控制与决策
Control and Decision

离散事件系统框架下信息物理系统攻击问题综述

王寿光, 赵玉美, 尤丹, 冉宁

引用本文:
王寿光,赵玉美,尤丹,冉宁. 离散事件系统框架下信息物理系统攻击问题综述[J]. 控制与决策, 2022, 37(8): 1934−1944.

在线阅读 View online: https://doi.org/10.13195/j.kzyjc.2021.0465

离散事件系统框架下信息物理系统攻击问题综述

王寿光[1†], 赵玉美[1], 尤 丹[1], 冉 宁[2]

(1. 浙江工商大学 信息与电子工程学院(萨塞克斯人工智能学院), 杭州 310018;
2. 河北大学 电子信息工程学院, 河北 保定 071000)

摘 要: 信息物理系统(cyber physical system, CPS)由受控对象、传感器、执行器、监控器和通信网络组成,通信网络的使用增加了信息物理系统面临外部攻击的风险. 鉴于此,综述基于离散事件系统框架处理信息物理系统攻击问题的相关研究工作. 首先对信息物理系统进行简要介绍;然后对信息物理系统中的攻击进行分类;最后重点阐述信息物理系统中攻击策略的设计、攻击的检测与防御以及攻击鲁棒性监控器设计的研究现状.

关键词: 信息物理系统; 离散事件系统; 网络攻击; 攻击策略; 攻击检测与防御

中图分类号: TP13 **文献标志码:** A

DOI: 10.13195/j.kzyjc.2021.0465

引用格式: 王寿光,赵玉美,尤丹,等. 离散事件系统框架下信息物理系统攻击问题综述[J]. 控制与决策, 2022, 37(8): 1934-1944.

Survey on attacks in cyber physical systems based on discrete event systems

WANG Shou-guang[1†], *ZHAO Yu-mei*[1], *YOU Dan*[1], *RAN Ning*[2]

(1. School of Information and Electronic Engineering (Sussex Artifical Intelligence Institute), Zhejiang Gongshang University, Hangzhou 310018, China; 2. School of Electronic Information Engineering, Hebei University, Baoding 071000, China)

Abstract: A cyber physical system (CPS) is composed of plants, sensors, actuators, supervisors and communication networks. The use of communication networks increases the vulnerability of CPS to cyber attacks. In this paper, we summarize the related research work of tackling the attack issues of CPS based on the framework of discrete event systems. Firstly, we give a brief introduction to CPS. Then, we classify attacks in CPS. Finally, the various work on the design of attacks strategies, the detection and defense of attacks and the design of robustness supervisors for CPS vulnerable to attacks are introduced.

Keywords: cyber physical system; discrete event systems; cyber attacks; attack strategy; attack detection and defense

0 引 言

信息物理系统(cyber physical system, CPS)最早由美国航天局于1992年提出,在2006年的美国科学基金会议“NSF Workshop on Cyber-Physical Systems”上首次详细描述. 它以computation、communication、control (3C)技术为载体,集成了计算和通信功能,用以监视和控制物理过程[1-2],实现了计算资源与物理资源的紧密结合与协调. CPS自提出以来受到各国的广泛关注,欧洲提出“嵌入智能与系统的先进研究与技术”(ARTMEIS)项目对CPS模型进行研究[3]、美国科学技术顾问委员会(PCAST)将CPS列为未来八大关键技术首位[4]、德国“工业4.0”将CPS作为核心技术[5]、中国提出“中国制造2025”[6]与“工业4.0”对接. 同时,信息物理系统的应用领域非常广泛,已经渗透到日常生活的各个方面,包括智能电网系统[7-8]、医疗检测系统[9-10]、智能交通系统[11-13]、网络控制系统[14]等. CPS的基本组成包括受控对象、传感器、执行器、监控器以及通信网络,可建模为图1所示的闭环系统[15]. 传感器对物理系统产生的信号进行采集,信息通过通信网络传输给监控器,监控器对数据进行分析后,下达的命令通过通信网络传输给执行器,执行器根据监控器的指令对物理系统施加控制作用. 通信网络的使用虽然使得CPS各个组件都具有信息处理和通信的能力,但增加了CPS应对网络攻击的脆弱性. 攻击可能会入侵传感器、执行器以及通信网络,进而破坏数据收集过程,干扰关键决策等,这

收稿日期: 2021-03-20; **录用日期:** 2021-07-19.

基金项目: 浙江省自然科学基金项目(LGJ21F030001, LQ20F020009); 国家自然科学基金项目(61903119); 浙江省新型网络标准与应用技术重点实验室项目(2013E10012).

†通讯作者. E-mail: wsg5000@hotmail.com.

可能对受控物理系统造成巨大的损害,导致不可估量的经济损失,甚至引发重大安全事故. 例如:2015年,乌克兰电力系统被植入计算机恶意软件BlackEnergy导致电力系统运行中断,造成严重的经济损失;2018年,荷兰一男子通过租用Mirai变种物联僵尸网络对几家荷兰企业发动拒绝服务攻击,导致荷兰所有银行瞬间崩溃;2021年,美国本土石油运输“大动脉”Colonial Pipeline管道遭受攻击,导致美国17个州及华盛顿特区进入紧急状态. 由上述事例可见,保护信息物理系统的安全尤为重要. 近年来,信息物理系统的安全问题成为一大研究热点[16-21].

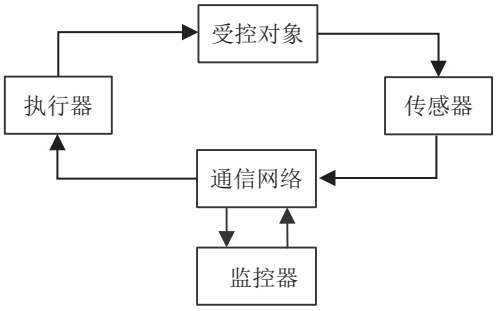

图 1　闭环控制系统

信息物理系统安全问题的研究最早是在连续系统框架下进行的[22-27]. 连续系统是指受控对象的输入输出变量均为连续变量. 在连续系统框架下,学者们针对拒绝服务攻击[28-34]、欺骗攻击[35-39]、重放攻击[40-45]等攻击类型进行研究. 近年来,也有很多学者在离散事件系统框架下研究此类问题. 实际上,生活中的人造系统,如智能电网系统、医疗检测系统等从逻辑层面上而言都可以建模为离散事件系统. 准确来说,离散事件系统是一个状态离散、状态的转移由事件的发生来触发的一个动态系统[46]. 在离散事件系统框架下,可以更关注上层的逻辑行为来研究问题.

本文将介绍离散事件系统框架下信息物理系统攻击问题的相关研究工作,具体包括攻击的分类、攻击的设计、攻击的检测与防御以及鲁棒性监控器的设计.

