CAA 中国自动化学会

中国自动化学会通讯

COMMUNICATIONS OF CAA

主办：中国自动化学会 http: //www.caa.org.cn E-mail: caa@ia.ac.cn

控制系统安全

扫描二维码 关注官方微信

扫描二维码 关注官方微博

ISSN 2151-335X

6 915920 700067

2016年8月

第4期

第37卷 总第187期

Contents 目

第37卷 第4期 总第187期 2016年8月 www.caa.org.cn 主办单位：中国自动化学会

主编寄语

信息通信技术与物理过程的协同作用为控制系统引入了新的功能，提高了它们的操作性能和智能化水平，但同时也引发了信息物理系统的安全性问题。为此，越来越多的专家学者投入这一领域，引发了新一轮的研究热潮。

为促进自动化及其他相关领域的研究人员了解控制系统安全研究的最新进展，《中国自动化学会通讯》2016年第四期专刊关注控制系统信息安全。感谢浙江大学教授、中国自动化学会副秘书长陈积明，他作为本期专刊的召集人，组织来自大学、研究所的专家学者，分别从信息物理系统、工业控制系统信息、网络化控制系统的安全性问题介绍领域研究和发展的动态，同时为本刊作序。

《信息物理系统的安全性和隐私性问题绪论》介绍了信息物理系统中安全性和隐私性的基本概念和问题。《弹性分布式能量管理研究》介绍了美国北卡罗来纳州立大学实验室提出的分布式能量管理算法，并针对信息交流安全问题，提出了基于“邻里守望”原理的分布式弹性控制模型。《工业控制系统信息安全防护中的风险评估方法及技术》从定量评估、定性评估、定量定性相结合的评估三种评估方法入手，对工业控制系统信息安全主流的风险评估方法进行了概括描述，并分析不同方法的优缺点。《控制系统安全的理论与应用研究进展》通过介绍实验成功的攻击模型，分析了现有系统存在的安全隐患，并重点介绍了对控制系统攻击的检测与辨识、弹性状态估计器及控制器等方向的研究进展。《网络化控制系统安全问题研究现状与挑战》总结了攻击建模、攻击特征与系统性能内在联系、攻击入侵检测机制、攻击防御机制等方面取得的研究成果，并指出了当前仍然面临并亟待解决的几大难题。《信息物理系统中的传感器信息完整性攻击》介绍了控制领域在攻击检测、攻击辨识以及安全状态估计方面的研究成果，并提出了基于控制理论的安全研究应与传统的信息安全相结合，从而实现对信息物理系统的多方位保护。《智能电网中通信组网的网络安全综述》介绍了通信组网的结构特点，并分析了DoS攻击检测与防御、安全通信协议、匿名通信等多种技术的应用。

郭南宁

本刊声明

为支持学术争鸣，本刊会登载学术观点彼此相左的不同文章。来稿是否采用并不反映本刊在学术分歧或争论中的立场。每篇文章只反映作者自身的观点，与本刊无涉。

录

Chinese Association of Automation

中国自动化学会通讯

Communications of CAA

形势通报

学会动态

党建强会

刊名题字：宋　健

编辑：中国自动化学会办公室

地址：北京市海淀区中关村东路95号　　邮编：100190

电话：(010) 8254 4542　E-mail: caa@ia.ac.cn

传真：(010) 6252 2248　http: //www.caa.org.cn

编辑委员会

关注官方微信　　关注官方微博

《中国自动化学会通讯》控制系统安全专刊序

程　鹏，陈积明

浙江大学

控制系统安全现状

控制系统，是包括物联网、智能电网、传感器网络等大规模应用系统的核心，其应用已经覆盖众多国民经济重大关键领域，如电力、石油、化工等能源行业，航空、铁路等交通行业，水处理、供暖、环境监测等市政服务行业。通过合理的反馈设计，物理空间与信息空间能够深度耦合、相互作用。由于反馈机制的引入，使得即使在内外部存在各种不确定性影响的情况下，控制系统仍然能够提供稳定可靠的系统性能和系统服务。

