网络系统的安全决策与控制: 容错博弈研究综述

杨 浩†, 许宇航, 倪 媛, 路 石, 姜 斌

(南京航空航天大学 自动化学院，南京 210016)

摘 要: 安全决策与控制是保证控制系统稳定安全运行的核心支撑技术,现代网络系统在物理层面、信息层面、个体决策和监管层面分别会出现部件损坏、网络攻击和恶意决策等完全不同类型的异常行为. 鉴于此,首先总结各类异常行为的特点,指出网络系统安全决策与控制的目标与难点,强调容错博弈控制相较于其他容错控制和博弈方法的特色和优势;其次,聚焦于 4 个层面上的各类异常行为及其特点,阐述容错博弈控制的基本问题和思想,立足于跨层调节的思路,详细总结各类容错博弈控制的最新研究成果及其特性;再次,以集群飞行器系统作为典型对象阐述容错博弈控制的应用前景;最后,对容错博弈控制在现代网络系统中的研究方向进行展望.

关键词: 网络系统；异常行为；容错控制；博弈论

中图分类号: TP273 **文献标志码:** A

DOI: 10.13195/j.kzyjc.2021.1557

引用格式: 杨浩, 许宇航, 倪媛, 等. 网络系统的安全决策与控制: 容错博弈研究综述 [J]. 控制与决策, 2022, 37(4): 769-781.

Safe decision and control of network systems: A survey on fault tolerant game

YANG Hao†, XU Yu-hang, NI Yuan, LU Shi, JIANG Bin

(College of Automation Engineering，Nanjing University of Aeronautics and Astronautics，Nanjing 210016，China)

Abstract: Safe decision and control is one of the most significant technologies that ensure stable and safe operations of control systems. Three different types of abnormal behaviors, namely physical faults, cyber attacks and malicious decision may take place respectively on the physical, cyber, individual decision and supervisory layers of the modern network systems. Firstly, this paper summaries the characteristic of each abnormal behavior, and points out the goals and difficulties in the safe decision and control of network systems. The features and merits of the fault-tolerant game control is emphasized by comparing to the other fault-tolerant control methods and game methods. Secondly, this paper focuses on characteristics of these abnormal behaviors and introduces the basic problems and main ideas of fault-tolerant game design based on the cross-layer adjustment. The latest works on fault-tolerant game methods are summarized with respect to their features. An example of the swarm control systems is taken to illustrate the application prospects of fault-tolerant game control. Finally, some prospectives are also provided.

Keywords: network systems；abnormal behaviors；fault tolerant control；game theory

0 引 言

0.1 现代层级网络系统

随着人工智能的快速发展,现代控制系统拥有更加庞大的系统规模和更加复杂的动态特性,传统的简单独立的控制系统已无法满足日益增长的实际生活和生产的需求,网络系统的模型和架构应运而生,其建模、分析与设计研究得到学术界和工业界的极大关注. 网络系统由一组子系统通过一定的耦合网络机制组成,通过各个子系统的共同作用,达到满意的局部 (子系统) 和全局 (网络系统) 性能. 根据其耦合机制的不同特点,网络系统可以分为两类: 通过机械部件耦合的网络系统和通过通信耦合的网络系统. 前者广泛地应用于高速列车[1]、多体航天器[2]、智能电网[3] 等互联系统,后者广泛地应用于集群无人机[4]、多机器人编队[5] 等多智能体系统. 网络系统通过各个子系统之间的协同作用,可以胜任单一独立的控制系统所不能完成的任务.

现代网络系统具有智能化和层级化的特点,如图

收稿日期: 2021-09-06；**录用日期:** 2021-12-30.

基金项目: 国家自然科学基金项目 (61773201, 62073165)；高等学校学科创新引智计划项目 (B20007).

†通讯作者. E-mail: haoyang@nuaa.edu.cn.

1所示,可将现代网络系统分为4层结构[6-7]:物理层、个体决策层、信息层和监管层. 其中:物理层由网络中的各个实际物理系统组成,包括传感元件、执行元件、放大元件和校正元件等机械部件[8]. 个体决策层包含每个物理系统的决策和控制单元,直接控制物理层的运行(一般文献中,层级系统分为物理、信息和监管3层,本文着重探讨决策与控制,故将常规的物理层分为个体决策层和物理层). 个体决策层和物理层是整个控制系统的基础,根据从物理层和个体决策层采集的信息,信息层构建出各个物理系统之间的通信网络. 不仅如此,信息层作为层间信息交互的媒介,负责各种信息在物理层、个体决策层和监管层之间的“上行”和“下行”传递:上行过程将物理层的运行情况(包括各种约束)和个体决策层的当前执行情况上传给监管层,根据这些信息,监管层作为整个网络系统的“大脑”,对当前局势进行监督和判断,进而作出相对应的决策指令;下行过程将决策指令传达给个体决策层,个体决策层根据决策指令和当前网络层的通讯信息得出具体的执行指令,反馈并作用于物理层. 可以看出,4个层面构成紧密的闭环结构,相互耦合和影响[7],这样的层级网络系统被广泛地应用于生活和生产中,如智能电网[9]、智能交通系统[10]和集群飞行器[11]等.

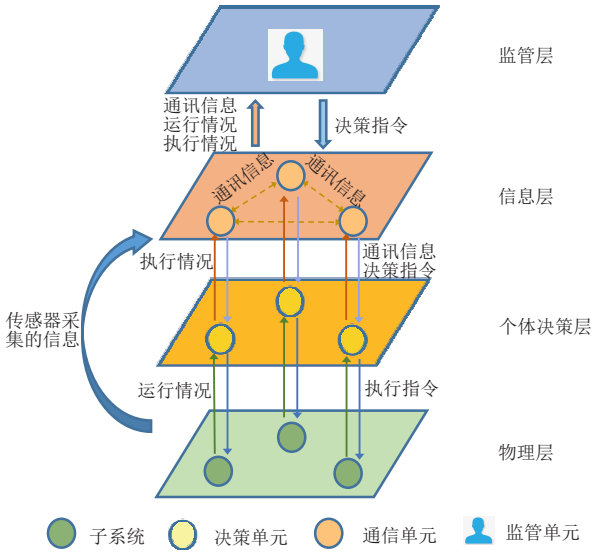

图1 现代层级网络系统

0.2 博弈控制

博弈理论最初由策梅洛、波莱尔等开始研究,经冯·诺依曼初步建立,最终由纳什为其一般化奠定了坚实的基础[12-14]. 博弈论主要研究数据化结构之间的相互作用,是事件发展趋势的一种可依据理论. 博弈的类型多种多样:依据合作与否分为合作博弈和非合作博弈;依据行为的时间序列性分为静态博弈和动态博弈;依据信息的完备程度分为不完备信息博弈和完备信息博弈等. 此外,依据模型特征也存在不同的划分.

博弈论能够有效描述网络系统与外部环境的信息交互以及系统内部个体的耦合特性,根据网络系统控制与决策过程中涉及对象的差异化目标,分别建立关于其控制输入的收益函数,从全局角度出发解决系统内部的控制器设计和决策优化问题. 例如,鲁棒控制可以建模为控制器和外部干扰两者间的零和博弈模型,广泛应用于外部干扰下控制器的设计[15];多智能体分布式优化以系统内部个体作为博弈的玩家,通过寻求纳什均衡策略,求解个体的最优控制输入,从而实现既定目标下系统的最优决策[16].

博弈论为解决现代层级网络系统的决策和控制提供了强有力的理论支撑:

在物理层,实际物理系统动态行为大多可以建模为微分方程,由此,博弈论产生了一个重要的分支——微分对策. 微分对策充分考虑物理层的动力学特点,是研究两个/多个玩家同时作用于一个由微分方程描述的动态系统,并最优化各自性能指标的理论[17-18]. 微分对策融合了博弈论和现代控制理论,是一个学科交叉的典范,其本质是处理两个/多个玩家的最优控制问题[19]. 微分对策根据玩家之间关系的不同衍生出多种类型,如零和微分对策、非零和微分对策、主从微分对策等,相应的成果广泛应用于经济、社会、工程等各个领域[17-19]. 例如,零和微分对策研究的是博弈中两个玩家支付函数之和为零的情况,既可用于玩家之间的对抗[20-23],也可用于研究系统内部控制器对不确定因素的对抗和抑制[24-26],广泛应用于追逃、拦截等场景,以及鲁棒和最优控制等问题.

