文章编号: 1001-0920(2019)11-2273-04 DOI: 10.13195/j.kzyjc.2019.ZKXY

“信息物理系统理论、方法及应用”专栏序言

郭 戈[1†], 张文安[2], 周 彬[3]

(1. 东北大学 流程工业综合自动化国家重点实验室，沈阳 110004；2. 浙江工业大学 信息工程学院，杭州 310023；3. 哈尔滨工业大学 航天学院, 哈尔滨 150001)

0 引 言

信息物理系统(cyber-physical systems, CPS)是综合计算、通信和物理环境的复杂系统,通过计算、通信和控制技术的有机融合与深度协作,实现大型系统的实时感知、动态控制和信息服务. CPS是传统数字控制系统融合网络通信技术的新一代分布式控制系统,其中的物理系统与信息系统高度融合,信息进程与物理进程可实时交换信息,以可靠、安全和协作的方式操作物理实体. CPS中的信息获取、通信、计算和控制等任务互相关联,其建模、分析和设计为相关领域尤其是控制科学与工程学科带来深刻变革.

CPS技术已广泛应用于医疗及保健系统、智能楼宇、智能电网、智能交通、工业过程等多个领域,成为工业界和学术界的热点研究领域之一,也是许多国家/地区的战略重点研究领域. 2006年美国科学院发布的《美国竞争力计划》,将CPS列为重要研究领域;2007年,美国总统科学技术顾问委员会发布的《挑战下的领先——竞争世界中的信息技术研发》报告,将CPS列在八大关键信息技术首位. 中国政府和学术界从2006年开始也高度重视CPS的重要性,国务院2015年发布的《中国制造2025》规划中重点鼓励研发信息物理系统相关技术.

与传统系统相比,信息物理系统面临着更严峻、更复杂的挑战. CPS结构复杂,任务多样,既涉及数据、信息传输与共享,也涉及能源传输与分配;既涉及离散、连续和随机变量的处理和计算,也涉及事件和逻辑的传递和扩散. 另外,CPS还面临木马攻击、系统漏洞、病毒等威胁,给信息获取、通信、计算和控制带来诸多挑战. 因此,推进CPS领域的研究刻不容缓,具有重要的理论与实际意义. CPS领域重点关注的问题包括:信息物理系统的基本架构及模型,信息获取、处理及传输,智能控制与决策方法,智能计算方法,资源优化调度,内生安全机制,信息安全技术,网络通信协议及QoS(quality of service),接入设备漏洞检测与入侵检测,安全防御与控制,风险评估与安全态势感知,时钟同步及物理实体统一标识,以及在工业、交通、电力、管网、金融、医疗健康等领域的应用.

为了促进CPS相关理论与应用研究,展示我国学者在本领域的最新研究成果,带动我国信息物理系统相关理论研究的深入开展,并希望由此促进交通、能源、医疗、工业控制等领域的CPS技术研发,《控制与决策》出版“信息物理系统理论、方法与应用”专栏. 经专家推荐和评审,最后录用论文22篇,集中反映了我国在CPS系统理论与应用研究中的最新成果,以供广大科技工作者了解和研讨. 本专栏收录的论文涉及CPS研究综述、CPS信息安全、CPS在网联汽车、智能电网、智能交通中的应用研究等方面. 期望这些优秀成果可以使读者受到鼓舞和启发,也希望能吸引和激发更多优秀学者投身于CPS研究,从而推动我国在CPS相关理论与应用研究中不断取得新成就.

1 信息物理系统理论研究

由于信息处理与动态过程的紧密关联,使得信息物理特别容易受到数据传输中的错误或攻击影响,进而造成损失或重大的破坏. 常见的外部攻击有阻断服务(denial-of service, DoS)、假数据注入(false data injection, FDI)、重启及哄骗等. 安全性是CPS研究的重要内容之一,本专栏有8篇论文专门研究此问题.