在泛在感知、估计与控制的内在要求下，依托嵌入式系统、通讯技术、控制技术、计算技术的不断革新，控制系统规模日益增大，逐步向分布式化、智能化迅速发展，并影响着国民经济的发展和人民生产生活。但与此同时，控制系统的内在与外在环境使得其正面临日益增大的安全威胁。从控制系统自身来看，由于通用操作系统、以太网通信等技术的广泛应用，导致控制系统的开放性日益增强，面临的安全风险也不断增加；而从外部环境看，攻击者的系统漏洞发现能力与攻击技术也不断提升，控制系统安全威胁日益升级。安全理论及其关键技术已成为控制系统发展与应用亟待克服的重大研究课题。

近年来世界范围内频繁发生的重大安全事件，将控制系统安全提升至前所未有的高度。2008年，攻击者入侵波兰某市的地铁系统，通过电视遥控器越过控制系统，改变轨道扳道器，导致4节车厢脱轨。2010年，“震网”病毒（Stuxnet）利用工业控制系统漏洞造成伊朗布尔什核电站核反应堆长时间无法运营。2011年，美国伊利诺伊州城市供水系统，由于数据采集和监控系统被入侵，大量供水泵被烧毁。2011年，全球独立安全检测机构NSSLabs发布报告称，西门子的一个工业控制系统存在新的漏洞，易遭受攻击。2012年，破坏力巨大的“火焰（Flame）”病毒对中东地区石油工业中的控制系统的正常运行造成了很大的冲击。另外，据美国国土安全部ICS-CERT统计，工业系统安全事件数已由2012财年的197起快速增加到2015年财年的295起。

鉴于控制系统对人类生产生活的重要性和潜在安全隐患的巨大破坏效应，世界各国都已大力开展控制系统安全相关的科学理论和实践研究，如何保障网络化控制系统安全已经成为世界范围的前沿课题。美国国家科学基金已经将控制系统安全作为一个重要的研究领域。美国国土安全部于2006年制定了“国家基础设施保护计划”，并通过其下属的“国家网控安全机构”开始实施“控制系统安全项目”。2010年英国发布了国家安全策略，拨款6.5亿英镑开展为期四年的“国家网控安全项目”，以支持工业控制系统安全研究。2012年日本发起“工业控制系统网络安全项目”，以保护日本重要基础和工业设施的安全。2013年，欧洲网络与信息安全局发布了《工业控制系统网络安全白皮书》，要求欧盟及其成员国针对工业控制系统的网络攻击事件做出灵活和综合应对。

近年来，我国也逐步将控制系统安全相关研

究纳入国家重点支持的研究领域。其中，国家中长期科学和技术发展规划纲要（2006-2020年）将信息安全列为优先发展的前沿技术。2011年9月工业和信息化部发布《关于加强工业控制系统信息安全管理的通知》，明确提出“加强工业控制系统信息安全管理”。2012年6月国务院在《关于大力推进信息化发展和切实保障信息安全的若干意见》中明确要求“保障工业控制系统的安全，加强重要领域工业控制系统，以及物联网应用、数字城市建设中的安全防护和管理”。2013年，国家发改委将工业控制信息安全领域列为国家信息安全专项重点支持的四大领域之一。2016年科技部发布的“国家网络空间安全”国家重点研发计划中特别强调控制系统安全的重要性，并且将工业控制系统深度安全技术列为重要共性关键技术类研究方向。

研究趋势分析

相比于传统的信息系统安全问题，控制系统安全问题存在很大区别。从目的性来看，信息系统关注如何保护信息本身安全性、机密性、完整性；而控制系统安全必须同时考虑信息空间和物理空间的恶意攻击对闭环系统性能与系统服务的影响。从运行系统特性来看，信息系统面向信息化领域的运行管理，所使用软件需要经常更新来适应最新的病毒；而控制系统针对大量实时动态过程，必须保证系统长期运行安全可靠。从研究挑战性来看，控制系统将面临包括信息空间攻击、物理空间攻击等多维度复杂攻击模态，且攻击与系统行为作用机理复杂，系统失控将对国民经济产生重大损失。因此，传统的信息安全方法已经不足以保障控制系安全，迫切需要开展控制系统安全理论和技术的研究。

