// 2012 IEEE 51st IEEE Conference on Decision and Control (CDC). IEEE, 2012: 3412-3417.

[35] TSAI T, YANG K, HO T Y, et al. Robust adversarial objects against deep learning models[C]// Proceedings of the AAAI Conference on Artificial Intelligence. 2020.

[36] MERDRIGNAC P, SHAGDAR O, NASHASHIBI F, et al. Fusion of perception and v2p communication systems for the safety of vulnerable road users[J]. IEEE Transactions on Intelligent Transportation Systems, 2017, 18(7): 1740-1751.

[37] MARZULLO K. Tolerating failures of continuous-valued sensors[J]. ACM Transactions on Computer Systems, 1990, 8(4): 284-304.

[38] IVANOV R, PAJIC M, LEE I. Attack-resilient sensor fusion for safety-critical cyber-physical systems [J]. ACM Transactions in Embedded Computing Systems, 2016, 15(1): 21.

[39] JO M, PARK J, BAEK Y, et al. Adaptive transient fault model for sensor attack detection [C]// IEEE International Conference on Cyber-physical Systems. 2016.

[40] LU P, ZHANG L, PARK B B, et al. Attack-resilient sensor fusion for cooperative adaptive cruise control[C]// 2018 21st International Conference on Intelligent Transportation Systems (ITSC). 2018: 3955-3960.

[41] PARK J, IVANOV R, WEIMER J, et al. Security of cyber-physical systems in the presence of transient sensor faults[J]. ACM Transactions on Cyber-Physical Systems, 2017, 1(3): 1-23.

[42] ZHANG L, WANG Z, LIU M, et al. Adaptive window-based sensor attack detection for cyberphysical systems[C]// Proceedings of the 59th ACM/IEEE Design Automation Confe-rence. 2022: 919-924.

[43] AKOWUAH F, KONG F. Real-time adaptive sensor attack detection in autonomous cyberphysical systems[C]// 2021 IEEE 27th Real-time and Embedded Technology and Applications Symposium (RTAS). IEEE, 2021: 237-250.

[44] ZHU F, TANG Y, WANG Z. Interval-observer-based fault detection and isolation design for ts fuzzy system based on zonotope analysis[J]. IEEE Transactions on Fuzzy Systems, 2021, 30(4): 945-955.

[45] DEGUE K H, LE NY J, EFIMOV D. Stealthy attacks and attack-resilient interval observers [J]. Automatica, 2022, 146: 110558.

[46] RAVI A, NARASIMHAN S, KAISARE N S. Sampled output augmentation method for handling measurement delays in multirate kalman filter[J]. Chemical Engineering Science, 2020, 224: 115763.

[47] DORIGONI D, FONTANELLI D. An uncertainty-driven analysis for delayed mapping slam[C]// 2021 IEEE International Instrumentation and Measurement Technology Conference (I2MTC). 2021: 1-6.

[48] KOLEY I, ADHIKARY S, DEY S. Catch me if you learn: Real-time attack detection and mitigation in learning enabled cps [C]// 2021 IEEE Real-Time Systems Symposium (RTSS). IEEE, 2021: 136-148.

[49] LV Y, LU J, LIU Y, et al. Resilient distributed state estimation under stealthy attack[J]. IEEE Transactions on Information Forensics and Security, 2022, 17: 3254-3263.

[50] LIU M, ZHANG L, LU P, et al. Fail-safe: Securing cyber-physical systems against hidden sensor attacks[C]// 2022 IEEE Real-Time Systems Symposium (RTSS). IEEE, 2022: 240-252.

[51] KO W H, SATCHIDANANDAN B, KUMAR P. Dynamic watermarking-based defense of transportation cyber-physical systems[J]. ACM Transactions on Cyber-Physical Systems, 2019, 4(1): 1-21.

[52] SATCHIDANANDAN B, KUMAR P R. Dynamic watermarking: Active defense of networked cyber-physical systems[C]// Proceedings of the IEEE. 2016: 219-240.