在信息层,大规模的网络系统中,信息的收集、交互、处理都对决策起着至关重要的作用. 面向网络信息层的博弈需求是个体如何利用局部有限的信息作出合理的决策,从而使得群体智能涌现. 在信息层,节点间往往存在资源共享、利益冲突的情形,若资源分配不协调、节点间不协作,则极有可能造成整体效益降低,甚至引发严重的干扰问题. 博弈论为解决信息层的资源分配问题提供了强大的工具,催生出大量的研究成果. 其中,演化博弈论作为博弈论与生物学的交叉学科,模拟了生物感知环境并从中学习进化的过程,为解决大规模自组织网络系统中的资源分配问题提供了数学框架,解决了传统资源分配方案中信息量大、复杂度高的问题,同时保证了分配的公平

性[27]. 此外,匹配博弈[28-29]、讨价还价博弈[30-31]、主从博弈[32-33]等模型也广泛地运用于解决通信资源的优化配置问题. 类似的博弈思想在水资源分配[34]、电力系统[35-37]等方向均有大量研究成果.

在监管层和个体决策层,整个网络系统的博弈演化过程被这两个层面全局或者局部地引导着[6,38]. 监管层从宏观的角度完成决策的制定和分配,并在决策执行过程中通过个体反馈的信息监管系统整体的博弈过程,以便及时调整宏观决策和实现预期目标. 个体决策层则通过信息层接收到监管层发出的决策后,基于分布式架构从微观的角度制定自身的博弈和控制策略,监管并控制物理层的运行. 可以看出,监管层和个体决策层是网络系统实现博弈的核心层面. 全局和个体往往会有不同的代价函数,进而导致利益冲突,在这两个层面引入人的干预,建立合适的人机博弈机制,可以有效弥补自主无人机制的缺陷,更好地协调各个层面的博弈,以执行更加复杂的任务[39-42]. 例如,相比无人集群飞行器,有人-无人集群飞行器能够高收益且低损耗地实现对目标的侦查、攻击等任务[43-44]. 但值得注意的是,人在决策时往往带有主观非理性因素,需要结合行为博弈论等相关理论加以研究.

0.3　异常行为与容错控制

现代层级网络系统的4个层面都有可能发生异常行为,如图2所示,分别为:部件故障(物理层)、网络攻击(信息层)、恶意决策(监管层). 为了更加直观地描述3类异常行为对系统博弈的影响,建立一类以仿射非线性系统作为子系统动态模型的层级网络系统,其子系统i的动态模型可以表述为

$$\dot{x}_i = f_i(x_i) + g_i(x_i)u_i(x_i, x_j) + \sum_{j\in N_i} h_{ij}(x_j). \quad (1)$$

其中:$i \in M \triangleq \{1, 2, \ldots, m\}$,$M$为所有子系统的集合,$x_i$和$u_i$为子系统$i$的状态量和控制输入,$N_i$为子系统$i$的邻居集合. 函数$f_i(x_i)$和$g_i(x_i)$分别表征子系统$i$的系统动态和输入动态,函数$h_{ij}(x_j)$表征子系统$j$对子系统$i$的耦合效应. 在层级网络系统中,子系统$i$的性能指标设计为

$$J_i(x_i, x_j, S),\ i \in M, \quad (2)$$

其中S为监管层的决策指令. 下面将结合层级网络系统(1)及其对应的性能指标(2),分别阐述3类异常行为的特点和相应的容错控制方法:

1) 部件故障是指物理系统上的某些部件发生异常,包括传感器故障、执行器故障等[45]. 这类故障一般由周边环境、自身机械使用寿命等客观因素决定.

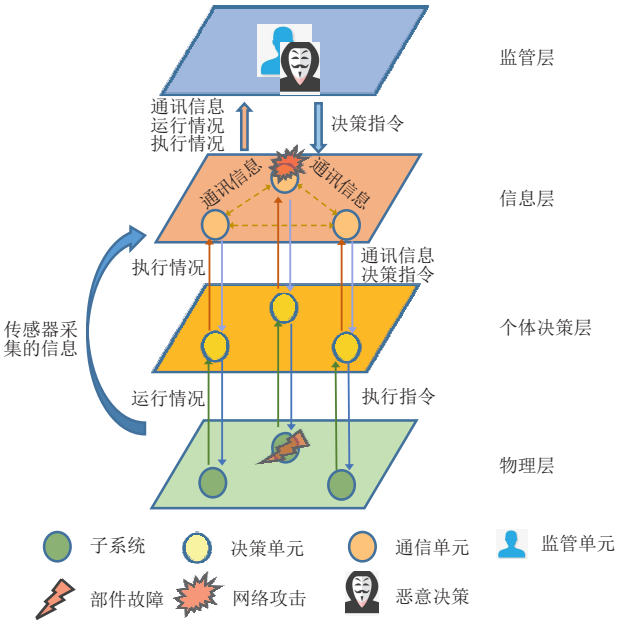

图 2　存在3类异常行为的现代层级网络系统

在层级网络系统(1)中,部件故障可以通过子系统i中与机械部件相关的函数表征,如:过程故障可以体现在系统动态函数$f_i(x_i)$中,执行器故障可以体现在输入动态函数$g_i(x_i)$中等. 当部件故障发生时,故障信息通过信息层上行至监管层. 监管层作出决策指令的调整,并下达至个体决策层. 由个体决策层生成具体容错控制指令来调节控制器以实现容错目标. 目前,针对部件故障的网络系统容错控制方法主要有两种思路:独立容错控制[46-48]和协同容错控制[49-50]. 独立容错从个体的角度出发,分析部件故障对整个网络的影响,通过单独调整个体决策层中故障个体的控制器以维持全局网络系统的性能,达到容错目的;协同容错则从全局网络系统的角度出发,同时调整健康个体和故障个体的控制器以达到容错目的. 由此可见,独立容错控制是传统容错控制方法的直接推广,而协同容错控制是根据网络系统的特点应运而生的新兴容错控制方法.

2) 网络攻击是指针对计算机信息系统、基础设施、计算机网络或个人计算机设备的任何类型的进攻行动,包括破坏、泄露、修改,在没有得到授权情况下窃取或篡改计算机上的数据,使软件或服务的正常功能丧失等[51]. 以计算机网络的5层体系结构,即物理层、链路层、网络层、传输层和应用层为准,网络攻击主要发生在后3层,少部分涉及链路层[52],目的是破坏网络安全的3要素,即信息的可用性、完整性和保密性[53]. 其中,主动攻击以破坏通信可用性及数据完整性为主,对应的常见类型有拒绝服务攻击[54](DoS攻击)和重放攻击[55]等. 被动攻击则以损

害信息保密性为主,常见的有密码破解、恶意软件和病毒等[56]. 在层级网络系统(1)中,网络攻击主要与通信网络拓扑相关,例如,当受到欺骗攻击时,来自于邻居$j \in N_i$的信息极有可能不准确,从而引起控制器和性能指标中的x_j信息产生变化. 目前的网络安全解决方案主要是防火墙等保护设备及入侵检测系统等反应设备,以事前保护重要的系统组件和事后识别攻击者注入的虚假数据为主[56-58].

3) 恶意决策是指在个体决策和监管层的决策主体主动地选择非最优决策或者改变自身的代价函数[59-60],这类异常行为主要源自于人类特有的情感、认知和心理特性. 回到系统模型(1)和(2),监管层的恶意决策通过改变性能指标$J_i(x_i, x_j, S)$中的决策指令S,进而引导整个网络系统的博弈趋向于非预期目标. 个体决策层通过恶意改变相邻个体的性能指标$J_i(x_i, x_j, S)$中的信息变量x_j,降低个体之间的协同能力,进而破坏整体性能. 拜占庭故障是常见的个体决策层的恶意决策情形,其中恶意个体对其相邻个体传输不同的信息量,导致集群的整体收益下降[61]. 针对这类恶意决策,可以通过基于值函数的强化学习等方法训练个体决策层学习恶意特征,从根源上降低其发生的概率[62],但是这并不能抑制恶意决策的发生,有效的方法是调节监管层和个体决策层的收益函数:前者可以对宏观的博弈机制进行重构[63],后者可以提高网络系统对监管层的恶意决策的鲁棒性[64-68],从而抑制因恶意决策导致的博弈性能下降,保证系统的整体收益仍然保持不变或者下降到一个可以接受的程度.