1　攻击分类

考虑图1所示的闭环控制系统,根据攻击发生的位置对攻击进行分类. 从监控器的角度出发,若攻击者篡改监控器接收的信息,则称为输入攻击;若攻击者篡改监控器发布的指令信息,则称为输出攻击;若一个系统既遭受输入攻击又遭受输出攻击,则称该系统遭受输入输出攻击. 另外,可以对输入、输出攻击进一步分类. 文献[47]将传感器与监控器相连的信道称为传感器信道,将执行器与监控器相连的信道称为执行器信道. 输入攻击可以进一步分为传感器攻击和传感器信道攻击两种,输出攻击可以进一步分为执行器攻击和执行器信道攻击两种. 攻击分类示意图见图2.

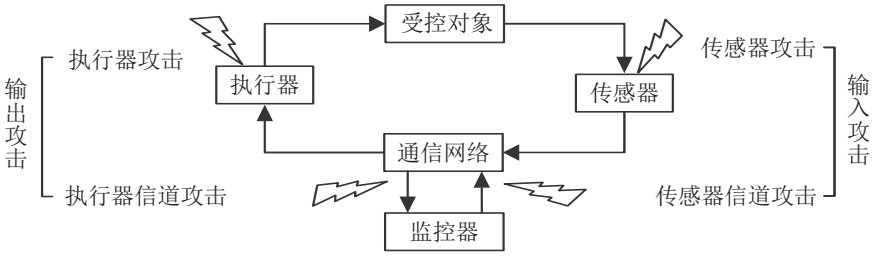

图 2　CPS攻击分类示意图

1.1　输入攻击

输入攻击主要包括传感器攻击和传感器信道攻击. 传感器攻击指攻击者可以直接对易受攻击的传感器的读数进行修改,如插入未发生的虚拟事件、删除已发生的真实事件或对已发生的事件进行替换;传感器信道攻击是指攻击者会对传感器与监控器相连的通信信道中传输的信息进行插入、删除或替换操作. 遭受输入攻击的闭环受控系统模型如图3所示. 模型中:G为受控对象;S为G的监控器,对其行为进行限制;E为G的事件集,表示由E中事件组成的有限长度事件序列集,包括空字符串ε,传感器可观事件集用E_o建模表示,$E_o \subseteq E$;从集合E映射到E_o的投影P_o表示监控器通过传感器观察系统G的部分事件(可观事件),即用P_o表示监控器对受控对象的

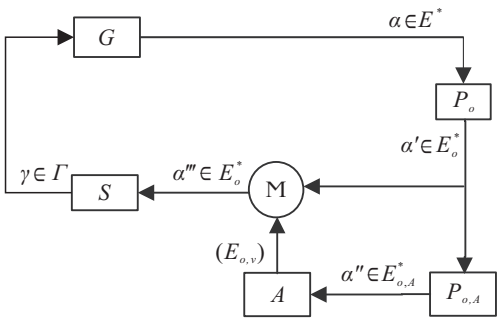

图 3　遭受输入攻击的闭环受控系统

观察函数; A 为攻击者,攻击者可观测事件集用 $E_{o,A}$ 建模表示, $E_{o,A} \subseteq E_o$; 从集合 E_o 映射到 $E_{o,A}$ 的投影 $P_{o,A}$ 表示攻击者的观察函数;攻击者 A 仅可访问受控系统中脆弱的传感器或传感器通道,用 $E_{o,v} \subseteq E_o$ 表示 A 可操作的可观事件集; "M" 为一个概念操作,表示攻击者 A 会对传输的事件序列进行修改,即对属于集合 $E_{o,v}$ 中的事件进行修改,通过对可操作的事件进行如插入、删除或替换等操作,将真实的可观序列 α' 修改为 α''',监控器将根据观察到的事件序列 α''' 向执行器发布控制指令 γ.

文献[48]研究传感器插入攻击、擦除攻击的入侵检测与防御策略的设计方法. 对于传感器插入攻击,为了使监控器不易察觉攻击者的存在,入侵者只能插入当前状态下监控器允许发生的事件,而对于传感器擦除攻击,攻击者可以在任意时刻对传感器收集的可观事件进行删除操作.

文献[49]研究遭受攻击系统的鲁棒性监控器设计方法. 文献[50]研究遭受攻击的系统存在无闭塞监控器的可判定性(decidability)问题. 二者都是针对同一类型的传感器数据欺骗攻击进行研究,即有界传感器替换攻击(attacks with bounded sensor reading alternations, ABSRA). 在ABSRA场景下,攻击者对于监控器的结构已知且能够窃取所有可观的传感器读数,并将一个字符修改为一个有限长度的字符串.

文献[51]从攻击者角度考虑CPS监控层传感器欺骗攻击的攻击策略设计问题. 文献[52]研究随机离散事件系统的传感器攻击下最优攻击策略的设计问题. 文献[53]研究如何合成对于传感器欺骗攻击具有鲁棒性的监控器. 虽然与文献[49-50]一样,文献[51-53]也是针对传感器欺骗攻击的攻击策略的设计以及鲁棒性监控器的合成进行研究,但与文献[49-50]中所有可观事件都会被攻击的情况不同,文献[51-53]定义了易受攻击事件集合,该集合是系统可观事件集的一个子集,这意味着系统中并不是所有可观事件都会被入侵者攻击,入侵者仅能任意插入或删除属于易受攻击事件集的传感器事件. 文献[51-53]基于攻击者对系统模型已知且与监控器有着相同可观事件集的假设条件,攻击者通过对易受攻击事件的插入或删除,达到在不被监控器发现的情况下使系统到达不安全状态的目的,进而对系统造成损害.

文献[54]研究了传感器信道攻击下鲁棒性监控器存在的条件. 该研究考虑攻击者能够从传感器输出序列中插入、删除或替换某些传感器数据. 与之前工作明确知道系统遭受哪个攻击函数作用相比,文献[54]并不知道系统正在遭受哪个攻击函数的作用. 准确地说,文献[54]假设已知一个所有可能作用的攻击函数的集合,并且假设系统只遭受该集合中一个攻击函数作用,但并不知道是哪一个攻击函数. 在文献[54]多攻击函数的基础上,文献[55]考虑了两种新型攻击的检测问题,即恒定攻击和转换攻击. 恒定攻击是指攻击者仅仅通过使用一个攻击函数便能达到破坏系统的目的,而转换攻击是指系统存在多个攻击函数,在不同阶段攻击者使用的攻击函数不同. 换言之,在不同状态下攻击者可以随意进行攻击函数的切换. 尽管文献[54]也存在多个攻击函数,但攻击者并不能进行攻击函数的转换.

1.2 输出攻击

输出攻击主要包括执行器攻击和执行器信道攻击. 执行器攻击指攻击者可以直接对易受攻击的执行器事件的使能性进行修改,例如禁止监控器原本使能事件的发生或使能监控器原本禁止发生的事件;执行器信道攻击是指攻击者会对监控器与执行器相连的通信信道中传输的执行器指令进行修改.