目前，根据研究切入点的不同，可以将针对控制系统安全问题的研究分为两大类：①信息物理融合视角下的控制系统安全问题。该类问题研究需要把握信息空间与物理空间交互融合、信息安全与物理安全深度耦合的特点。现有研究多数通过系统冗余信息和系统物理动态演化特征构建安全防御技术，初步实现了信息物理融合安全防护，但是基于信息物理耦合特征的深度安全防护技术研究相对缺乏。②以电力网络、车联网、工业过程控制网等为代表的具体网络系统的安全控制问题。这类问题研究主要包括以具体网络系统物理性能安全为目标和以网络信息安全为目标的安全防护技术研发。其中物理性能安全主要通过分析系统物理演化的静态或者动态特征，设计风险评估和安全防御机制，信息安全方面的研究则基于具体网络系统的信息特性和传统信息安全技术构建安全防护方法。而研究具体网络系统在信息物理交互融合下的安全问题相对缺乏。

大数据、机器学习和人工智能的兴起和飞速发展必然推动控制系统走向更加智能、更加开放，也必将加剧控制系统安全风险。因而，未来的研究也需要充分吸收大数据、机器学习和人工智能等技术优势，构建信息物理深度安全融合的控制系统安全理论和关键技术，实现针对不断升级的复杂攻击的深度立体全面防御，有力保障控制系统安全稳定与高效运行。

本专刊内容提要

本刊邀请来自控制系统安全不同领域的专家学者撰文从不同视角介绍控制系统安全的发展状况和趋势。八篇文章的作者分别来自国内外知名大学，其中前四篇从信息物理融合安全控制角度和后四篇从具体网络系统的安全控制角度全面介绍了该领域的前沿问题。

美国宾夕法尼亚州立大学的路洋、胡智圣、朱明辉的文章《信息物理系统的安全性和隐私性问题绪论》从信息空间和物理世界的强耦合性引出了两个新的挑战，即安全性和隐私性。针对安全性，从攻击模型、安全检测、抗攻击控制、安全经济四个方面梳理当前研究热点问题。对于隐私性，介绍了破坏隐私的攻击模型、隐私的概念和典型的隐私增强机制。

新加坡南洋理工大学的莫一林、韩铎、谢立华的文章《信息物理系统中的传感器信息完整性攻击》介绍了信息完整性攻击下的系统演化模

型，总结了针对信息完整性攻击的入侵检测机制、攻击辨识和安全状态估计方面取得的最新研究成果，并指出研究中存在的不足之处。

张恒（淮海工学院）、何建平（加拿大维多利亚大学）、程鹏（浙江大学）、王文海（浙江大学）、陈积明（浙江大学）的文章《网络化控制系统安全问题研究现状与挑战》从攻击建模、攻击特征与系统性能内在联系、攻击入侵检测机制、攻击防御机制等方面概述了网络化控制系统安全方向当前热点问题和最新研究成果，并且指出了该方向研究的一些开放问题和面临的研究挑战。

美国宾夕法尼亚大学苗菲的文章《控制系统安全的理论与应用研究进展》结合美国宾夕法尼亚大学的PRECISE LAB 课题组在理论和应用层面取得的重要成果，阐述了针对信息物理系统的攻击实现、对控制系统攻击的检测和辨识、弹性状态估计器及控制器等方面的前沿问题，指出今后需要聚焦非线性、大规模非同质网络系统的安全理论，并结合自动驾驶车、智能城市等应用研发安全可靠的信息物理系统。