0.4 容错博弈控制

网络系统安全决策与控制的目标是针对部件故障、网络攻击和恶意决策等异常行为,依托4个层次中可调节的手段,设计容错控制方法,以确保层级网络系统稳定、安全和高效地运行. 然而,对该问题的研究主要存在以下难点尚未解决:

1) 网络系统中不仅有被广泛研究的部件故障和网络攻击,决策主体还往往带有主观特征,会给决策和控制带来偏差,进而影响系统的安全性,而常规的容错控制方法对此无能为力. 因此,如何在网络系统中建模决策偏差,并在该模型下实现容错目标是一个挑战.

2) 现代层级网络系统中的4个层面具有紧密耦合的特点,这使得单独针对某一层的安全决策与控制的方法效果受限,因此,如何综合考虑各个层面的异常行为并设计行之有效的跨层调节的容错控制方法是一个难题.

3) 在网络系统的安全决策与控制过程中,容错和保持最优性能是两个难以兼顾和平衡的目标,大多数方法只能实现保性能容错控制[69]. 因此,如何既能实现容错目标,又能保证每个子系统的最优性能甚至整个网络系统的全局最优性能,是网络系统的安全决策与控制中一个重要的研究方向.

为了解决以上问题,容错博弈控制应运而生,其主要思想是将每个子系统视为玩家,通过为每个子系统设计自身性能指标的方式,赋予其自私属性;通过子系统之间的不断博弈,同时实现网络系统在各个层面异常行为下的容错目标、子系统局部最优性能以及整个网络系统的全局最优性能. 作为博弈论与容错控制理论的有机结合,容错博弈采用博弈论对系统内部个体和系统外部因素及其相应的收益函数进行建模,运用自适应动态规划、迭代法、强化学习等方法对博弈的均衡点进行求解和分析,进而基于容错控制理论设计容错控制律以调节博弈的均衡点. 与传统的博弈论相比,容错博弈控制不再仅仅关注博弈均衡点的求解和特性分析,而是进一步在此基础上,通过设计强有力的控制律实现对各控制器博弈进程的有效干预和对均衡点的有效调节,从而实现个体的最优决策和系统的期望状态.

0.5 问题描述

综上所述,3类异常行为对于层级网络系统的博弈机制会产生严重的影响,虽然有一些相关的容错控制成果,但如何设计有效的容错博弈控制需要深入和系统性的研究,这是保证网络系统安全决策与控制的关键问题.

面向部件故障,容错博弈控制着眼于设计合适的博弈安全控制策略,保证物理层系统的性能和博弈均衡点的存在性,继而维持整个层级网络系统正常运作的能力.

面向网络攻击,容错博弈控制着眼于补偿攻击对通信资源分配的影响,同时为各个网络节点规划最优的防御资源,以确保系统的稳定性和网络的安全性.

面向恶意决策,容错博弈控制着眼于如何分层调整博弈机制,控制博弈演化过程,进而保证全局和局部的博弈性能.

下面的章节将分别阐述面向3类异常行为的容错博弈控制方法.

1 面向部件故障的容错博弈控制

协同优化容错控制方面的工作对部件故障的容错博弈控制问题的研究起到了奠基性的作用,特别是

针对编队控制分层协同优化容错控制的方法在各个领域发挥着重要作用[70-71]. 其主要思想是将编队的协同容错控制分解为个体容错-队形恢复-性能检测3个模块,当每个模块完成各自的任务,所有模块融合贯通之时,即可保证整个编队在发生故障情况下仍能顺利完成既定任务. 这一套“分而治之,合则愈之”的协同优化容错控制策略广泛地应用于实际生活和生产中,如飞机和卫星的编队控制[72-74]. 与传统控制系统相比较,现代层级网络系统的自身规模不断扩大,系统复杂度不断提升,且运行环境更加多变,这便需要发展新的面向部件故障的容错控制方法. 因此,基于微分对策的容错控制方法应运而生.

考虑每个物理系统“由外及里”的递进式博弈关系,基于微分对策的容错控制方法可以分为两类: 第1类仅考虑子系统之间的博弈关系,称之为“外环容错博弈控制”;在此基础上,发展出第2类容错博弈控制,其不仅考虑子系统之间的博弈关系,而且深入到子系统内部,考虑控制器与故障之间的博弈关系,称为“内外环容错博弈控制”. 这两种容错博弈控制的核心思想如图3所示,通过调节个体决策层的控制器实现对部件故障的容错目的.

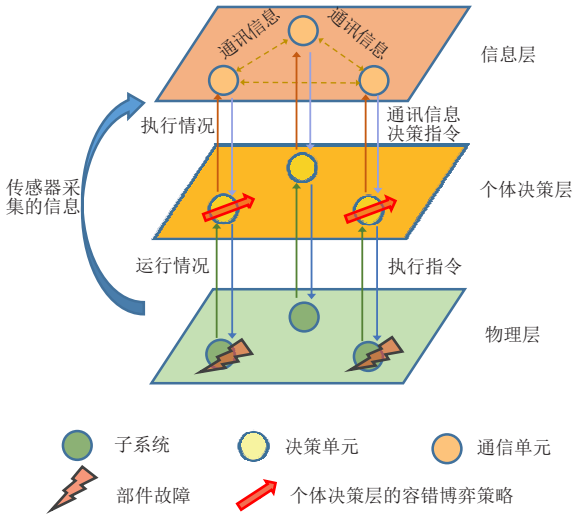

图 3　面向部件故障的容错博弈控制

1.1　外环容错博弈控制

外环容错博弈控制聚焦于子系统与子系统之间的博弈特性,研究成果可以有两个分支: 一个分支是针对不同博弈问题中玩家发生部件故障的情况,设计对应的容错博弈控制实现容错目标[75-76]. 基于该思想,文献[76]探究了离散非线性追逃博弈中追击者和逃逸者同时发生执行器故障情况,设计故障估计器补偿部件故障对网络系统的影响,进而在个体决策层中设计近最优容错控制器以保证追击者仍然能捕捉到逃逸者. 这一分支研究的问题本身是一种博弈,另一个分支针对的问题本身并非博弈,而是将其转换为博弈问题,进而用博弈工具加以研究. 其主要思想是将1个复杂系统视为由多个子系统耦合构成的互联系统,将子系统作为玩家,充分利用不同子系统之间合作与非合作的关系,构建它们之间的博弈关系,进而设计对应的容错博弈控制策略. 基于该思想,文献[77]利用合作博弈实现四轮独立驱动电动车的容错控制,将电动车的4个执行器当做4个玩家进行博弈,寻求其Pareto解,从而保证电动车在发生执行器故障时仍然可以保持稳定. 在此基础上,文献[78]将人的行为影响融入容错博弈控制的设计中,从而有效地降低电动车的工作负载.

值得一提的是,上述工作有一个共同的特点: 其博弈的特性均体现在子系统与子系统之间,很少深入探讨子系统内部控制器与故障之间相互博弈的逻辑关系. 为揭示这种博弈机理,内外环容错博弈控制得以发展.

1.2　内外环容错博弈控制

内外环容错博弈控制方法的本质是基于“games in games”的框架[79],其主要目的是为了深入到子系统内部,揭示控制器与故障之间潜在的博弈关系. 为此,文献[80]针对发生多重故障的网络系统设计了一种基于两层博弈的容错控制方法. 其中,每个子系统内部进行控制器和部件故障的零和博弈,与此同时,各个子系统之间进行图博弈,所设计的容错博弈控制保证了网络系统的Nash均衡. 由于零和博弈本质上延续了鲁棒控制的思想,其容错博弈控制器是针对最差故障情况下设计的,为了降低这种保守性,文献[81]提出了一种基于主从微分图博弈的容错思想,深入探究了被控系统及其对应的诊断观测器之间的双向影响,分析了两者决策的次序性. 将被控系统作为领导者,观测器作为跟随者,进行顺序博弈,从而保证网络系统的稳定性和最优性能.

外环容错博弈控制从网络系统组成多样性的特点出发,充分利用各个子系统之间竞争与合作的关系,构建各个子系统之间博弈的联系,而在处理故障的手段上,延续经典容错控制理论的思想,采用主动/被动容错控制方法实现容错目标. 相较于外环容错博弈控制,内外环容错博弈控制不仅关注子系统之间的博弈关系,而且关注子系统内部控制器与故障之间的作用关系,揭示其博弈机理,与外环博弈共同构成了“博弈中的博弈”,从而摆脱了传统容错控制方法的约束,使容错本身带上了“博弈”的色彩.