遭受输出攻击的闭环受控系统模型如图4所示. 受控对象 G 在监控器 S 的监控下运行,执行器可控事件集用 E_c 建模表示, $E_c \subseteq E_o$. 另外, A 表示的攻击者只能访问受控系统中脆弱的执行器或执行器信道,用 $E_{c,v} \subseteq E_c$ 表示 A 可操作的可控事件. "M" 是一个概念性操作,代表攻击者 A 能够对属于集合 $E_{c,v}$ 中事件的使能性进行修改,将监控器发出的控制指令 γ 修改为 γ'. 例如,攻击者 A 能将监控器控制指令"禁止某一事件的发生"修改为"允许该事件的发生",此时受控对象 G 将执行由攻击者修改过的指令. 需要注意的是,在很多研究工作中[48,56],攻击者和监控器对受控对象有相同的观察能力,即 $E_o = E_{o,A}$,但也有部分工作[57-59]二者并不相同,即 $E_o \neq E_{o,A}$. 准确来说,Lin等[57-59]考虑攻击者只能够观察到系统的部分可观事件.

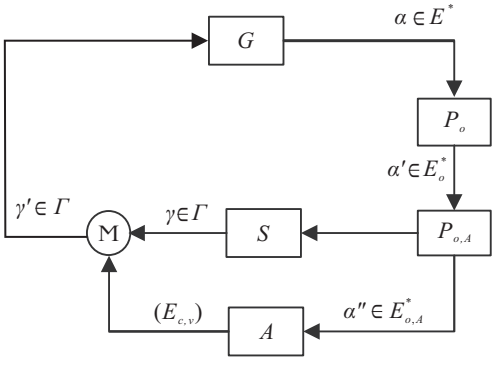

图4 遭受输出攻击的闭环受控系统

执行器攻击和执行器信道攻击均可分为执行器使能攻击和禁用攻击. 执行器使能攻击是指攻击者使能监控器禁止发生的事件,而执行器禁用攻击是指攻击者禁止监控器允许发生的事件. 可见,执行器禁用攻击只是对系统行为进行进一步的限制,仅仅影响系统行为许可性,并不会引起安全问题(即并不会使系统进入监控器不允许进入的状态). 因此,从系统安全角度考虑,更多研究工作关注执行器使能攻击.

文献[48,56]首先在离散事件系统框架下对CPS执行器攻击的检测及防御问题进行研究. 文中假设攻击者已知系统模型且可以观察到系统所有可观事件的发生,但只可以修改易受攻击的执行器事件的使能性,并且可以在任意时刻对系统发起攻击,将禁止某一事件发生的指令修改为允许该事件发生的指令.

文献[57-59]所研究的执行器攻击与文献[48,56]的主要区别在于攻击者可观察的事件集不同. 后者系统事件对于攻击者完全可观,前者系统事件对于攻击者并不完全可观,即攻击者只能观察到系统部分事件的发生. 此外,前者中的攻击者虽然能够观察到监控器向执行器发送的每一个控制指令,但只能对部分控制指令进行修改.

1.3　输入输出攻击

输入输出攻击是指由输入攻击和输出攻击组合而成的攻击,遭受输入输出攻击的闭环受控系统模型如图5所示,它可以被看作图3与图4两个模型的合成. 这里有两个“M”,从右向左分别代表输入攻击和输出攻击,攻击者可以将传感器产生的可观序列α'修改为α''',将监控器发布的控制指令γ修改为γ'. 现有文献中提及的输入输出攻击有“传感器执行器攻击”和“通信信道攻击”. “传感器执行器攻击”是指攻击者可以同时入侵系统脆弱的传感器与脆弱的执行器,换言之,传感器执行器攻击是传感器攻击与执行器攻击的结合; “通信信道攻击”是指攻击者可以攻击传感器与监控器相连的信道和监控器与执行器相连的通信信道,换言之,通信信道攻击是传感器信道攻击与执行器信道攻击的结合.

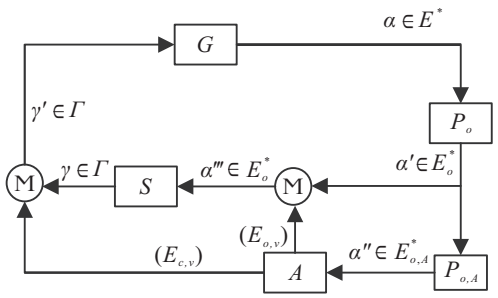

图 5　遭受输入输出攻击的闭环受控系统

文献[47,60-62]针对“中间人攻击”的检测与防御问题进行研究. “中间人攻击”是指攻击者既能入侵传感器信道也能对执行器信道发起攻击. 文献[61]假设系统存在多条传感器信道和执行器信道,但只有某一条或几条传感器信道/执行器信道容易遭受攻击的入侵. 入侵者能够隐藏、插入或替换由传感器收集的受控对象中发生的事件信息,也能够通过攻击执行器来修改监控器发布给执行器的控制指令,进而达到使系统到达不安全状态的目的.

文献[47, 60-61]只考虑了一条或几条传感器/执行器信道可能被攻击的情况. 然而通信网络一旦被入侵,通常意味着所有传感器信道和执行器信道都面临被攻击的风险. 文献[63]考虑了所有通信信道都会被攻击的情况,基于Petri网模型,提出一种检测所有传感器和执行器信道是否遭受隐蔽攻击和重放攻击的方法. 重放攻击是指攻击者拦截并重新发送该传感器数据给监控器,攻击者不需要系统的先验知识,只需要收集传感器信道中传输的受控对象信息,并在合适的时间将传感器发生序列进行替换即可. 隐蔽攻击要求攻击者对于系统运行状况完全已知,攻击者通过访问通信信道中传输的信息复现一个与真实的受控对象有相同行为的虚拟受控对象模型. 在虚拟的受控对象模型建立后,将其与监控器相连,而真实的受控对象则由攻击者进行操纵. 由于虚拟的受控对象完全复刻了系统本身受控对象的行为,监控器不会发现攻击者的存在.

Zhang等[64]研究传感器攻击和执行器攻击同时入侵系统时攻击策略的设计问题. 虽然文献[47-48, 60-61]也考虑了两种攻击——传感器信道攻击和执行器信道攻击同时入侵系统的问题,但是并未考虑攻击的隐蔽性问题. 在Zhang等[64]的研究中,攻击者既能插入未发生的传感器事件,也能删除已发生的传感器事件,还可以使能监控器禁止发生的事件,其设计的攻击在对系统造成伤害之前不会被系统监控器发现.

本节介绍了当前学者们研究的多种攻击类型. 需要说明的是,实际系统遭受的攻击不仅仅局限于上文提到的这些类型,现实中仍有一部分攻击未被学者们研究过,其主要原因有两点: 第一,学者在研究过程中由于实践的局限性,未接触过某一类型的攻击,但该类型的攻击却是真实存在的; 第二,某一类型的攻击过于复杂,其研究过于艰难.