加拿大阿尔伯塔大学的邓瑞龙、梁浩的文章《智能电网数据注入攻击与防御综述》围绕智能电网安全问题研究前沿，综述了数据注入攻击问题的研究历程，细致阐述了数据注入攻击的构造和防御技术，并指出在分布式的数据注入攻击与防御、基于博弈论的信息安全策略、资源有效的防御优化等方面依然存在许多亟待解决的问题。

美国纽约州立大学布法罗分校的秦湛、任奎的文章《智能电网中通信组网的网络安全综述》从系统架构、功能需求等方面介绍了智能电网通信组网不同于一般网络的特点，从网络攻击的侦测与防御性、数据认证与访问控制以及安全通信协议三个方面比较了通信组网的安全需求和传统互联网安全需求的差异，总结了当前基于网络与密码技术的安全机制，并指出智能电网通信组网安全研究尚未成熟，仍有大量急需解决的问题。

美国北卡罗来纳州立大学段杰、周武元的文章《弹性分布式能量管理研究》介绍了分布式能量管理系统可能遭受的恶意攻击及其严重后果，阐述了北卡罗来纳州立大学ADAC实验室提出的分布式能量管理算法，并基于信息交流的安全性需求构建了一种分布式弹性控制模型，通过动态调整一致性网络的权重因子实现攻击下系统信息的准确估计。

华中科技大学周纯杰、张琦、秦元庆的文章《工业控制系统信息安全防护中的风险评估方法及技术》从定量评估、定性评估和定量定性相结合的评估三个方面概述了工业控制系统信息安全主流的风险评估方法，分析了现有方法的优缺点，并指出了工控系统风险评估存在的问题以及面临的严峻挑战，需要从战略高度重视风险评估，建立健全各类配套的安全标准和法规，全力保障工控系统安全。

作者简介

程鹏　浙江大学控制学院教授、博士生导师。主要研究领域为工业控制系统安全、网络化系统估计与控制、信息物理融合系统等。先后承担国家自然科学基金重大/重点项目，科技部863计划、支撑计划项目等国家级项目10余项，并担任国家重点研发计划"内生安全的主动防御工控系统防护技术研究"课题技术负责人。成果在ACM MobiSys, ACM MobiHoc、IEEE INFOCOM和IEEE TAC、IEEE TDSC、Automatica等发表论文50余篇。获IEEE ICCC'14 Best Pape Award、IEEE INFOCOM'14 Best Demo Award，2014年教育部科技进步一等奖，以及日本学术振兴会JSPS Fellowship等荣誉。担任IEEE Trans. Control of Network Systems，Wireless Networks等国际期刊编委，并任IEEE TCNS 信息物理融合系统安全控制特刊特邀编委。

陈积明　教育部长江学者特聘教授，浙江大学工业控制技术国家重点实验室副主任。入选中组部首批万人计划（青年拔尖人才）、教育部新世纪人才、IEEE VTS Distinguished Lecturer等；曾获教育部科技进步一等奖、教育部霍英东青年教师奖、IEEE通信学会亚太区杰出青年研究学者奖等荣誉。主要研究领域为传感网、网络优化与控制、控制系统安全等。

信息物理系统的安全性和隐私性问题绪论

路　洋，胡智圣，朱明辉

School of Electrical Engineering and Computer Science，Pennsylvania State University，201 Old Main，University Park，PA 16802，USA

1　引言

在过去的几十年中，计算和通信设备的功耗、移动性和效率均获得了突飞猛进的发展，促进了信息和通信技术的广泛应用。其中，互联网就是人类最伟大的发明之一。最近，信息和通信技术正越来越多地与物理世界中的控制系统集成在一起，产生了很多新一代的工程应用，包括智能电网、智能建筑、智能交通系统、自动驾驶汽车以及医疗设备网络。这些新一代的系统被统称为信息物理系统（Cyber-Physical Systems）。信息通信技术与物理过程的协同作用为控制系统引入了新的功能，提高了它们的操作性能，使其实现前所未有的智能化。美国国家科学基金会预计信息物理系统技术将会改变人类与工程系统的交互方式——就像互联网改变了人类与信息交互的方式一样[1]。最近的一份报告估计，信息物理系统的技术创新能够被直接应用于目前经济总值超过32.3万亿美元经济活动的各类部门中，并且有望在2025年达到82万亿美元的输出——约为全球经济总量的二分之一[2]。美国和欧洲都已将信息物理系统列入科研投入的优先领域。