随着工业控制系统(industrial control systems, ICS)的网络化,其原有的封闭性被打破,各种病毒、木马等随着信息流进入ICS,严重威胁ICS的安全性,如何做好ICS安全防护已迫在眉睫. 入侵检测方法作为一种主动的信息安全防护技术可有效弥补防火墙等传统安全防护技术的不足,被认为是ICS的第2道安全防线,可实现对ICS外部和内部入侵的实时检测. 浙江工业大学张文安等对工业控制系统ICS网络入侵检测方面的国内外最新研究进展进行了综述,对来自计算机、自动化及通信等领域的研究人员从不同角度提出的工控系统入侵检测方法给出了全面的

收稿日期: 2019-10-16.

†通讯作者. E-mail: geguo@yeah.net.

总结和分析评价,指出了ICS入侵检测的现状、存在的问题及有待解决的关键问题. 在另一篇论文中,顾曹源等针对网络攻击下的不确定网络化多轴运动控制系统,提出一种基于分布式中间观测器的容侵同步控制方法. 首先将不确定性分解为匹配分量和不匹配分量,继而通过分布式中间观测器估计由执行器攻击、领航者的非零输入以及匹配不确定性分量构成的组合未知输入信号,进而设计基于估计值的容侵同步控制协议对匹配未知输入进行有效补偿,同时通过调节特定参数充分抑制不匹配不确定性效应,最终得到满意的容侵同步控制性能.

东北大学叶丹等从攻击者的角度研究了配备有分散式卡尔曼滤波器和χ^2检测器的多传感器系统的安全性问题. 为了最大程度地破坏系统性能,论文以数学期望的形式推导出子系统误差协方差表达式,并量化其与融合误差协方差的关系. 此外,结合矩阵理论,分析受攻击前后系统性能指标的变化并给出了可躲避检测器的最优线性欺骗攻击形式.

上海大学孙洪涛等针对CPS的安全控制设计问题,提出了DoS攻击下具有任意有界丢包的事件触发预测控制(event-triggered predictive control, ETPC)方法. 首先,考虑DoS攻击能量的有限性及攻击行为的任意性,将DoS攻击描述为事件触发通信机制下的任意有界丢包;其次,在控制器端利用最近一次收到的状态信息进行控制器增益序列的预测设计以补偿DoS攻击造成的数据包丢失;随后,基于Lyapunov稳定性理论及切换系统分析方法考虑了DoS攻击下CPS的安全性并给出了控制序列设计方法. 所提出的ETPC设计方法只需利用最近时刻收到的状态信息,无需满足传统CPS稳定性对最大允许丢包数的约束,为大时滞CPS的稳定性分析及控制提供了有效的解决方案.

东北大学秦皇岛分校王立夫等利用复杂网络描述信息物理系统个体间的相互作用,考虑了复杂网络中的割点在遭到攻击或破坏而造成的割点失效对网络可控性的影响. 首先给出复杂网络中割点失效的可控性模型,然后研究割点失效对可控性的影响,同时选取节点的随机失效和以度为依据的蓄意攻击作为对比. 发现随机失效对可控性的影响较小,而割点失效和蓄意攻击对可控性有较大影响;平均度较低时割点失效和蓄意攻击对可控性影响基本相同,但平均度增大后,割点失效比蓄意攻击对可控性的影响更大;另外,平均度的增加能够提高网络对割点失效的控制鲁棒性.

燕山大学李丽等针对带有过程噪声和测量噪声的领导-跟随多智能体系统,研究了拒绝服务攻击下多智能体系统的一致性问题. 首先,设计基于卡尔曼滤波的状态观测器,对智能体状态进行有效准确的估计;其次,基于预测控制理论,提出一种基于状态估计信息的分布式预测控制算法,从而实现领导-跟随多智能体系统的均方一致性控制,并给出了拒绝服务攻击环境下实现领导-跟随多智能体系统均方一致性的充分必要条件.

江南大学孙子文等基于不同网络攻击的特征提出了网络攻击防御策略,构建了离散系统的工业信息物理系统结构. 根据信息物理系统攻击者的攻击空间及攻击模型,采用控制理论方法讨论攻击空间模型的模型知识、披露资源和破坏资源的数学表达,对拒绝服务攻击、重放攻击、虚假数据注入攻击3种典型网络攻击及其对应攻击模型的表现形式进行了分析.