本文在此介绍一种未被研究过的攻击类型,即在这类攻击中系统不同状态下遭受的攻击函数不

同. 例如,智能电网系统白天和晚上遭受攻击的可能性不同. 白天大型企业、工厂的用电设备多、负荷变动量大,而且大多数都是感性负荷,消耗的无用功较多,因此电压波动范围容易超出国家规定标准,此时传感器容易被入侵者攻击;晚上随着工厂、企业工人下班,用电设备的使用减少,感性负荷波动范围随之变小,电压始终在国家标准所允许的范围内波动,此时传感器不容易被攻击. 换言之,在不同的时间段,传感器遭受攻击的概率不同. 对于离散事件系统框架下的攻击模型而言,这意味着系统不同状态遭受的攻击函数不同. 可以将系统状态分为两部分,一部分状态容易遭受网络攻击,而另一部分状态不会遭受网络攻击. 此外,也可以考虑在不同状态下,同一事件遭受的攻击函数不同的场景.

2 攻击设计、攻击检测与防御及鲁棒性监控器设计

对于信息物理系统安全问题的研究主要从3个角度出发:攻击策略的设计、攻击的检测与防御以及攻击鲁棒性监控器设计. 攻击策略的设计是指从攻击者的角度出发对攻击行为进行设计,即针对不同类型的攻击,研究如何设计攻击策略使得系统进入不安全状态或不期望的状态. 攻击的检测与防御以及鲁棒性监控器的设计是从防御者角度出发,攻击检测与防御一般指在系统运行时实时检测是否有攻击入侵系统并在检测到攻击后采取防御手段;攻击鲁棒性监控器的设计一般指离线设计一种对攻击具有鲁棒性的监控器.

下文分别从攻击策略的设计、入侵检测与防御、鲁棒性监控器的设计3方面对目前离散事件系统框架下的信息物理系统攻击问题的研究工作进行介绍. 为了便于阅读,表1对下文即将重点介绍的研究工作进行了分类.

2.1 攻击策略的设计

攻击者的目的只有一个,即如何能将系统带入不安全的状态进而对系统造成破坏,研究攻击策略的设计主要是为了之后更好地研究应对该类型攻击的防御措施. 若攻击者想要对系统造成危害,则必定满足文献[49]所提出的几个条件:1)攻击后系统产生的观察序列是系统在监控器作用下产生的观察序列的子集,即攻击具有隐蔽性;2)攻击者不能禁止不可控事件的发生;3)攻击者最后一定会促使受控对象生成监控器所禁止发生的序列,即攻击具有破坏性;4)考虑到系统存在不可观事件,闭环系统的输出序列与真实发生的序列都应是监控器作用下的闭环系统产生的序列.

Góes等[65]针对信息物理系统的监控层提出一种欺骗攻击的模型,研究了如何合成一个隐蔽型欺骗攻击使得系统进入不期望的状态,同时引入一种名为IDA(insertion-deletion attack)的二叉离散结构,该结构能同时描述系统的真实状态和监控器观察到的系统状态. IDA包含了攻击者对于易受攻击的可观事件所有可能的处理结果,即在任一状态下对易受攻击事件执行插入还是删除操作. 一旦IDA构造成功,便可以解决隐蔽型欺骗攻击者的合成问题.

文献[51]对文献[65]的工作进行补充,进一步研究了传感器欺骗攻击下攻击策略的设计问题. Goés等[51]考虑了3种攻击情景:1)在攻击者对传感器读数完成修改之前,受控对象不会执行任何事件;2)攻击者只更改有限个传感器读数时,受控对象不会进入到坏的状态;3)系统可以在任意时刻中断攻击者对于系统传感器读数的修改. 在3种攻击情境下,提出一种名为AIDA (all insertion- deletion attack structure)的结构对攻击后的闭环系统进行建模. AIDA包含了所有攻击者可能对系统执行的操作,在此基础上,构造ISDA (interruptible stealthy deceptive attack)和USDA (unbounded stealthy deceptive attack)的隐蔽型攻击结构.

文献[49]针对离散事件系统框架下的信息物理系统提出了一种方法用于设计有界传感器替换攻击的攻击策略. 由于攻击具有隐蔽性,监控器并不能检测到攻击的存在,监控器认为系统处于正常运行的状态,即系统处于安全状态,而攻击者的目的是在不被监控器发现的情况下,引导系统进入不安全状态. 该研究工作的挑战在于如何“欺骗”监控器,使其认为系统是正常运行的. 文献[49]的解决办法是用监控器发布的指令对系统实行攻击,即攻击后所生成的语

表1 离散事件系统框架下信息物理系统攻击相关研究工作分类

	攻击策略的设计	入侵检测与防御	鲁棒性监控器的设计
输入攻击	文献[49,51-52,65]	文献[55]	文献[53-54]
输出攻击	文献[57]	文献[56]	文献[58-59,68]
输入输出攻击	文献[64,66]	文献[48,60-61,63,67]	文献[69-70]

言是系统在监控器作用下生成的语言的子集. 文献[49]提出了系统可攻击性和ABSRA的概念,并证明了只要受控对象和监控器都可以用有限状态自动机表示,那么对系统行为限制最小的ABSRA存在,并提出一种算法用于合成最优的ABSRA.

Lin等[57]针对信息物理系统隐蔽型执行器攻击的合成问题进行研究,给出系统可攻击性的定义,并给出了执行器攻击者存在的条件和最优执行器攻击者存在的条件,最后提出一种由Moore自动机表示的最优执行器攻击合成算法.

文献[66]探究了信息物理系统传感器攻击与执行器攻击不可检测的条件. 针对文献[48]所提出的四种攻击——传感器插入/擦除攻击,执行器使能/禁用攻击,文献[66]从语言角度考虑了能够对系统造成破坏并且不被系统监控器发现的攻击者所需满足的条件. 基于系统的某个事件既为易受攻击的传感器事件又为易受攻击的执行器事件的假设,该文献建立了攻击后的系统模型,进而研究了攻击不可检测的条件. 简单来讲,给定系统的一个规范语言,该条件要求攻击语言是其子集且攻击语言与系统的规范语言的观察值相同,此外,攻击语言是可控的.

文献[64]针对信息物理系统的传感器攻击与执行器攻击的攻击器合成问题进行研究. 攻击者能够对传感器读数进行插入或删除操作,也能够启用被监控器禁用的可控事件. 攻击者的目的是在不被监控器发现的情况下引导系统进入不安全状态. 文献[64]首先提出一种算法用于构造攻击作用后的受控对象和攻击作用后的监控器,其次将二者同步合成攻击结构. 该攻击结构能够同时表示受控对象真实的状态和监控器所观察到的受控对象所处于的状态. 初次合成的攻击结构中包含一些可能会将攻击者暴露的状态,例如虽然受控对象发生了某个事件,但监控器的观察结果并未改变,因此需要对攻击结构中的某些状态进行删除操作. 在攻击结构的筛选过程中,需要删除会暴露攻击者的状态,进而确定最终的具有隐蔽性的攻击结构,即攻击者所采用的攻击策略.