2 面向网络攻击的容错博弈控制

博弈论为网络安全问题的分析、建模和设计提供了强大的数学工具,既可以描述正常网络系统的资源分配、博弈和决策过程,又可以描述网络攻击下攻防双方的博弈对抗,下文将针对这两种情况下的容错博弈控制展开讨论.

2.1 基于博弈论的攻击补偿设计

在信息层的资源分配问题中,节点间的良好协作对网络系统的正常运行有着重要意义,而网络攻击则会导致节点出现阻塞、中断甚至攻击其他节点等异常行为. 因此在信息层,促进节点合作、设计容错控制律以补偿攻击造成的影响,是网络安全的一个重要议题.

演化博弈论为信息层的资源分配问题提供了良好的数学框架,能够描述和解释网络中各个节点行为的形成和演化过程. 与此同时,通过对其演化动态的研究,还能帮助研究者提炼出相关的促进机制,进而实现合作行为的涌现. 目前,已有大量研究利用演化博弈论的机理设计网络节点间合作的激励机制[82-85],通过建立基于信用的评价体系,对不同信用度的节点进行奖励/惩罚,从而调整博弈的支付矩阵/支付函数,以补偿攻击造成的影响. 图4给出一种典型的基于演化博弈论的攻击补偿设计框架:首先根据节点的行为特征以及可采集的数据量,借助数据挖掘的手段,总结出信用度评价的规则,进而得到各节点的信用度. 当某个节点受到攻击时,其异常行为会降低信用度,此时与该节点协作所能获得的协作激励便会相应降低,在演化博弈的机理下,邻居节点会逐渐选择不与该节点协作以保留自身资源. 由此可见,这类机制能够推动高信用节点间的协作,同时规避与低信用节点合作导致的风险,确保了网络系统的正常运行.

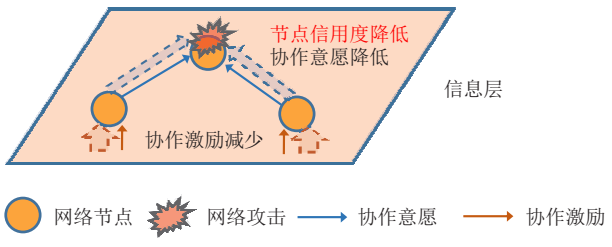

图 4 基于演化博弈论的攻击补偿设计

2.2 基于博弈论的防御资源配置

网络的攻击者和防御者存在鲜明的利益冲突关系,而攻防博弈可以很好地刻画这种竞争问题,是在信息层实现容错博弈控制的一个重要思路. 其中,防御者具有一定的防御资源和目标集合,而攻击者能够通过侦察获取防御者的策略,并在规划后实施攻击. 在博弈类型的选取上,研究者们大多选择了主从博弈模型[86-87]:防御者为领导者,首先选定某一策略;然后追随者根据领导者的决策进行自身的决策. 这一具有先后时序的动态博弈,与同时行动假设相比,更符合先有防御资源部署后有攻击及应对措施的实际情况. 双方根据对方的可能策略选择自身策略以保证自身收益最大化,从而达到Nash均衡. 从防御者的角度而言,也获得了最优的防御资源配置. 除了最为常见的主从博弈外,常和博弈特别是零和博弈也是使用频率较高的模型[88-89],其特征为博弈参与者的收益之和是一个常数(或零). 前者能更详细地刻画攻防成本和收益量化下的对抗问题,但作为一个NP-hard问题,在Nash均衡的求解方面往往需要借助强化学习或智能算法.

2.3 个体决策层-信息层联合容错博弈控制

前两节在考虑面向网络攻击的容错控制问题时均从信息层切入,这是很自然的想法. 值得注意的是,如前文所述,现代层级网络系统各层之间相互影响、高度融合,这种多层结构为设计容错策略提供了更丰富的手段. 一些研究者则着眼于个体决策层,运用控制理论的方法对网络攻击进行容错,以确保系统的稳定性. 以Dos攻击为例,Persis等[90]从输入状态稳定(ISS)的角度分析了这类攻击的特征和对系统的影响,并确定了采用状态反馈进行容错时DoS攻击的频率和持续时间的限制条件. 此后,多名学者在其基础上进行了拓展,包括事件驱动[91]、基于预测器的控制[92]等.

基于信息层的容错方法注重网络的安全性,而基于个体决策层的容错方法更侧重于维持物理系统的稳定性,从这两个角度分别考虑网络攻击的容错控制问题往往不能发挥最佳效果. 针对这一现状,一些学者建立了如图5所示的跨层博弈控制模型[93]. 其中:信息层采用攻防博弈的模型;个体决策层的控制器致力于最优化系统性能,而网络攻击在物理层造成的扰动与控制器的作用相反,两者之间也可以用博弈模型进行描述. 由于个体决策层需要来自信息层的通讯信息以设计控制器,层级之间的交互关系可以采用主从博弈进行建模,信息层为主,个体决策层为从. 目前,已有部分研究利用跨层容错博弈的思路解决现代层级系统中的安全性和可自愈性问题[93-95].

防御资源配置侧重于“防御”,通过保护网络中的重要节点,尽可能消除或削弱网络攻击带来的影响;攻击补偿设计侧重于“重构”,通过网络节点间自发的拓扑重构,在网络受到攻击、遭到破坏后尽可能恢

复其性能;而联合容错博弈控制综合考虑了网络层面的安全性和物理层面的稳定性,其容错效果相比前两者更为全面.

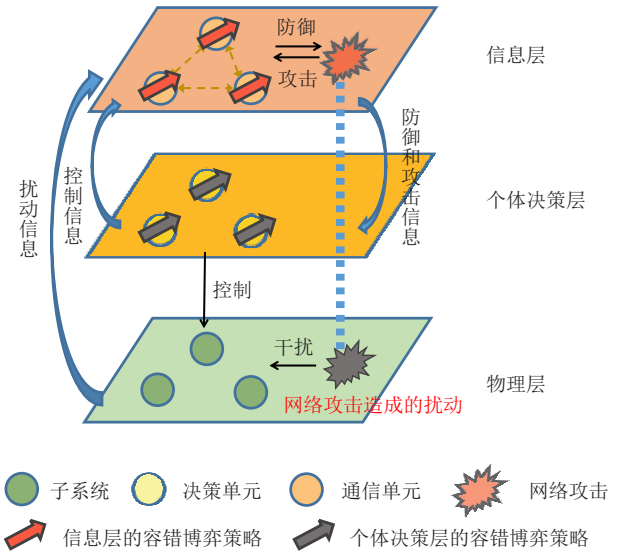

图 5　跨层容错博弈控制模型

3　面向恶意决策的容错博弈控制

监管层和个体决策层中个体发生的恶意决策行为会给网络系统的博弈走向带来不期望的偏差,进而影响各个层面的运行情况.

3.1　恶意决策

监管层和个体决策层是以人为主导作用的层次,其中监管层负责网络系统的任务规划、分配和全局监管,个体决策层负责任务执行和局部监管. 人具有复杂的社会情感、心理偏好、风险感知差异等心理学特性,在复杂场景中也易受到外界各种因素的干扰. 在人的行为博弈建模方面有着较为丰富的研究成果,例如,前景理论描述了人的确定效应、反射效应、参考依赖效应和损失效应[96],因此人在面对问题时会选择前景值最大的策略[97]. 概率敏感性刻画了人重视小概率轻视大概率事件的情形[98]. 累积的前景理论是基于概率敏感性的前景理论,考虑了重复博弈中人的多种行为因素[99]. 作为决策主体的人极有可能恶意地选择非最优策略,破坏正常的博弈演化过程,导致系统的整体收益最小化[97,100-101].

Zhang 等[38] 提出了基于博弈论框架控制系统的研究方法,其中监管层作为系统的全局控制器首先作出决策,进而每个个体根据全局的决策优化自身的个体收益函数. 该方法本质上是通过控制每个个体收益函数使得博弈演化过程按照预期发展. 恶意决策对网络系统博弈的影响也遵循这样的机理,具有明显的计划性和目的性,表现为监管层的策略选择异常或者收益函数的变化,进而影响到网络层面的通信拓扑,以及个体决策层的代价函数等,使得整个网络系统的博弈趋向于不期望的Nash均衡甚至无法达到均衡,最终导致系统的收益趋向于最小化.

3.2　基于重构的容错博弈控制

博弈调节方法如图6所示,对应于监管层、个体决策层和信息层,主要分为监管层决策调节、个体收益函数调节和通信网络拓扑重构.