西安理工大学吴亚丽等针对CPS所处地理位置复杂及网络传输不可靠导致的检测鲁棒性不高问题,提出基于堆栈式稀疏降噪自编码网络的入侵检测算法,考虑到CPS对模型适应性及推广性的需求,将DBSO(difference brain storm optimization)与改进的自编码网络相结合,形成DBSO-SDAE(stacked auto-encoder)检测算法,可自动提取入侵数据的最优特征,提高了模型的鲁棒性和适应性.

CPS系统的信息获取、处理及传输方式、智能计算方法、系统的优化与资源调度、计算任务分配是影响CPS系统性能的关键因素,本专栏有5篇论文专门研究此问题.

天津大学杨洪玖等针对多子系统间存在复杂因果逻辑关系的CPS,建立带有未知非线性项和不确定耦合项的CPS多因系统模型,并提出了基于云控制技术的分布式控因方法. 利用非线性解耦观测器对CPS多因系统进行动态前馈线性化,使得CPS多因系统分解为多个无耦合关联的CPS因系统. 所设计的基于非线性解耦观测器的分布式模型预测控制器以及分布式优化算法,对于解耦后的CPS因系统能够实现在线约束优化控制.

沈阳化工大学李金娜等针对具有数据包丢失的网络化系统跟踪控制问题,提出了一种非策略Q-学习方法,完全利用可测数据,在系统模型参数未知且存在数据丢失的情况下,实现系统以近似最优的方式跟踪目标. 首先,刻画具有数据包丢失的网络控制系统,提出线性离散网络控制系统跟踪控制问题,基于Smith预测器提出具有数据包丢失补偿的最优跟踪

控制器;融合动态规划和强化学习方法,提出一种非策略Q-学习算法,该算法能保证基于Q-函数的迭代Bellman方程解的无偏性.

昆明理工大学张晶等针对无线传感器网络分区恢复连通后仍容错不足的问题,提出了斯坦纳树和凸多边形的分区双连通恢复方法. 首先以距离为依据选取现有叶子节点来促使少数未连通的离散节点统一成区,然后把分区抽象成点后枚举出所有的非退化型四边形,进而将计算得到的四边形中的2个斯坦纳点与4个顶点连接构造斯坦纳边部署中继节点使分区实现单连通. 再利用格雷厄姆凸壳算法选取抽象点中的凸壳顶点连接形成凸多边形实现分区的双连通,并对第2轮连通路径上的中继节点实施休眠唤醒机制. 在保证关键节点二次失效不会使网络再次瘫痪的基础上,简化了网络结构且降低了数据通信延迟,减少了中继节点的部署数量,延长了网络寿命.

兰州理工大学陈作汉等针对无线传感网络生命周期问题,分析了拓扑控制对于延长网络生命周期的重要性. 针对分簇结构无线传感网络的簇首选择问题,提出一种多目标簇首选择算法. 同时考虑网络通信距离、能量消耗、负载均衡以及节点生存时间等多个优化目标,通过理论计算确定最优簇首数量以指导种群初始化,引入正交实验机制降低搜索次数,提高寻优效率.

华北水利水电大学吕灵灵等考虑了移动边缘计算环境下的计算任务分配问题. 移动边缘计算将边缘服务器部署到无线局域网侧,将部分计算密集任务卸载到边缘云服务器,从而缩短了计算服务与移动设备的距离,降低了数据传输成本. 通过探索用户体验敏感度的异质性,建立了CPU运算周期数-数据量-价格的三元组合约模型,提出了基于合约理论的计算任务分配策略,以最大化云服务商的利润,同时保证了移动用户的非负效益,并讨论了完整信息场景下和统计信息场景下的最优合约设计策略.