2.2　入侵检测与防御

本节主要介绍目前针对信息物理系统的攻击检测与防御的研究工作. 攻击的检测与防御是指如何在线检测系统是否遭受了攻击的入侵,并在检测到攻击后采取一定的防御措施以阻止攻击对系统造成进一步伤害.

针对闭环系统下执行器使能攻击的检测与防御问题,Carvalho等[56]提出了执行器使能攻击下的系统模型及检测防御策略,该策略在线检测攻击并在攻击被检测到后禁止所有的可控事件以保证系统安全. 该工作定义了“执行器使能安全可控性”这一性质,若系统是执行器使能安全可控的,则在检测到执行器使能攻击后,监控器能阻止受控对象到达不安全状态,否则监控器无法阻止攻击者达成目的. 该工作提出了一种算法用于验证系统是否是执行器使能安全可控的. 若系统是安全可控的,则入侵检测模块能在受控对象到达不安全状态之前检测到攻击,且监控器能够通过禁止所有的可控事件阻止系统到达不安全状态.

文献[48]对文献[56]的研究工作进行了扩展,不仅针对执行器使能攻击的检测与防御进行研究,还对执行器禁用攻击、传感器插入攻击、传感器擦除攻击的检测与防御进行研究. 对于传感器擦除攻击与执行器使能攻击,攻击者能在任意时刻对系统发起攻击;而对于传感器插入攻击,攻击者只能插入当前状态下监控器允许发生的事件. 图6描述了包含检测模块的遭受攻击的闭环受控系统模型. 这里,攻击者A与监控器S对受控对象G有相同的观察函数P_o. “$+/-$”代表4种类型的攻击:执行器使能攻击、执行器禁用攻击、传感器擦除攻击和传感器插入攻击. 对于传感器擦除攻击,攻击者能删除已发生的属于集合$E_{o,v}$中的可观事件,监控器S因此不会观察到该事件的发生;对于传感器插入攻击,攻击者能插入未发生的属于$E_{o,v}$中的事件,监控器S因此除了会观察到真实的已发生事件外,还会观察到由攻击者插入的虚拟事件. 总体而言,攻击者可以修改传感器读数进而影响监控器S对受控对象行为的观测. 类似地,攻击者也可以通过改变执行器的使能事件进而影响应用于受控对象G的实际控制操作. G_D是检测攻击的模块,主要负责监视监控器的输入,并在检测到攻击后通知监控器使其转换到安全模式. 文献[48]将“执行器使能安全可控性”进一步扩展为同样适用于传感器插

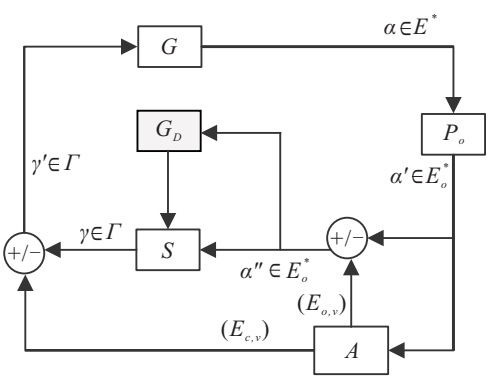

图6　包含入侵检测模块的受攻击的闭环受控系统

入以及擦除攻击的“通用安全可控性”,并提出一种算法对该性质进行验证.

文献[66]基于自动机模型对攻击后系统进行建模,提出了一种方法用于检测攻击并避免故障,同时研究了系统满足攻击可检测性(attack detectability)和故障可避免性(failure avoidability)的条件,并对二者之间的关系进行了探究.

Lima等[47]针对信息物理系统中间人攻击的入侵检测以及如何阻止中间人攻击对系统造成危害的问题进行了研究. 与文献[48]只考虑传感器信道或执行器信道中的网络攻击不同,前者同时考虑了两种通信信道的攻击检测与防御问题,提出一种防御策略,设计入侵检测模块以实时监测系统. 首先,对攻击下的受控对象以及监控器采用自动机进行建模,对于传感器信道的攻击,对受控对象的自动机模型进行修改,在易受攻击事件不能发生的状态下增加该事件的自环,在易受攻击事件原本就能发生的状态下增加一个名为“ε”的平行变迁;对于执行器信道攻击,在监控器自动机模型中易受攻击事件不能发生的状态下增加该脆弱事件的自环. 然后提出攻击下安全可控性的定义,以检测攻击并阻止系统到达不安全状态,并提出一种算法用于验证该性质. 最后说明如何构造入侵检测模块以实现对攻击的监测,并在检测到攻击后立即禁用系统所有的可控事件以阻止攻击者达成目的.

在文献[47, 56]的研究中,一旦检测到攻击,安全模块立即禁用所有的可控事件使攻击不对系统造成危害. 然而,当攻击的效率不高或攻击危害性不强时,若在此时立即禁用所有的可控事件则可能造成不必要的经济损失,尤其对于某些重要的生产周期而言,它们的突然中断会造成严重的后果. Lima等[61]旨在设计一个安全模块,该模块仅在攻击会使系统进入不安全状态时才禁止系统的可控事件,不会与已有的闭环系统监控器发生任何冲突,也不会在攻击没有入侵系统时对系统行为做出任何改变. 为此,提出了可检测网络攻击安全性与不可检测网络攻击安全性的定义,给出系统满足这两个性质的充要条件,并指出在某些情况下即使攻击是隐蔽的,该模块也能阻止攻击将系统带入不安全状态.

受文献[67]关于隐蔽攻击和零动态攻击的研究的启发,Fritz等[63]针对信息物理系统“重放攻击”和“隐蔽攻击”的检测问题进行研究. 首先构建了在离散事件系统框架下重放攻击和隐蔽攻击的攻击模型,并提出一种攻击检测方法,其基本思想是通过引入置换矩阵改变受控对象的输入和输出行为,并将监控器观察到的受控对象行为与预期行为进行比较以实现攻击检测的目的. 以输出置换矩阵为例,介绍了3种允许输出信号在输出向量中位置可以互换的情况,并通过使用随机数生成器使得排列矩阵的间隔变得不规则,进而更好地检测到攻击. 与以往基于自动机的研究不同,文献[63]是基于Petri网的输入输出矩阵进行研究的.

文献[55]针对信息物理系统中多种攻击的检测问题进行研究,采用自动机分别对恒定攻击和转换攻击作用下的系统进行建模,提出了一个用于诊断系统是否遭受攻击并判断攻击者采用哪种攻击函数的算法.