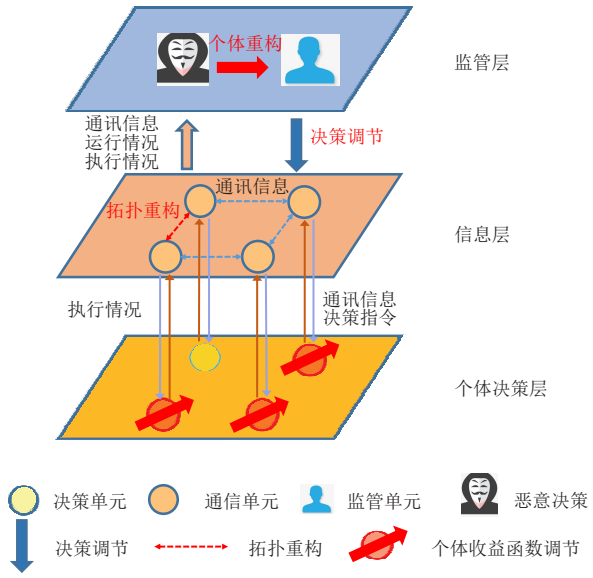

图 6　基于博弈重构抑制监管层恶意行为

1) 监管层决策调节. 监管层或者个体决策层的主体作出恶意决策,可以通过更换主体或者调节决策的方式重新设定决策指令,即调整式(2)中的 S,从而控制网络系统的演化过程,恢复整体的收益. 例如,阻塞博弈中政府的不合理设定道路收费规则必然导致整体的阻塞程度增加,因此重构道路的收费规则进而使得个体收益最优同时最小化阻塞程度[63].

2) 个体收益函数调节. 通过调节个体收益函数以遏制监管层或者个体决策层中个体的恶意决策带来的影响,即调节式(2)中的 J_i. 宏观的恶意决策会影响网络系统中的部分甚至全部个体的收益函数,个体决策层通过协同调节自身的个体收益函数,尽可能使得网络整体收益最大化或者降低到可以接受的水平. 例如,演化博弈中的监管层的恶意决策会导致部分群体收益下降,因此可以基于个体决策层协同调节的思路,利用激励机制更改其他群体中个体的收益函数来恢复系统整体性能[102]. 阻塞博弈中通过更改部分正常道路的收费规则同样可以使得阻塞程度最小化[103].

3) 通信网络拓扑重构. 信息层在层级架构中扮演着信息传递的桥梁角色,通过改变信息层的拓扑结构可以使得个体之间的互联关系发生变化,进而改变

个体的收益函数,仍然调节式(2)中的J_i. 压缩感知可以从少量感知数据中恢复信号,是网络重构最有效的手段,然而存在精度丢失和重构失败的概率. 但是基于演化博弈动态方程,通过重新组织策略矩阵可以克服压缩重构的缺陷并实现信号的重构[104].

监管层具有完备的全局信息,因此监管层决策调节的容错范围更广,但其实现涉及到全局系统,实现成本较高,而个体决策层收益函数调节和通信拓扑重构两种方法仅需要局部信息,调控小范围个体的收益函数进而间接影响全局博弈的走向更易于实现.

4 容错博弈在集群飞行器中的应用前景

上述容错博弈控制的最新研究成果在层级网络系统中有着广泛的应用前景,下面以大规模集群飞行器[4,44]为典型对象进行简要介绍. 集群飞行器系统可分为4个层面:地面监管中心作为监管层,负责飞行器的任务分配和监管;各个飞行器作为个体决策层,负责任务的执行和再分配;飞行器各机械部件作为物理层,负责构建飞行器的系统动态. 此外,基于演化博弈机制,各飞行器节点依据距离损耗、通信容量等要素选取下一跳通信节点,形成通信拓扑,构成集群的信息层. 下面将分别阐述容错博弈控制在4个层面的应用前景:

1) 针对地面监管中心的恶意决策[105],建立基于个体收益函数调节的容错博弈控制机制. 监管中心负责任务分配,通过合理设计飞行器与任务之间的博弈机制实现任务的有效分配,使得集群整体收益最大化. 但是以人为核心的监管中心在任务分配的过程中,由于信息不完备或者主观情绪等原因,存在恶意决策情形,造成任务执行效率低下、整体收益受损等不良后果. 容错博弈控制为调整监管层恶意决策提供了思路和方法,可通过改变任务分配机制下的个体收益函数,恢复集群受损的收益.

2) 针对集群通信的网络攻击[106],建立“防御”与“重构”并行的容错博弈机制. 一方面,基于网络的节点重要度和网络攻击的分布情况,采用攻防博弈对各节点进行防御资源配置;另一方面,建立关于节点历史通信行为的信用度评价体系,改进通信拓扑形成的演化博弈机制,促使飞行器节点规避与低信用节点合作,实现节点出现中断、阻塞等异常行为时拓扑的有效重构,完善集群通信的攻击补偿设计.

3) 针对个体飞行器的恶意决策[107],建立基于监管层决策调节的容错博弈控制机制. 基于飞行器与集群中其余飞行器以及外部环境的博弈机制,完成各飞行器的航迹规划和编队控制. 而人操控下的飞行器同样存在恶意决策情形,导致飞行器之间的合作能力以及自身的生存能力下降. 基于容错博弈控制思想,可通过地面监管中心直接改变恶意飞行器中的任务执行指令,调整个体决策层恶意决策带来的不良影响.

4) 针对飞行器的部件故障[70-71],建立内外环容错博弈控制. 首先基于图博弈,构建各架飞行器之间竞争和合作的关系;其次在飞行器内部根据实际控制性能的需求,构建控制器与故障之间的零和博弈或主从博弈. 在控制器结构和参数不可变的情况下,通过构建控制器与故障之间对抗的性能指标设计两者的零和博弈,保证系统存在最差故障的情况下系统的性能仍然可以保持. 在控制器结构和参数可变的情况下,为每个飞行器设计故障诊断观测器,形成主从博弈,对飞行器故障的情况进行监测,实时估计故障信息,并将估计的故障信息反馈给飞行器,进而重构故障飞行器的控制器,实现容错博弈的目标.

5 展 望

本文总结了现代网络系统容错博弈控制的研究成果,在4个层面的层级架构下,面向部件故障、网络攻击、恶意决策3类异常行为,全面介绍了容错博弈控制方法,总结为表1. 可以看出,异常行为的多样性和层级架构的关联性,为容错博弈控制带来了极大的学术挑战,同时也提供了丰富的容错手段. 针对该方向的研究仍十分有限,很多挑战性的问题值得作进一步研究.

表1 容错博弈控制文献分类

异常行为	容错博弈手段
部件故障[1, 45-50, 69-72, 75-78, 80-81]	外环容错博弈控制[75-78] 内外环容错博弈控制[79-81]
网络攻击[51-58, 82-95, 106]	攻击补偿设计[82-85] 防御资源配置[86-89] 联合容错博弈控制[93-95]
恶意决策[59-61, 64-68, 105, 107]	监管层决策调节[38, 63] 个体收益函数调节[102-103] 通信网络拓扑重构[104]

最后,对网络系统容错博弈控制方向的发展趋势做一个展望:

1) 现有成果大多在各个层面单独开展,没有充分挖掘层级网络系统各个层面的关联机理,这不仅无法与网络系统多层面高度融合的特性相匹配,而且极大地限制了容错博弈控制的适用范围和应用效果. 因此,未来需要从4个层面加以综合考虑和联合设计,从而充分挖掘各个层面的容错调节手段,这对于提高

容错博弈控制效果有着非常重要的意义.

2) 对于带有个体主观非理性网络系统容错博弈控制的研究较少,非理性因素使得博弈的实际均衡解与期望均衡解之间产生偏差,如何探究决策主体主观性的作用机理,进而建立有效的非理性决策下的博弈模型,是提高人机共融智能,使容错博弈更符合工程实际的必经之路.

3) 目前,针对恶意决策个体的处理方式是将其直接从网络系统中移除,并研究剩余网络的鲁棒性. 这类方法并不适用于带有空间几何属性的网络系统. 例如飞行器编队,随意移除恶意个体可能会带来机群的碰撞,甚至整个编队系统的瓦解. 因此,如何设计安全移除恶意决策个体的机制,使其在不影响其他个体的情况下安全移除是一个难题. 不仅如此,如何从定量的角度设计针对恶意个体的感知和估计方法来处理具有未知恶意决策行为的恶意个体是一个全新的挑战.