2　信息物理系统应用研究

随着智能交通、网联车辆、微电网等技术的不断发展,交通、智能汽车和电力领域成为信息物理系统非常活跃和重要的几个应用领域. 因此,本专栏也收录了这些领域的综述论文和应用研究论文9篇.

网联车辆、交通大数据、共享出行等技术给智能交通系统的发展与应用革新带来了诸多新的机遇和挑战. 东北大学郭戈等在全面总结共享出行系统、网联车辆协同控制、交通大数据解析等领域的最新研究成果的基础上,系统地论述了智能交通的最新研究进展. 特别对智能交通系统中的交通流及出行需求预测、按需出行的车辆调度,交通网及电网联合调度和网联车辆的协同优化控制等方面进行了全面综述,分析了智能交通系统存在的问题及挑战,并对其未来发展方向做了展望.

网联车辆凭借先进的环境感知、实时信息获取和处理能力,可实现车辆与车辆、车辆与道路设施的信息共享和运行协调控制,是新一代智能交通信息物理系统的核心. 本专栏有多篇论文专门研究网联车辆系统的控制与优化问题.

吉林大学陈虹等针对人机协同转向控制中对于驾驶员参与和驾驶员状态考虑较少这一问题,提出了一种基于驾驶员状态预测的人机力矩协同转向控制方法. 该方法以力矩为人机交互接口,提高了驾驶员的参与程度;同时,在控制器设计过程中,采用模型预测控制方法,将驾驶员状态考虑在内,对驾驶员状态进行预测. 采用高精度车辆仿真软件进行仿真验证,结果表明与不考虑驾驶员状态的人机协同力矩转向控制方法相比,可以使辅助力矩更好地跟随驾驶员动作,提高车辆转向性能,减小侧向位移偏差;同时,对于不同驾驶员也有较好的适应性. 进而,以驾驶员下一步动作为参考,使驾驶员当前力矩尽可能接近下一步期望的力矩,在转向性能几乎不受影响的情况下,可适当减轻驾驶员操作负担.

东北大学王云鹏等针对人类驾驶车辆与自动驾驶车辆混合交通环境,提出了一种基于交通信息物理系统的车辆速度与交通信号协同优化控制方法,用于降低城市交通中的行车延误与燃油消耗. 首先,综合考虑了路口交通信号、人类驾驶车辆、自动驾驶车辆三者之间的相互影响,设计了一种适用于自动驾驶车辆与人类驾驶车辆混合组队特性的过路口速度规划模型;其次,针对车辆速度规划单一应用时的局限性,即无法减少车辆路口通行延误且易出现无解情况,提出了一种双目标协同优化模型,能够综合考虑车辆速度规划与路口交通信号控制,同时降低车辆燃油消耗与路口平均延误. 由于双目标优化问题求解的复杂性,设计了一种遗传算法——粒子群算法混合求解策略.

浙江工业大学宋秀兰等针对异构通信下的不确定网联车系统协同自适应巡航控制(cooperative adaptive cruise control, CACC)问题,提出了一种网联车系统鲁棒协同自适应巡航控制器设计方法. 采用伯努利随机过程和具有可变输入延迟的跟踪模型描述具有参数不确定性和丢包及时延的异构通信网联

车系统. 为降低CACC控制器设计的复杂性,采用分散输出反馈控制结构和线性矩阵不等式技术,求解不确定异构通信网联车系统的CACC控制器. 进一步,利用时滞系统方法和频域分析,建立保证闭环系统稳定和网联车辆系统弦稳定结果.

吉林大学于树友等针对线控车辆的信息安全问题提出了一种基于事件触发策略的四轮线控车辆系统的预测控制方案. 所谓事件触发是指将设备和模型的状态大于或等于某个预先设定的阈值作为一个事件,只有在事件发生时网络中传感器节点才会发送状态. 该方案利用事件触发控制对控制通道进行选择,根据李雅普诺夫稳定理论给定幂指数稳定的充分条件,进而设计出事件触发条件,并结合模型预测控制对未来动态信息进行预测,能在潜在对手攻击的情况下,保证车辆安全行驶. 仿真结果表明,该方案具有良好的抗干扰能力和抗黑客攻击能力.