2.3 鲁棒性监控器的设计

本节主要介绍不同网络攻击下鲁棒性监控器设计的研究现状. 设计鲁棒性监控器一般是指在离线情况下设计一个无论系统是否遭受攻击都能保证系统正常安全运行的监控器. 相较于攻击的检测与防御策略,鲁棒性监控器一旦设计完成,其在系统控制阶段仅需要较少量的在线计算量.

Thorsley等[68]针对离散事件系统的攻击检测问题进行研究,设计了在正常情况和在系统遭受攻击的情况下都能满足系统给定规范的监控器. Wakaiki等[54]考虑了部分可观可控系统存在多个攻击者情况下监控器的设计问题,攻击者通过篡改传感器读数使监控器允许系统生成规范语言之外的序列,而防御者的任务是设计一个能够抵御任一攻击的防御策略,在假设监控器不知道哪一个攻击者对系统发动攻击的条件下,给出该防御策略存在的充要条件,即系统期望语言除了满足可控性外,还要满足新定义的可观性. 此外,该文献针对能删除或插入传感器输出的攻击给出一种算法生成能够抵御该攻击的监控器.

针对ABSRA攻击,文献[49]提出一种鲁棒性监控器合成算法,对于任何ABSRA攻击,该受控系统都不会被带入不安全状态. 文献[50]针对ABSRA提出了非阻塞鲁棒性监控器存在的条件,并给出了一种算法用于合成鲁棒性监控器. 文献[54]研究了攻击函数已给定情况下鲁棒性监控器的设计问题. 文献[53]针对部分可观的离散事件系统,研究了如何合成对传感器攻击具有鲁棒性的监控器. 具体而言,首先对于部分可观系统建立受攻击的受控系统模型,该模型能够同时捕获未遭受攻击时受控对象中事件真实的发

生情况,同时又能捕获到监控器认为受控对象所处的状态;其次提出一种监控方法使得攻击后的系统在满足一定规范情况下永远不会到达不安全状态,即不存在任何传感器攻击能够对系统造成危害. 文献[49]计算监控器的方法利用三次指数计算复杂度,文献[53]利用一次指数计算复杂度.

Zhu等[59]针对文献[57]提出的执行器攻击,研究了监控器合成的相关问题. 在Zhu等的研究中,与合成一个对攻击具有鲁棒性监控器的想法不同,其通过混淆原来的监控器达到阻止攻击对系统造成损害的目的. 系统防御者无法干预攻击者观察到的系统的执行情况,也无法改变监控器发布的执行器指令,但是可以对监控器发布的指令进行混淆,以干扰攻击者观察到的监控器发布的控制指令. 这样一来,攻击者虽然得到了监控器指令,但无法根据观察到的监控器指令推断出系统所处的真实状态,进而达到保护系统的目的. 文献[58]进一步研究了能够抵御执行器攻击(执行器启用攻击和执行器禁用攻击)的有界弹性监控器的设计问题. 他们将监控器合成问题转化为"∀∃二阶合成问题",即对于任意执行器攻击,是否存在一个监控器使得攻击后的受控系统满足安全规范,并将"∀∃二阶合成问题"进一步转化为布尔可满足性问题(boolean satisfiability problem, SAT)下的量化布尔公式问题(quantified boolean formula, QBF)进行研究.

Wang等[69]考虑了攻击只发生在传感器、只发生在执行器和同时发生在传感器、执行器3种情况下,鲁棒性监控器的构建问题. 从数学意义上而言,攻击破坏了系统的输入与输出语言之间的规则关系,为了更好地对抗攻击并保证监控器的鲁棒性,采用有穷状态转换器(finite state transducer, FST)对系统进行建模分析. FTS建模的监控器允许攻击者对信息进行修改,针对攻击可能发生的3种位置,提出了可控性以及弱可控性的定义,并分别针对每一种攻击提出一种算法以合成对攻击具有鲁棒性的监控器. 文献[70]采用FST研究了对于通信网络攻击具有鲁棒性的监控器的合成问题. 首先计算系统期望语言的最大可控子语言,然后提出一种算法用于计算在没有对通信信道施加任何限制时能够抵御攻击所带来伤害的监控器;其次在考虑到通信信道中传输信息数量受限,监控器对通信网络进行间歇性访问的情况下,设计出对攻击具有鲁棒性的监控器.

文献[71-73]研究了有不确定观察值的系统非阻塞鲁棒性监控器的设计问题. 其研究模型与遭受输入攻击的离散事件系统模型相似,因此该研究工作也可以应用于系统存在攻击的情况.

针对前文所提及的一类未被研究的攻击类型,即不同状态下,对于同一事件攻击者所采用的攻击函数不同的问题,未来可以研究攻击策略的设计、攻击的检测与防御以及鲁棒性监控器的设计问题. 首先从攻击者的角度出发,针对这类攻击进行攻击策略的研究,即如何构造攻击结构,使其在不被监控器发现的情况下,诱导系统进入不安全状态;然后针对该攻击结构研究如何在线检测攻击以及如何设计鲁棒性监控器.

3　总结与展望

本文对离散事件系统框架下信息物理系统攻击的相关问题进行综述. 首先简要介绍了信息物理系统的相关概念及其发展历程;然后根据攻击发生位置的不同对现有的攻击类型进行分类;最后从攻击策略的设计、入侵检测与防御以及鲁棒性监控器的设计3个方面对信息物理系统安全问题的研究工作进行回顾.

现有工作只针对一部分类型的攻击进行了研究,未来有望在离散事件系统框架下研究更多类型的攻击. 例如,针对本文介绍的不同状态下攻击函数不同这一攻击类型,未来可以研究该类型攻击策略的设计、入侵检测与防御以及鲁棒性监控器的设计. 此外,离散事件系统框架下活性问题的研究十分重要,而目前如何在系统遭受攻击时保持系统活性的研究成果相对匮乏. 因此,也可以围绕受攻击的信息物理系统的活性问题展开研究.

参考文献(References)

[1] Baheti R, Gill H. Cyber-physical systems[J]. The Impact of Control Technology, 2011, 12: 161-166.

[2] 李洪阳, 魏慕恒, 黄洁, 等. 信息物理系统技术综述[J]. 自动化学报, 2019, 45(1): 37-50.
(Li H Y, Wei M H, Huang J, et al. Survey on cyber-physical ssystems[J]. Acta Automatica Sinica, 2019, 45(1): 37-50.)

[3] Khaitan S K, McCalley J D. Design techniques and applications of cyberphysical systems: A survey[J]. IEEE Systems Journal, 2015, 9(2): 350-365.

[4] Technology PCOAOSA. Leadership under challenge: Information technology R&D in a competitive world. An assessment of the federal networking and information technology R&D program[Z]. 2011.

[5] Kagermann H, Helbig J, Hellinger A, et al.

Recommendations for implementing the strategic initiative INDUSTRIE 4.0: Securing the future of German manufacturing industry; final report of the industrie 4.0 working group[M]. Berlin: Forschungsunion, 2013: 1-10.