[53] RUBIO-HERNAN J, DE CICCO L, GARCIA-ALFARO J. On the use of watermark-based schemes to detect cyber-physical attacks[J]. EURASIP Journal on Information Security, 2017, 2017(1): 1-25.

[54] FANG C, QI Y, CHENG P, et al. Optimal periodic watermarking schedule for replay attack detection in cyber-physical sys-

tems[J]. Automatica, 2020, 112: 108698.
[55] LIU H, ZHANG Y, LI Y, et al. Proactive attack detection scheme based on watermarking and moving target defense[J]. Automatica, 2023, 155: 111163.
[56] LIU H, LI Y, HAN Q L, et al. Watermark-based proactive defense strategy design for cyber physical systems with unknown-but-bounded noises[J]. IEEE Transactions on Automatic Control, 2023, 68(6): 3300-3315.
[57] TU Y J, PIRAMUTHU S. On addressing rfid/nfc-based relay attacks: An overview [J]. Decision Support Systems, 2020, 129: 113194.
[58] KHALAJMEHRABADI A, GATSIS N, AKOPIAN D, et al. Real-time rejection and mitigation of time synchronization attacks on the global positioning system[J]. IEEE Transactions on Industrial Electronics, 2018, 65(8): 6425-6435.
[59] PU W, LIU Y F, YAN J, et al. Optimal estimation of sensor biases for asynchronous multi-sensor data fusion[J]. Mathematical Programming, 2018, 170: 357-386.
[60] LIN H, SUN S. Distributed fusion estimator for multi-sensor asynchronous sampling systems with missing measurements[J]. IET Signal Processing, 2016, 10(7): 724-731.
[61] CABALLERO-ÁGUILA R, GARCÍA-GARRIDO I, LINARES-PÉREZ J. Information fusion algorithms for state estimation in multi-sensor systems with correlated missing measurements[J]. Applied Mathematics and Computation, 2014, 226: 548-563.
[62] TANG W, WANG Z, WANG Y, et al. Interval estimation methods for discrete-time linear time-invariant systems[J]. IEEE Transactions on Automatic Control, 2019, 64(11): 4717-4724.
[63] HE N, SHI D, CHEN T. Self-triggered model predictive control for networked control systems based on first-order hold[J]. International Journal of Robust and Nonlinear Control, 2018, 28(4): 1303-1318.
[64] 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.
[65] MUELLER M W, HAMER M, D'ANDREA R. Fusing ultra-wideband range measurements with accelerometers and rate gyroscopes for quadrocopter state estimation[C]// 2015 IEEE International Conference on Robotics and Automation (ICRA). IEEE, 2015: 1730-1736.
[66] CORRALES J A, CANDELAS F A, TORRES F. Hybrid tracking of human operators using imu/uwb data fusion by a kalman filter[C]// Proceedings of the 3rd ACM/IEEE International Conference on Human Robot Interaction. 2008: 193-200.
[67] WANG J, ZHANG B, GAO S, et al. A data fusion algorithm of the improved bp neural network by particle swarm optimization [C]// 2021 CAA Symposium on Fault Detection, Supervision, and Safety for Technical Processes (SAFEPROCESS). 2021: 1-8.
[68] KARAFYLLIS I, KRSTIC M. Nonlinear stabilization under sampled and delayed measurements, and with inputs subject to delay and zero-order hold[J]. IEEE Transactions on Automatic Control, 2011, 57(5): 1141-1154.
[69] LI G, YI W, LI S, et al. Asynchronous multi-rate multi-sensor fusion based on random finite set[J]. Signal Processing, 2019, 160: 113-126.
[70] GIRBÉS-JUAN V, ARMESTO L, HERNÁNDEZ-FERRÁNDIZ D, et al. Asynchronous sensor fusion of gps, imu and can-based odometry for heavy-duty vehicles[J]. IEEE Transactions on Vehicular Technology, 2021, 70(9): 8617-8626.
[71] YU B, HU W, XU L, et al. Building the computing system for autonomous micromobility vehicles: Design constraints and architectural optimizations[C]// 2020 53rd Annual IEEE/ACM International Symposium on Microarchitecture. IEEE, 2020: 1067-1081.
[72] SKOG I, HANDEL P. Time synchronization errors in loosely coupled gps-aided inertial navigation systems[J]. IEEE Transactions on Intelligent Transportation Systems, 2011, 12(4): 1014-1023.
[73] TANG W, WANG Z, ZHANG Q, et al. Set-membership estimation for linear time-varying descriptor systems[J]. Automatica, 2020, 115: 108867.
[74] HUANG J, CHE H, RAÏSSI T, et al. Functional interval observer for discrete-time switched descriptor systems[J]. IEEE Transactions on Automatic Control, 2021, 67(5): 2497-2504.
[75] GUO S, REN W, AHN C K, et al. Reachability analysis-based interval estimation for discretetime takagi-sugeno fuzzy systems [J]. IEEE Transactions on Fuzzy Systems, 2021, 30(6): 1981-1992.
[76] VEIBÄCK C, HENDEBY G, GUSTAFSSON F. Uncertain timestamps in linear state estimation[J]. IEEE Transactions on Aerospace and Electronic Systems, 2018, 55(3): 1334-1346.
[77] VEIBÄCK C, HENDEBY G, GUSTAFSSON F. On fusion of sensor measurements and observation with uncertain timestamp for target tracking[C]// 2016 19th International Conference on Information Fusion. IEEE, 2016: 1268-1275.
[78] LI B, XIAO G, LU R, et al. On feasibility and limitations of detecting false data injection attacks on power grid state estimation using d-facts devices[J]. IEEE Transactions on Industrial Informatics, 2020, 16(2): 854-864.
[79] ZHAO D, DING S X, KARIMI H R, et al. Robust l filtering for two-dimensional uncertain linear discrete time-varying systems: A krein space-based method[J]. IEEE Transactions on Automatic Control, 2019, 64(12): 5124-5131.
[80] WANG Y, LIU Y, FUJIMOTO H, et al. Vision-based lateral state estimation for integrated control of automated vehicles considering multi-rate and unevenly delayed measurements[J]. IEEE/ASME Transactions on Mechatronics, 2018, 23(6): 2619-2627.
[81] 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.
[82] CHONG M S, WAKAIKI M, HESPANHA J P. Observability of linear systems under adversarial attacks [C]// 2015 American