参考文献(References)

[1] Wang Y J, Song Y D, Gao H, et al. Distributed fault-tolerant control of virtually and physically interconnected systems with application to high-speed trains under traction/braking failures[J]. IEEE Transactions on Intelligent Transportation Systems, 2016, 17(2): 535-545.

[2] Di Gennaro S. Output stabilization of flexible spacecraft with active vibration suppression[J]. IEEE Transactions on Aerospace and Electronic Systems, 2003, 39(3): 747-759.

[3] Vournas C D, Papadias B C. Power system stabilization via parameter optimization-application to the hellenic interconnected system[J]. IEEE Transactions on Power Systems, 1987, 2(3): 615-622.

[4] 杜继永, 张凤鸣, 毛红保, 等. 多UAV协同搜索的博弈论模型及快速求解方法[J]. 上海交通大学学报, 2013, 47(4): 667-673.
(Du J Y, Zhang F M, Mao H B, et al. Game theory based multi-UAV cooperative searching model and fast solution approach[J]. Journal of Shanghai Jiao Tong University, 2013, 47(4): 667-673.)

[5] Lashkari N, Biglarbegian M, Yang S X. Development of a novel robust control method for formation of heterogeneous multiple mobile robots with autonomous docking capability[J]. IEEE Transactions on Automation Science and Engineering, 2020, 17(4): 1759-1776.

[6] Huang Y H, Chen J T, Huang L N, et al. Dynamic games for secure and resilient control system design[J]. National Science Review, 2020, 7(7): 1125-1141.

[7] Albaba B M, Yildiz Y. Modeling cyber-physical human systems via an interplay between reinforcement learning and game theory[J]. Annual Reviews in Control, 2019, 48: 1-21.

[8] 胡寿松. 自动控制原理[M]. 北京: 科学出版社, 2007: 1-20.
(Hu S S. Principles of automatic control[M]. Beijing: Science Press, 2007: 1-20.)

[9] Ding L, Wang L Y, Yin G Y, et al. Distributed energy management for smart grids with an event-triggered communication scheme[J]. IEEE Transactions on Control Systems Technology, 2019, 27(5): 1950-1961.

[10] Menelaou C, Timotheou S, Kolios P, et al. Minimizing traffic congestion through continuous-time route reservations with travel time predictions[J]. IEEE Transactions on Intelligent Vehicles, 2019, 4(1): 141-153.

[11] Yu D X, Chen C L P. Smooth transition in communication for swarm control with formation change[J]. IEEE Transactions on Industrial Informatics, 2020, 16(11): 6962-6971.

[12] Morgenstern O. The collaboration between oskar morgenstern and john von neumann on the theory of games[C]. Theory of Games and Economic Behavior. Princeton: Princeton University Press, 2007: 712-726.

[13] Nash J F. Equilibrium points in N-person games[J]. Proceedings of the National Academy of Sciences, 1950, 36(1): 48-49.

[14] Nash J F. 7. non-cooperative games[C]. The Essential John Nash. Princeton: Princeton University Press, 2002: 85-98.

[15] 庞岩, 王娜, 夏浩. 基于博弈论的信息物理融合系统安全控制[J]. 自动化学报, 2019, 45(1): 185-195.
(Pang Y, Wang N, Xia H. A game theory approach for secure control of cyber-physical systems[J]. Acta Automatica Sinica, 2019, 45(1): 185-195.)

[16] Baar T, Olsder G J. Dynamic noncooperative game theory[M]. The 2nd edition. Philadelphia: Society for Industrial and Applied Mathematics, 1998: 77-159.

[17] 张嗣瀛. 微分对策[M]. 北京: 科学出版社, 1987: 1-5.
(Zhang S Y. Differential games[M]. Beijing: Science Press, 1987: 1-5.)

[18] 李登峰. 微分对策以及应用[M]. 北京: 国防工业出版社, 2000: 1-8.
(Li D F. Differential games and applications[M]. Beijing: National Defence Industry Press, 2000: 1-8.)

[19] 谭拂晓, 刘德荣, 关新平, 等. 基于微分对策理论的非线性控制回顾与展望[J]. 自动化学报, 2014, 40(1): 1-15.
(Tan F X, Liu D R, Guan X P, et al. Review and perspective of nonlinear systems control based on diferential games[J]. Acta Automatica Sinica, 2014, 40(1): 1-15.)

[20] Liu M S, Wan Y, Lewis F L, et al. Adaptive optimal control for stochastic multiplayer differential games using on-policy and off-policy reinforcement learning[J]. IEEE Transactions on Neural Networks and Learning Systems,

2020, 31(12): 5522-5533.

[21] Lopez V G, Lewis F L, Wan Y, et al. Solutions for multiagent pursuit-evasion games on communication graphs: Finite-time capture and asymptotic behaviors[J]. IEEE Transactions on Automatic Control, 2020, 65(5): 1911-1923.

[22] Garcia E, Casbeer D W, Pachter M. Design and analysis of state-feedback optimal strategies for the differential game of active defense[J]. IEEE Transactions on Automatic Control, 2018, 64(2): 553-568.

[23] Jagat A, Sinclair A J. Nonlinear control for spacecraft pursuit-evasion game using the state-dependent riccati equation method[J]. IEEE Transactions on Aerospace and Electronic Systems, 2017, 53(6): 3032-3042.

[24] Sun J, Liu C. Decentralised zero-sum differential game for a class of large-scale interconnected systems via adaptive dynamic programming[J]. International Journal of Control, 2019, 92(12): 2917-2927.

[25] Vrabie D, Lewis F. Adaptive dynamic programming for online solution of a zero-sum differential game[J]. Journal of Control Theory and Applications, 2011, 9(3): 353-360.

[26] Wei Q L, Song R Z, Yan P F. Data-driven zero-sum neuro-optimal control for a class of continuous-time unknown nonlinear systems with disturbance using ADP[J]. IEEE Transactions on Neural Networks and Learning Systems, 2016, 27(2): 444-458.

[27] Huang J, Yin Y, Duan Q, et al. A game-theoretic analysis on context-aware resource allocation for device-to-device communications in cloud-centric Internet of things[C]. The 3rd International Conference on Future Internet of Things and Cloud. Rome, 2015: 80-86.

[28] Feng D Q, Lu L, Yi Y W, et al. Device-to-device communications underlaying cellular networks[J]. IEEE Transactions on Communications, 2013, 61(8): 3541-3551.

[29] Gu Y N, Zhang Y R, Pan M, et al. Matching and cheating in device to device communications underlying cellular networks[J]. IEEE Journal on Selected Areas in Communications, 2015, 33(10): 2156-2166.

[30] Zheng Z J, Song L Y, Niyato D, et al. Resource allocation in wireless powered relay networks: A bargaining game approach[J]. IEEE Transactions on Vehicular Technology, 2017, 66(7): 6310-6323.

[31] Zhang H J, Jiang C X, Beaulieu N C, et al. Resource allocation for cognitive small cell networks: A cooperative bargaining game theoretic approach[J]. IEEE Transactions on Wireless Communications, 2015, 14(6): 3481-3493.

[32] Yang B, Li Z, Chen S, et al. Stackelberg game approach for energy-aware resource allocation in data centers[J]. IEEE Transactions on Parallel and Distributed Systems, 2016, 27(12): 3646-3658.

[33] Aujla G S, Singh M, Kumar N, et al. Stackelberg game for energy-aware resource allocation to sustain data centers using RES[J]. IEEE Transactions on Cloud Computing, 2019, 7(4): 1109-1123.

[34] Ramírez-Llanos E, Quijano N. A population dynamics approach for the water distribution problem[J]. International Journal of Control, 2010, 83(9): 1947-1964.

[35] Marden J R, Ruben S D, Pao L Y. A model-free approach to wind farm control using game theoretic methods[J]. IEEE Transactions on Control Systems Technology, 2013, 21(4): 1207-1214.

[36] Du L, Grijalva S, Harley R G. Game-theoretic formulation of power dispatch with guaranteed convergence and prioritized best response[J]. IEEE Transactions on Sustainable Energy, 2015, 6(1): 51-59.

[37] 梁易乐, 刘锋, 梅生伟. 基于状态势博弈的电力系统分布式经济调度方法[J]. 系统科学与数学, 2016, 36(3): 413-425.
(Liang Y L, Liu F, Mei S W. A state-based potential game approach for distributed economic dispatch[J]. Journal of Systems Science and Mathematical Sciences, 2016, 36(3): 413-425.)