[6] 国家制造强国建设战略咨询委员会.《中国制造2025蓝皮书(2017)》[J]. 理论与当代, 2017(9): 45.

[7] Yu X H, Xue Y S. Smart grids: A cyber-physical systems perspective[J]. Proceedings of the IEEE, 2016, 104(5): 1058-1070.

[8] Cassandras C G. Smart cities as cyber-physical social systems[J]. Engineering, 2016, 2: 156-158.

[9] Lee I, Sokolsky O, Chen J S, et al. Challenges and research directions in medical cyber-physical systems[J]. Proceedings of the IEEE, 2012, 100(1): 75-90.

[10] Jiang Z H, Pajic M, Mangharam R. Cyber-physical modeling of implantable cardiac medical devices[J]. Proceedings of the IEEE, 2012, 100(1): 122-137.

[11] Narayanan S N, Khanna K, Panigrahi B K, et al. Security in smart cyber-physical systems: A case study on smart grids and smart cars[M]. Amsterdam: Elsevier, 2019: 147-163.

[12] 原豪男, 郭戈. 交通信息物理系统中的车辆协同运行优化调度[J]. 自动化学报, 2019, 45(1): 143-152.
(Yuan H N, Guo G. Vehicle cooperative optimization scheduling in transportation cyber physical systems[J]. Acta Automatica Sinica, 2019, 45(1): 143-152.)

[13] 夏元清, 闫策, 王笑京, 等. 智能交通信息物理融合云控制系统[J]. 自动化学报, 2019, 45(1): 132-142.
(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.)

[14] Lu C Y, Saifullah A, Li B, et al. Real-time wireless sensor-actuator networks for industrial cyber-physical systems[J]. Proceedings of the IEEE, 2016, 104(5): 1013-1024.

[15] Ramadge P J, Wonham W M. Supervisory control of a class of discrete event processes[J]. Aualysis and Optimizization of Systems, 1984: 475-498.

[16] Cao L W, Jiang X N, Zhao Y M, et al. A survey of network attacks on cyber-physical systems[J]. IEEE Access, 2020, 8: 44219-44227.

[17] Rashidinejad A, Wetzels B, Reniers M, et al. Supervisory control of discrete-event systems under attacks: An overview and outlook[C]. The 18th European Control Conference (ECC). Naples, 2019: 1732-1739.

[18] Yin X, Li S. Recent advances on formal methods for safety and security of cyber-physical systems[J]. Control Theory and Technology, 2020, 18: 459-461.

[19] Dibaji S M, Pirani M, Flamholz D B, et al. A systems and control perspective of CPS security[J]. Annual Reviews in Control, 2019, 47: 394-411.

[20] 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.

[21] 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[J]. 自动化学报, 2019, 45(1): 5-24.
(Liu T, Tian J, Wang J Z, et al. Integrated security threats and defense of cyber-physical systems[J]. Acta Automatica Sinica, 2019, 45(1): 5-24.)

[22] Pasqualetti F, Dörfler F, Bullo F. Attack detection and identification in cyber-physical systems[J]. IEEE Transactions on Automatic Control, 2013, 58(11): 2715-2729.

[23] 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.

[24] Humayed A, Lin J, Li F, et al. Cyber-physical systems security—A survey[J]. IEEE Internet of Things Journal, 2017, 4: 1802-1831.

[25] Giraldo J, Urbina D, Cardenas A, et al. A survey of physics-based attack detection in cyber-physical systems[J]. ACM Computing Surveys, 2018, 51(4): 1-36.

[26] Cardenas A, Amin S, Sinopoli B, et al. Challenges for securing cyber physical systems[J]. First Workshop on Cyber Physical Systems Security, DOI: 10.1109/SIORC.2008.25.

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

[28] Long M, Wu C H, Hung J Y. Denial of service attacks on network-based control systems: Impact and mitigation[J]. IEEE Transactions on Industrial Informatics, 2005, 1(2): 85-96.

[29] Befekadu G K, Gupta V, Antsaklis P J. Risk-sensitive control under Markov modulated denial-of-service (DoS) attack strategies[J]. IEEE Transactions on Automatic Control, 2015, 60(2): 3299-3304.

[30] Pang Z H, Liu G, Dong Z. Secure networked control systems under denial of service attacks[J]. IFAC Proceedings Volumes, 2011, 44(1): 8908-8913.

[31] Zhang X M, Han Q L, Ge X H, et al. Resilient control design based on a sampled-data model for a class of networked control systems under denial-of-service attacks[J]. IEEE Transactions on Cybernetics, 2020, 50(8): 3616-3626.

[32] 汪慕峰, 胥布工. DoS干扰攻击下的信息物理系统状态反馈稳定[J]. 控制与决策, 2019, 34(8): 1681-1687.
(Wang M F, Xu B G. State feedback stabilization of cyber-physical system under DoS jamming attacks[J]. Control and Decision, 2019, 34(8): 1681-1687.)

[33] 孙洪涛, 彭晨, 王志文. DoS攻击下的信息物理系统事件触发预测控制设计[J]. 控制与决策, 2019, 34(11): 2303-2309.
(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.)

[34] 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[J]. 自动化学报, 2019, 45(1): 110-119.
(Yang F S, Wang J, Pan Q, et al. Resilient event-triggered control of grid cyber-physical systems against cyber attack[J]. Acta Automatica Sinica, 2019, 45(1): 110-119.)

[35] Ding D R, Wang Z D, Han Q L, et al. Security control for discrete-time stochastic nonlinear systems subject to deception attacks[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2016, 48(5): 779-789.

[36] Ding D R, Wang Z D, Ho D W, et al. Observer-based event-triggering consensus control for multiagent systems with lossy sensors and cyber-attacks[J]. IEEE Transactions on Cybernetics, 2016, 47(8): 1936-1947.

[37] Amin S, Litrico X, Sastry S, et al. Cyber security of water SCADA systems—Part I: Analysis and experimentation of stealthy deception attacks[J]. IEEE Transactions on Control Systems Technology, 2012, 21(5): 1963-1970.

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

[39] 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.

[40] Lee P, Clark A, Bushnell L, et al. A passivity framework for modeling and mitigating wormhole attacks on networked control systems[J]. IEEE Transactions on Automatic Control, 2014, 59(12): 3224-3237.

[41] Sanchez H S, Rotondo D, Escobet T, et al. Detection of replay attacks in cyber-physical systems using a frequency-based signature[J]. Journal of the Franklin Institute, 2019, 356(5): 2798-2824.

[42] Hosseinzadeh M, Sinopoli B, Garone E. Feasibility and detection of replay attack in networked constrained cyber-physical systems[C]. The 57th Annual Allerton Conference on Communication, Control, and Computing (Allerton). Monticello, 2019: 712-717.