信息物理系统的显著特点是其信息空间与物理世界的强耦合。然而，这一强耦合带来了两个新的挑战：安全性和隐私性。在信息物理系统的安全性问题中，攻击者利用信息基础设施中固有的弱点中止信息物理系统任务，破坏物理机器。在信息物理系统的隐私性问题中，攻击者利用合法实体公开的数据来推断他们的隐私数据。就经典的CIA三合体（保密性、完整性、可用性）而言，信息物理系统的隐私性涉及保密性，而信息物理系统的安全性涉及完整性和可用性。

2　信息物理系统的安全性

信息通信技术系统容易受到包括阻塞攻击和缓冲区溢出攻击在内的网络攻击。这些信息安全漏洞可以被攻击者用来突破网络防御，瘫痪控制系统，甚至会给物理世界造成损害。此外，很多信息物理系统都是大规模网络系统，其各个部分在地理上分布于相距较远的广阔区域。广域布局扩大了受攻击范围，攻击者可以通过瘫痪一部分结点进而潜在地瓦解整个网络。信息物理系统易受网络攻击的弱点在最近的一系列事故中得以证实。2000年，一名普通人仅用一台笔记本电脑和一部无线电发射器就控制了150个污水泵站。在

三个月内，他向一个雨水渠排放了一百万升未经处理的污水，这些污水经雨水渠流向当地水道。2006年，两名交通工程师入侵了洛杉矶交通灯控制系统，延长了红灯的时间，导致交通陷入拥堵。2010年，恶意软件Stuxnet攻击了工业可编程逻辑控制器，据说这一攻击摧毁了伊朗近五分之一的核离心机[3]。2011年，一架美国无人机被伊朗网络战部队击落。2013年，美国工业控制系统网络应急小组收到了181次关于工业控制系统漏洞的报告[4]。很多信息物理系统在社会中发挥着关键作用，这对保护信息物理系统免受网络攻击提出了迫切需求。对于信息物理系统的安全性问题，以下四个方面至关重要：攻击模型、安全检测、抗攻击控制以及安全经济。

2.1　攻击模型

最常见的攻击包括拒绝服务、重放、欺骗攻击和恶意软件。拒绝服务攻击[61]拦阻数据发送者和接收者之间的通信。重放攻击[62]向数据接收者重新发送过时的消息。欺骗攻击或隐蔽攻击[63]篡改所传输的数据。恶意软件[64]修改、破坏、窃取信息或者获得对系统资源的非授权访问。

2.2　安全检测

在信息通信技术系统中，入侵检测系统用于检测信息空间中的异常行为。从功能上，它们可以分为三类：基于异常的检测[5-7]、基于特征的检测[8]、基于规范的检测[9]。然而，传统的入侵检测系统没有考虑物理世界，因此可能会漏掉其中的异常行为。所以传统的入侵检测系统对信息物理系统的安全检测能力尚且不足。最近已经有了基于物理世界的检测器，以弥补现有入侵检测系统的不足[10-15]。其中，文献[13]研究了攻击检测和识别中的基本限制。文献[11]将攻击检测构造为一个零范数优化问题，一般来说，该优化问题是NP-hard。为得到凸松弛，零范数被一范数所代替。文献[12]将这一方法扩展到含有已知有界扰动的系统。文献[15]设计了一类未知输入状态滤波器以检测随机线性动态系统中的数据注入攻击和切换攻击。