[38] Zhang R R, Guo L. Controllability of Nash equilibrium in game-based control systems[J]. IEEE Transactions on Automatic Control, 2019, 64(10): 4180-4187.

[39] Bauer A, Wollherr D, Buss M. Human-robot collaboration: A survey[J]. International Journal of Humanoid Robotics, 2008, 5(1): 47-66.

[40] Chen J, Zhang X, Xin B, et al. Coordination between unmanned aerial and ground vehicles: A taxonomy and optimization perspective[J]. IEEE Transactions on Cybernetics, 2016, 46(4): 959-972.

[41] Chen J Y C, Barnes M J. Human-agent teaming for multirobot control: A review of human factors issues[J]. IEEE Transactions on Human-Machine Systems, 2014, 44(1): 13-29.

[42] Chen J Y C, Barnes M J, Harper-Sciarini M. Supervisory control of multiple robots: Human-performance issues and user-interface design[J]. IEEE Transactions on Systems, Man, and Cybernetics — Part C: Applications and Reviews, 2011, 41(4): 435-454.

[43] 陈杰, 辛斌. 有人/无人系统自主协同的关键科学问题[J]. 中国科学: 信息科学, 2018, 48(9): 1270-1274.
(Chen J, Xin B. Key scientific problems in the autonomous cooperation of manned-unmanned systems[J]. Scientia Sinica: Informationis, 2018, 48(9): 1270-1274.)

[44] 牛轶峰, 沈林成, 李杰, 等. 无人-有人机协同控制关键问题[J]. 中国科学: 信息科学, 2019, 49(5): 538-554.
(Niu Y F, Shen L C, Li J, et al. Key scientific problems in cooperation control of unmanned-manned aircraft systems[J]. Scientia Sinica: Informationis, 2019, 49(5): 538-554.)

[45] Yang H, Han Q L, Ge X H, et al. Fault-tolerant cooperative control of multiagent systems: A survey of trends and methodologies[J]. IEEE Transactions on Industrial

Informatics, 2020, 16(1): 4-17.

[46] Shi J T, Zhou D H, Yang Y H, et al. Fault tolerant multivehicle formation control framework with applications in multiquadrotor systems[J]. Science China Information Sciences, 2018, 61(12): 1-3.

[47] Liu C, Jiang B, Patton R J, et al. Hierarchical-structure-based fault estimation and fault-tolerant control for multiagent systems[J]. IEEE Transactions on Control of Network Systems, 2019, 6(2): 586-597.

[48] Liu Y, Yang G H. Integrated design of fault estimation and fault-tolerant control for linear multi-agent systems using relative outputs[J]. Neurocomputing, 2019, 329: 468-475.

[49] Yang H, Zhang C C, An Z X, et al. Exponential small-gain theorem and fault tolerant safe control of interconnected nonlinear systems[J]. Automatica, 2020, 115: 108866.

[50] Xu Y H, Yang H, Jiang B. Fault-tolerant control of multilayer interconnected nonlinear systems: An inclusion principle approach[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2021, 51(4): 2403-2414.

[51] 王群. 网络攻击与防御技术[M]. 北京: 清华大学出版社, 2019: 1-20.
(Wang Q. Network attack and defence [M]. Beijing: Tsinghua University Press, 2019: 1-20.)

[52] 石荣, 刘畅. 信息战中通信干扰与主动网络攻击的特性对比[J]. 通信技术, 2020, 53(5): 1138-1145.
(Shi R, Liu C. Comparison of communication jamming and active network attack in information warfare[J]. Communications Technology, 2020, 53(5): 1138-1145.)

[53] Policy S. National institute for standards and technology[M]. New York: Springer US, 2009: 1001.

[54] 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.

[55] Pries R, Yu W, Fu X, et al. A new replay attack against anonymous communication networks[C]. IEEE International Conference on Communications. Beijing, 2008: 1578-1582.

[56] 赖英旭, 刘增辉, 蔡晓田, 等. 工业控制系统入侵检测研究综述[J]. 通信学报, 2017, 38(2): 143-156.
(Lai Y X, Liu Z H, Cai X T, et al. Research on intrusion detection of industrial control system[J]. Journal on Communications, 2017, 38(2): 143-156.)

[57] Hao J P, Piechocki R J, Kaleshi D, et al. Sparse malicious false data injection attacks and defense mechanisms in smart grids[J]. IEEE Transactions on Industrial Informatics, 2015, 11(5): 1-12.

[58] 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.

[59] Gadiraju U, Kawase R, Dietze S, et al. Under standing malicious behavior in crowdsourcing platforms: Thecase of online surveys[C]. Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems. New York: ACM, 2015: 1631-1640.

[60] Sain R, Khari M. Defining malicious behavior of a node and its defensive techniques in ad hoc networks[J]. International Journal of Smart Sensor and Adhoc Network, 2011: 17-20.

[61] Shang Y L. Consensus of hybrid multi-agent systems with malicious nodes[J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2020, 67(4): 685-689.

[62] Camerer C F. Behavioral game theory: Experiments in strategic interaction[M]. Princeton: Princeton University Press, 2011: 1-24.

[63] Marden J R, Young H P, Arslan G, et al. Payoff-based dynamics for multiplayer weakly acyclic games[J]. SIAM Journal on Control and Optimization, 2009, 48(1): 373-396.

[64] Eliaz K. Fault tolerant implementation[J]. The Review of Economic Studies, 2002, 69(3): 589-610.

[65] Aiyer A S, Alvisi L, Clement A, et al. BAR fault tolerance for cooperative services[C]. Proceedings of the 20th ACM Symposium on Operating Systems Principles. New York: ACM, 2005: 45-58.

[66] Chen J, Micali S. Collusive dominant-strategy truthfulness[J]. Journal of Economic Theory, 2012, 147(3): 1300-1312.

[67] Gradwohl R, Reingold O. Fault tolerance in large games[J]. Games and Economic Behavior, 2014, 86: 438-457.

[68] Gradwohl R, Kalai E. Large games: Robustness and stability[J]. Annual Review of Economics, 2021, 13(1): 39-56.

[69] Yin S, Luo H, Ding S X. Real-time implementation of fault-tolerant control systems with performance optimization[J]. IEEE Transactions on Industrial Electronics, 2014, 61(5): 2402-2411.

[70] Azizi S M, Khorasani K. Cooperative actuator fault accommodation in formation flight of unmanned vehicles using relative measurements[J]. International Journal of Control, 2011, 84(5): 876-894.

[71] Azizi S M, Khorasani K. A hierarchical architecture for cooperative actuator fault estimation and accommodation of formation flying satellites in deep space[J]. IEEE Transactions on Aerospace and Electronic Systems, 2012, 48(2): 1428-1450.

[72] Tousi M M, Khorasani K. Optimal hybrid fault recovery in a team of unmanned aerial vehicles[J]. Automatica, 2012, 48(2): 410-418.

[73] Ogretim E O, Huebsch W W, Narramore J, et al. Investigation of relative humidity and induced-vortex effects on aircraft icing[J]. Journal of Aircraft, 2007, 44(6): 1805-1814.

[74] Lampton A, Valasek J. Prediction of icing effects on the lateral/directional stability and control of light airplanes[C]. AIAA Atmospheric Flight Mechanics Conference and Exhibit. DOI: 10.2514/6.2006-6834.

[75] Grunnet J D, Bendtsen J D, Bak T. Automated fault tolerant control synthesis based on discrete games[C]. Proceedings of the 48h IEEE Conference on Decision and Control. Shanghai, 2009: 8476-8481.

[76] Yuan Y, Zhang P, Li X L. Synchronous fault-tolerant near-optimal control for discrete-time nonlinear PE game[J]. IEEE Transactions on Neural Networks and Learning Systems, 2021, 32(10): 4432-4444.

[77] Zhang B H, Lu S B. Fault-tolerant control for four-wheel independent actuated electric vehicle using feedback linearization and cooperative game theory[J]. Control Engineering Practice, 2020, 101: 104510.

[78] Zhang B H, Lu S B, Wu W J, et al. Robust fault-tolerant control for four-wheel individually actuated electric vehicle considering driver steering characteristics[J]. Journal of the Franklin Institute, 2021, 358(11): 5883-5908.

[79] Zhu Q Y, Basar T. Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: Games-in-games principle for optimal cross-layer resilient control systems[J]. IEEE Control Systems Magazine, 2015, 35(1): 46-65.

[80] Xu Y H, Jiang B, Yang H. Two-level game-based distributed optimal fault-tolerant control for nonlinear interconnected systems[J]. IEEE Transactions on Neural Networks and Learning Systems, 2020, 31(11): 4892-4906.