Control Conference(ACC). IEEE,2015:2439-2444.

[83] ZHOU S,LIU C,YE D,et al. Adversarial attacks and defenses in deep learning:From a perspective of cybersecurity[J]. ACM Computing Surveys,2022,55(8):1-39.

[84] HUANG H,CHEN Z,CHEN H,et al. T-sea:Transfer-based self-ensemble attack on object detection[C]// Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2023:20514-20523.

[85] NESTI F,ROSSOLINI G,NAIR S,et al. Evaluating the robustness of semantic segmentation for autonomous driving against real-world adversarial patch attacks[C]// Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision. 2022:2280-2289.

[86] WANG J,WANG C,LIN Q,et al. Adversarial attacks and defenses in deep learning for image recognition:A survey[J]. Neurocomputing,2022,514:162-181.

[87] MUHAMMAD F,ANJUM W,MAZHAR K S. A critical analysis on the security concerns of internet of things(iot) [J]. International Journal of Computer Applications,2015,111(7):1-6.

[88] SUN J,CAO Y,CHEN Q A,et al. Towards Robust LiDAR-based Perception in Autonomous Driving:General Black-box Adversarial Sensor Attack and Countermeasures[J]. arXiv:2006.16974,2020.

CHEN Yanfeng,born in 1992,Ph.D,is a member of CCF (No. T9340G). His main research interests include cyber-physical system,sensor fusion,and sensor attack-resilience.

WANG Yan,born in 1978,Ph.D,professor,Ph.D supervisor,is a member of CCF(No. 18011M). Her main research interests include big data analysis,block-chain and artificial intelligence.

(责任编辑:柯颖)