2.3　抗攻击控制

当前的信息通信技术系统的防御机制是通过缓慢精细的过程来管理的，如测试和补丁过程。据文献[71]报告，2014年名列前五的零日攻击所需平均补丁时间是59天。显然，这一缓慢过程与控制系统的快速变化不相匹配，这对开发新的抗攻击信息物理系统方案提出了迫切的需求，即控制系统自动应对恶意攻击，避免任务失败并在信息漏洞修复前尽量减少系统性能的下降。文献[16]和文献[17]将有限时域线性二次高斯控制问题描述为一对控制器和干扰机之间的动态零和博弈。文献[18]利用博弈论开发了一种分层架构，保证了跨层安全性。文献[19]研究了拒绝服务攻击下的事件触发控制。文献[20]和文献[21]讨论了针对无人机群抵抗拒绝服务攻击、重放攻击以及欺骗攻击的分布式抗攻击编队控制。

2.4　安全经济

在很多信息物理系统中，各参与者的利益往往是不同的，因此，系统级别的安全性可能并不是每个个体的最佳利益所在。单个参与者的安全性失败可能会通过各参与者之间的相互联系加以传播，并进一步导致整个系统安全性的崩溃。微观经济学为解决这一问题提供了可能的方案。通过给予参与者金钱奖励来激励他们参与执行信息物理系统的安全性保护机制。文献[22]研究了无穷时域线性二次高斯问题中抵抗拒绝服务攻击的安全独立性，并全面描述了安全投资博弈问题的纳什均衡点性质。文献[23]将一类抗攻击网络控制系统的合作（相应地，竞争）资源分配问题构造为凸规划（相应地，凸博弈）问题。

3 信息物理系统隐私性

信息物理系统由大量地理上分散的实体组成，因此，分布式数据共享对于实现网络全局目标是必要的。然而，由分布式数据共享导致的合法实体的隐私和机密信息可能被泄露给恶意实体这一风险引起了广泛的关注。隐私性已经成为信息物理系统广泛部署前优先需要解决的问题之一。例如，由于目前没有可被接受的解决方案来解决隐私问题，荷兰的强制部署智能电表陷入停滞状态，因为人们普遍认为智能电表是必然的隐私侵犯对象[24]，从而导致荷兰的强制智能电表部署陷入了停滞状态。2010年，加利福尼亚州对智能电表隐私性的新法案第一次表明了保护终端用户的能耗数据隐私的强烈要求[25]。此外，美国联邦贸易委员会提供了数据收集和处理的建议，以保护城市交通中驾驶员的隐私[26]。2015年1月，美国联邦贸易委员会发布了一份期待已久的报告，呼吁开发网络连接设备（如健身显示器和车联网）的公司采取积极措施保护消费者的隐私。2015年3月，两名美国议员提出两院制法案以建立机制来保护个人隐私免受无人机的广泛使用所造成的危害[27]。对于信息物理系统的隐私性问题，以下三个方面至关重要：攻击模型、隐私概念以及隐私增强技术。

3.1 攻击模型

攻击者的行为通常由三个方面来描述：损坏策略，允许敌对行为以及计算能力。

损坏策略。损坏策略主要有两种，即静态损坏模型和自适应损坏模型。在静态损坏模型[65]中，攻击者在整个协议执行过程中损坏一组固定的参与者。在自适应损坏模型[66]中，攻击者可以在协议执行过程中，根据他们对执行过程的观察自适应地损坏参与者。

允许敌对行为。主要有两种敌对行为：半诚实（又称为诚实但好奇，或者称为被动）敌对行为和恶意敌对行为。在半诚实敌对行为[67]中，攻击者正确遵守协议的规定，但是试图从协议执行过程所传送的数据中获得和/或利用有用的隐私信息。在恶意敌对模型[68]中，攻击者可以根据攻击者的指令任意偏离协议规定。

计算能力。人们主要考虑两类计算能力：多项式时间和无限计算能力。对于多项式计算模型[69]，攻击者允许在概率多项式时间内进行运算。概率多项式时间是可行计算的标准概念，任何不能在多项式时间内进行的攻击都被认为不会对现实生活构成威胁。在无限计算能力模型[70]中，攻击者的计算能力没有任何限制。