[81] Xu Y H, Yang H, Jiang B, et al. Distributed optimal fault estimation and fault-tolerant control for interconnected systems: A stackelberg differential graphical game approach[J]. IEEE Transactions on Automatic Control, 2021, 4284(99): 1-10.

[82] Sun W, Kong X W, He D Q, et al. Information security problem research based on game theory[C]. International Symposium on Electronic Commerce and Security. Guangzhou, 2008: 554-557.

[83] Kamhoua C A, Pissinou N, Makki K. Game theoretic modeling and evolution of trust in autonomous multi-hop networks: Application to network security and privacy[C]. IEEE International Conference on Communications. Kyoto, 2011: 1-6.

[84] 王锐, 朱青林, 钱德沛, 等. 一种可容错的覆盖网节点合作激励策略[J]. 电子学报, 2010, 38(2): 327-332.
(Wang R, Zhu Q L, Qian D P, et al. A fault-tolerant cooperation incentive strategy for overlay network nodes[J]. Acta Electronica Sinica, 2010, 38(2): 327-332.)

[85] 沈士根, 马绚, 蒋华, 等. 基于演化博弈论的WSNs信任决策模型与动力学分析[J]. 控制与决策, 2012, 27(8): 1133-1138.
(Shen S G, Ma X, Jiang H, et al. Evolutionary game theory based trust strategy model and dynamics analysis in wireless sensor networks[J]. Control and Decision, 2012, 27(8): 1133-1138.)

[86] Tsai J, Yin Z, Kwak J Y, et al. Urban security: Game-theoretic resource allocation in networked physical domains[C]. The 24th Aaai Conference on Artificial Intelligence DBLP. New York: AAAI, 2011: 1-10.

[87] Kiekintveld C, Jain M, Tsai J, et al. Security and game theory: Computing optimal randomized resource allocations for massive security games[M]. Cambridge: Cambridge University Press, 2011: 193-253.

[88] Panfili M, Giuseppi A, Fiaschetti A, et al. A game-theoretical approach to cyber-security of critical infrastructures based on multi-agent reinforcement learning[C]. The 26th Mediterranean Conference on Control and Automation. Zadar, 2018: 460-465.

[89] Riehl J R, Cao M. A centrality-based security game for multihop networks[J]. IEEE Transactions on Control of Network Systems, 2018, 5(4): 1507-1516.

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

[91] Dolk V S, Tesi P, De Persis C, et al. Event-triggered control systems under denial-of-service attacks[J]. IEEE Transactions on Control of Network Systems, 2017, 4(1): 93-105.

[92] Feng S, Tesi P. Resilient control under denial-of-service: Robust design[C]. American Control Conference. Boston, 2016: 4737-4742.

[93] Zhu Q, Xu Z. Cross-layer design for secure and resilient cyber-physical systems[M]. Berlin: Springer, 2020: 9-15.

[94] Xu Z H, Zhu Q Y. Cross-layer secure cyber-physical control system design for networked 3D printers[C]. American Control Conference. Boston, 2016: 1191-1196.

[95] Xu Z H, Zhu Q Y. A cyber-physical game framework for secure and resilient multi-agent autonomous systems[C]. The 54th IEEE Conference on Decision and Control. Osaka, 2015: 5156-5161.

[96] Kahneman D, Tversky A. Prospect theory: An analysis of decision under risk[Z]. 2013: 99-127.

[97] Wang L, Wang Y M, Martínez L. A group decision method based on prospect theory for emergency situations[J]. Information Sciences, 2017, 418/419: 119-135.

[98] Prelec D. The probability weighting function[J]. Econometrica, 1998, 66(3): 497-527.

[99] Tversky A, Kahneman D. Advances in prospect theory: Cumulative representation of uncertainty[J]. Journal of Risk and Uncertainty, 1992, 5(4): 297-323.

[100] Jaggi S, Langberg M, Katti S, et al. Resilient network coding in the presence of Byzantine adversaries[C]. IEEE Inforcom 26th IEEE International Conference on Computer Communications. Anchorage, 2007: 616-624.

[101] Paarporn K, Canty B, Brown P N, et al. The impact of complex and informed adversarial behavior in graphical coordination games[J]. IEEE Transactions on Control of Network Systems, 2020, 8(1): 200-211.

[102] 倪媛, 杨浩, 姜斌. 蜂群对抗决策故障下的容错博弈控制[J]. 航空学报, 2021, 42(4): 534-545.
(Ni Y, Yang H, Jiang B. Fault tolerant game control of swarm confrontation with decision faults [J]. Acta Aeronautica et Astronautica Sinica, 2021, 42(4): 534-545.)

[103] Lu S, Yang H, Jiang B. Fault tolerant control of centralized potential games[C]. The 39th Chinese Control Conference. Shenyang, 2020: 4233-4238.

[104] Zheng X P, Wu W H, Deng W F, et al. Reconstruction of tree network via evolutionary game data analysis[J]. IEEE Transactions on Cybernetics, DOI: 10.1109/TCYB.2020.3043227.

[105] 吴立珍, 牛轶峰, 王菖, 等. 多无人机监督控制系统设计与实践[J]. 无人系统技术, 2020, 3(4): 42-52.
(Wu L Z, Niu Y F, Wang C, et al. Design and practice of supervisory control system for multiple unmanned aircraft systems[J]. Unmanned Systems Technology, 2020, 3(4): 42-52.)

[106] 杨伟. 关于未来战斗机发展的若干讨论[J]. 航空学报, 2020, 41(6): 524377.
(Yang W. Development of future fighters[J]. Acta Aeronautica et Astronautica Sinica, 2020, 41(6): 524377.)

[107] Sanjab A, Saad W, Baar T. A game of drones: Cyber-physical security of time-critical UAV applications with cumulative prospect theory perceptions and valuations[J]. IEEE Transactions on Communications, 2020, 68(11): 6990-7006.

作者简介

杨浩(1982–), 男, 教授, 博士生导师, 从事切换与网络系统的控制、优化、博弈与容错等研究, E-mail: haoyang@nuaa.edu.cn;

许宇航(1993–), 女, 博士生, 从事动态系统容错控制与容错博弈的研究, E-mail: xuyuhang@nuaa.edu.cn;

倪媛(1997–), 女, 博士生, 从事动态系统容错控制与容错博弈的研究, E-mail: yuanni@nuaa.edu.cn;

路石(1995–), 男, 博士生, 从事动态系统容错控制与容错博弈的研究, E-mail: lushi@nuaa.edu.cn;

姜斌(1966–), 男, 教授, 博士生导师, 从事故障诊断、容错控制与健康管理及其应用等研究, E-mail: binjiang@nuaa.edu.cn.

科研团队简介

南京航空航天大学姜斌教授带领的“故障诊断与健康管理团队”是江苏省“青蓝工程”创新科研团队,以国防特色学科、江苏省优势学科、工信部和江苏省重点实验室等平台为依托,在智能系统安全运行和维护的学术以及应用研究方面取得了系统性创新成果.

团队聚焦学术难题,建立了故障诊断与容错控制一体化设计理论,形成一套面向多模态切换、网络化集群等典型复杂特性的动态系统故障诊断与容错控制理论体系,为基础控制理论的发展和工程系统安全技术的推进做出了重要贡献. 面向国防重大需求,突破了单机和集群飞行器故障注入、智能诊断与协同容错控制关键技术,建立了航天器寿命预测、动态监测、故障诊断与重构控制的健康管理体系,有力推动了飞行器安全控制技术的发展. 同时,面向国家重大工程,攻克了高速列车牵引系统建模、微小和复合故障智能诊断与容错的技术瓶颈,产生了可观的经济效益,为提升我国轨道车辆的安全性提供了重要技术支撑.

团队近年来承担了国家自然科学基金重大项目课题、重点项目、国际合作重点项目、国家优秀青年基金,牵头负责国家重点研发计划项目、高等学校学科创新引智计划项目等国家级项目,获得国家自然科学二等奖、江苏省科学技术一等奖、中国自动化学会与航空学会的优秀博士论文奖等. 团队负责人姜斌教授是教育部“长江学者”特聘教授、电子电气工程师学会(IEEE)会士、国际系统与控制科学院院士、亚太人工智能协会(AAIA)会士、中国自动化学会会士. 2014～2020年连续获评“Elsevier中国高被引学者”.

(责任编辑: 郑晓蕾)