[43] Abbadi R E, Jamouli H. Stabilization of cyber physical system exposed to a random replay attack modeled by Markov chains[C]. The 6th International Conference on Control, Decision and Information Technologies (CoDIT). Paris, 2019: 528-533.

[44] 彭大天, 董建敏, 蔡忠闽, 等. 假数据注入攻击下信息物理融合系统的稳定性研究[J]. 自动化学报, 2019, 45(1): 196-205.
(Peng D T, Dong J M, Cai Z M, et al. On the stability of cyber-physical systems under false data injection attacks[J]. Acta Automatica Sinica, 2019, 45(1): 196-205.)

[45] 王琦, 邰伟, 汤奕, 等. 面向电力信息物理系统的虚假数据注入攻击研究综述[J]. 自动化学报, 2019, 45(1): 72-83.
(Wang Q, Tai W, Tang Y, et al. A review on false data injection attack toward cyber-physical power system[J]. Acta Automatica Sinica, 2019, 45(1): 72-83.)

[46] Cassandras C G, Lafortune S. Introduction to discrete event systems[M]. Huwer: Noruell MA, 1999.

[47] Lima P M, Alves M V S, Carvalho L K, et al. Security against network attacks in supervisory control systems[J]. IFAC-PapersOnLine, 2017, 50(1): 12333-12338.

[48] Carvalho L K, Wu Y C, Kwong R, et al. Detection and mitigation of classes of attacks in supervisory control systems[J]. Automatica, 2018, 97: 121-133.

[49] Su R. Supervisor synthesis to thwart cyber attack with bounded sensor reading alterations[J]. Automatica, 2018, 94: 35-44.

[50] Su R. On decidability of existence of nonblocking supervisors resilient to smart sensor attacks[J/OL]. 2020, arXiv: 2009.02626.

[51] Góes R M, Kang E, Kwong R H, et al. Synthesis of sensor deception attacks at the supervisory layer of cyber-physical systems[J]. Automatica, 2020, 121: 109172.

[52] Góes R M, Kwong R, Lafortune S. Synthesis of sensor deception attacks for systems modeled as probabilistic automata[C]. American Control Conference. Philadelphia, 2019: 8814710.

[53] Góes R M, Marchand H, Lafortune S. Towards resilient supervisors against sensor deception attacks[C]. The 58th IEEE Conference on Decision and Control (CDC). Nice, 2019: 5144-5149.

[54] Wakaiki M, Tabuada P, Hespanha J P. Supervisory control of discrete-event systems under attacks[J]. Dynamic Games and Applications, 2019, 9(4): 965-983.

[55] Gao C, Seatzu C, Li Z, et al. Multiple attacks detection on discrete event systems[C]. IEEE International Conference on Systems, Man and Cybernetics (SMC). Bari, 2019: 2352-2357.

[56] Carvalho L K, Wu Y C, Kwong R, et al. Detection and

prevention of actuator enablement attacks in supervisory control systems[C]. The 13th International Workshop on Discrete Event Systems (WODES). Xi'an, 2016: 298-305.

[57] Lin L Y, Thuijsman S, Zhu Y T, et al. Synthesis of supremal successful normal actuator attackers on normal supervisors[C]. American Control Conference (ACC). Philadelphia, 2019: 5614-5619.

[58] Lin L Y, Zhu Y T, Su R. Towards bounded synthesis of resilient supervisors against actuator attacks[J/OL]. 2019, arXiv: 1903.08358.

[59] Zhu Y T, Lin L Y, Su R. Supervisor obfuscation against actuator enablement attack[C]. The 18th European Control Conference (ECC). Naples, 2019: 1811.02932.

[60] Lima P M, Alves M V S, Carvalho L K, et al. Security against communication network attacks of cyber-physical systems[J]. Journal of Control, Automation and Electrical Systems, 2019, 30(1): 125-135.

[61] Lima P M, Carvalho L K, Moreira M V. Detectable and undetectable network attack security of cyber-physical systems[J]. IFAC-PapersOnLine, 2018, 51(7): 179-185.

[62] Comer D. Computer networks and internets[M]. Beijing: Tsinghua University Press, 1998: 35-45.

[63] Fritz R, Zhang P. Modeling and detection of cyber attacks on discrete event systems[J]. IFAC-PapersOnLine, 2018, 51(7): 285-290.

[64] Zhang Q, Seatzu C, Li Z W, et al. A framework for the analysis of supervised discrete event systems under attack[J/OL]. 2020, arXiv: 2005.00212.

[65] Góes R M, Kang E, Kwong R, et al. Stealthy deception attacks for cyber-physical systems[C]. The 56th IEEE Annual Conference on Decision and Control (CDC). Melbourne, 2017: 4224-4230.

[66] Khoumsi A. Sensor and actuator attacks of cyber-physical systems: A study based on supervisory control of discrete event systems[C]. The 8th International Conference on Systems and Control (ICSC). Marrakesh, 2019: 176-182.

[67] Hoehn A, Zhang P. Detection of covert attacks and zero dynamics attacks in cyber-physical systems[C]. 2016 American Control Conference (ACC). Boston, 2016: 302-307.

[68] Thorsley D, Teneketzis D. Intrusion detection in controlled discrete event systems[C]. Proceedings of the 45th IEEE Conference on Decision and Control. San Diego, 2006: 6047-6054.

[69] Wang Y, Pajic M. Supervisory control of discrete event systems in the presence of sensor and actuator attacks[C]. The 58th IEEE Conference on Decision and Control (CDC). Nice, 2019: 5350-5355.

[70] Wang Y, Pajic M. Attack-resilient supervisory control with intermittently secure communication[C]. The 58th IEEE Conference on Decision and Control (CDC). Nice, 2019: 2015-2020.

[71] Xu S, Kumar R. Discrete event control under nondeterministic partial observation[C]. 2009 IEEE International Conference on Automation Science and Engineering. Bangalore, 2009:127-132.

[72] Yin X. Supervisor synthesis for mealy automata with output functions: A model transformation approach[J]. IEEE Transactions on Automatic Control, 2017, 62(5): 2576-2581.

[73] Takai S, Ushio T. Verification of codiagnosability for discrete event systems modeled by mealy automata with nondeterministic output functions[J]. IEEE Transactions on Automatic Control, 2012, 57: 798-804.

作者简介

王寿光(1977−), 男, 教授, 博士, 从事离散事件系统、Petri网理论与应用等研究, E-mail: wsg5000@hotmail.com;

赵玉美(1997−), 女, 硕士生, 从事离散事件系统、Petri网理论与应用的研究, E-mail: zhaoyumei0310@hotmail.com;

尤丹(1991−), 女, 博士生, 从事离散事件系统、Petri网理论与应用的研究, E-mail: youdan000@hotmail.com;

冉宁(1987−), 男, 副教授, 博士, 从事离散事件系统、Petri网理论与应用等研究, E-mail: ranning87@hotmai.com.

(责任编辑：郑晓蕾)