3.2 隐私概念

差分隐私、信息论安全和语义安全，这三个重要概念被广泛用于界定信息物理系统中的隐私性。

差分隐私[47-48]。非正式而言，一个协议是差分隐私的如果对于任意两个相似的数据集，该协议作用于两个数据集所表现的行为几乎一致。更具体地来说，差分隐私协议以一种巧妙的方式故意对隐私数据施加噪声，一方面使攻击者无法推测数据制造者的原始数据，另一方面使所加噪声对计算准确性的影响最小化。

信息论安全[51]。非正式而言，一个协议是信息论安全的如果对于任何攻击者，其在整个协议执行过程中所接收到的数据可以仅通过其输入输出加以模拟，并且该攻击者无法区分模拟数据和接收数据，即使他有无限的计算能力。

语义安全[52]。非正式而言，一个协议是语义安全的如果对于任何攻击者，其在整个协议执行过程中所接收到的数据可以仅通过其输入输出加以模拟，并且该攻击者无法通过任何多项式时间算法区分模拟数据和接收数据。语义安全是信息论安全在计算复杂度上的对应概念。

3.3 隐私增强技术

人们已经提出了多种保护信息物理系统数据隐私的技术，包括匿名化、可信计算、加密运算、扰动、可验证计算以及数据混淆。

匿名化[28-32]。匿名化的想法是，数据消费者虽然可能执行计算，但数据与数据源之间的联系已被删除。因此，数据消费者可以接收它所需要用来执行计算的数据，但无法知道数据制造者的身份。

可信计算[34-35]。在可信计算中，数据制造者本身是可信任的，或者存在一个附加的可信任第三方。数据消费者只能接收到计算的聚合结果，但不能接收到个体的数据。一方面，可信任第三方的存在是一个相当强的假设；另一方面，可信任第三方的存在使得协议几乎能够实现理想情形下完全的灵活性。

加密运算[36-39]。加密运算依赖于加密或秘密共享方案的同态运算性质。数据以密文或秘密共享项的形式到达数据消费者，协议确保数据消费者只能解密计算聚合密文或秘密共享项，但无法解密个体数据。

扰动[30-40]。扰动技术故意向数据施加噪声，该噪声的施加一方面可以保持数据消费者所需的计算效用，另一方面可以充分保护数据隐私。采用这一策略的协议通常希望能够提供差分隐私。

可验证计算[29,41-42]。在可验证计算中，计算者伴随计算结果提供一份计算已经按照所声明的方式执行的证明。因此，不受信任的计算者可以执行计算，同时保证计算结果的完整性。这样的证明可以通过将数据消费者作为验证者的零知识证明系统来提供。

数据混淆[43-46,56]。混淆技术通常用于云计算问题，其中云端是不可信的。设想一个客户端持有一个线性规划问题。该客户端使用可逆矩阵混淆成分函数的系数，并将混淆后的问题提交至云端。云端求解混淆后的问题并将解决方案发送给该客户端，后者即可通过混淆矩阵将混淆问题的解变换为原问题的真实解。

近年来，上述隐私增强技术在控制界得到了扩展应用。其中一个分支的研究使用扰动技术来保护信息物理系统的数据隐私。文献[60]通过对线性时不变系统的输入和输出施加确定性扰动来保护动态系统状态和输入的隐私。一系列工作采用差分隐私作为隐私定义，例如，文献[53-55]分别为分布式优化、一致性以及滤波问题开发了差分隐私协议。另一分支的研究采用信息论安全作为隐私定义，例如，文献[57]使用Shamir秘密共享方案，文献[59]实现了树拓扑结构下分布式优化问题的数据隐私，文献[58]为势博弈中的安全多项式计算问题开发了基于同态加密的数据隐私保护方案。