同济大学张皓等研究了存在有界扰动的非线性无人车辆模型的路径跟随问题,提出了一种基于事件触发的模型预测控制算法. 与现有的基于时间周期的模型预测控制算法相比,可以在保证车辆对参考轨迹跟随的准确性的同时减少跟随过程中的求解优化问题的计算量,降低在线实时优化的计算负担.

电动汽车动力电池是分布式储能的重要组成部分. 华南理工大学陈渊睿等基于信息物理社会融合系统理论,深度融合了信息(对私家车出行的调查数据)、物理(动力电池的充放电物理模型)及社会(实际用户对电价或激励的响应)因素,借鉴平行系统思想,以软件定义的方式构建了映射真实电动汽车群体的平行人工电动汽车群体,研究电动汽车作为分布式储能参与储能汇聚复用的可行性与有效性. 以参与辅助电网平抑区域负荷波动为例,论文采用蒙特卡洛方法得到不同场景下人工电动汽车群体的日充放电曲线,进而研究了: 1) 给定价格策略下,不同理性程度用户充放电行为差异; 2) 不同价格策略下,电动汽车群体充放电行为对区域负荷方差的影响和相应的电网成本与收益; 3) 不同动力电池参数下,电动汽车群体接入电网后区域负荷方差缩减量变化的仿真实验研究.

燕山大学任丽娜等研究了电动汽车充电导航问题. 在电网分时电价的基础上,考虑电动汽车充电路径的选择与车主的驾驶行为的关系,通过对电动汽车的负荷设备分类建模,根据不同设备类型的重要程度及用户的电动汽车实际工况和地形因素,利用遗传算法分析最佳出行路径,提出了以时间成本与经济成本之和最优为目标,引导用户驾驶行为的充电导航策略.

随着电力信息通信技术的发展与应用,电力流与信息流深度融合,开放的通信环境与复杂的信息物理耦合交互,使得信息安全风险成为影响电力系统安全稳定运行的重要因素. 上海电力大学彭道刚等考虑了影响火电厂控制系统信息安全风险评估准确性的因素,如主观性强和不确定性等问题,提出了基于D-AHP(analytic hierarchy process)和TOPSIS(Technique for order preference by similarity to ideal solution)相结合的电厂控制系统信息安全风险评估方法. 根据工业控制系统风险评估的相关行业标准,识别工业控制系统的资产、威胁、脆弱性及现有安全措施,建立了评估指标体系和层次结构模型. 针对评估专家经验差异导致的评估信息不确定性,使用D-AHP方法求解各指标影响权重,然后使用TOPSIS法求出专家权重,最后得到电厂控制系统信息安全风险值.

3 结 语

本专栏论文大都得到了国家自然科学基金等各级各类研究基金的资助,研究成果具有一定的代表性,丰富了CPS系统理论体系. 需要指出的是,由于时间和篇幅所限,本专栏并未能全面涵盖CPS研究的所有课题领域,也不能反映国内该领域的全部研究方向及最新进展. 但我们期望本专栏能够对该领域的研究人员有所参考和启发,以推动信息物理系统理论及相关应用技术研究.

专栏编委

郭戈(1972–), 男, 教授, 博士生导师, 从事信息物理系统CPS优化决策理论及应用研究,以智能交通、共享出行等CPS应用研究为特色,是中国自动化学会信息物理系统专委会委员, E-mail: geguo@yeah.net;

张文安(1982–), 男, 教授, 博士生导师, 从事网络化系统融合估计与控制的理论及应用研究,以网络化运动控制、自主体运动姿态测量等应用研究为特色,是中国自动化学会信息物理系统专委会委员, E-mail: wazhang@zjut.edu.cn;

周彬(1981–), 男, 教授, 博士生导师, 从事线性和非线性控制理论及应用研究,以时滞系统、网络控制系统、多智能体系统和航天器控制系统的研究为特色,是中国自动化学会信息物理系统专委会委员, E-mail: binzhou@hit.edu.cn.