4 总结

安全性和隐私性是信息物理系统中至关重要又富有挑战的课题，它们的研究尚处于起步阶段。本文的主要目的在于介绍信息物理系统中安全性和隐私性的基本概念和问题，而非提供全面的文献综述。这一领域仍然有许多问题尚待解决。例如，在信息物理系统的安全性方面，如何协调信息空间与物理世界的防御以实现更好的安全性仍不明确。在信息物理系统的隐私性方面，如何激励自私的参与者出售其个人信息仍是一个开放性课题。

致谢：本文研究得到了U.S. Army Research Office（W911NF-13-1-0421, multidisciplinary university research initiative），U.S. National Security Agency（H98230-15-1-0289）和U.S. National Science Foundation（CNS-1505664）的资助。

参 考 文 献

[1] U.S. NSF Cyber-physical Systems (CPS) program. http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503286.

[2] P. Evans and M. Annunziata. Pushing the Boundaries of Minds and Machines. General Electric, 2012(11).

[3] N. Falliere, L. O. Murchu and E. Chien. W32.stuxnet Dossier. Symantec Corporation, 2011.

[4] Industrial Control Systems Cyber Emergency Response Team[R]. ICS-CERT Year in Review 2013. The U. S. Department of Homeland Security, 2013.

[5] P. Garcia-Teodoro, Diaz-Verdejo, G. Macia-Fernandez and E. Vazquez. Anomaly-based network intrusion detection: Techniques, systems and challenges[J]. Computers and Security, 2009,28(1):18-28.

[6] A. Patcha and J. Park. An overview of anomaly detection techniques: Existing solutions and latest technological trends[J]. Computer Networks, 2007,51(12):3448-3470.

[7] S. Rajasegarar, C. Leckie and M. Palaniswami. Anomaly detection in wireless sensor networks[J]. IEEE Wireless Communications, 2008,15(4):34-40.

[8] L. Besson and P. Leleu. A distributed intrusion detection system for ad-hoc wireless sensor networks: The AWISSENET Distributed Intrusion Detection System[R]. International Conference on Systems, Signals and Image Processing, 2009,6:18-20.

[9] M. S. Islam, R. H. Khan and D. M. Bappy. A hierarchical intrusion detection system in wireless sensor networks[J]. International Journal of Computer Science and Network Security, 2010,10(8):21-26.

[10] S. Amin, X. Litrico, S. Sastry and A. Bayen. Stealthy deception attacks on water SCADA systems[R]. 13th ACM international conference on Hybrid systems: Computation and control, 2010:161-170.

[11] H. Fawzi, P. Tabuada and S. Diggavi. Secure estimation and control for cyber-physical systems under adversarial attacks[J]. IEEE Transactions on Automatic Control, 2014,59(6):1454-1456.

[12] M. Pajic, J. Weimer, N. Bezzo, P. Tabuada, O. Sokolsky, I. Lee and G. Pappas. Robustness of attack-resilient state estimators[R]. ACM/IEEE International Conference on Cyber-Physical Systems, 2014,4:163-174.

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

[14] A. Teixeira, S. Amin, H. Sandberg, K. Johansson and S. Sastry. Cyber security analysis of state estimators in electric power systems[R]. 49th IEEE Conference on Decision and Control, 2010:5991-5998.

[15] S. Yong, M. Zhu and E. Frazzoli. Resilient state estimation against switching attacks on stochastic cyber-physical systems[R]. IEEE Conference on Decision and Control, 2015:5162-5169.

[16] S. Amin, A. Cardenas and S. S. Sastry. Safe and secure networked control systems under denial-of-service attacks[R]. International Conference on Hybrid Systems: Computation and Control, 2009:31-45.

[17] A. Gupta, C. Langbort and T. Basar. Optimal control in the presence of an intelligent jammer with limited actions[R]. IEEE Conference on Decision and Control, 2010,9:1096-1101.

[18] Q. Zhu, C. Rieger and T. Basar. A hierarchical security architecture for cyber-physical systems[R]. International Symposium on Resilient Control Systems, 2011.:15-20.

[19] H. Shisheh Foroush and S. Martinez. On multi-input controllable linear systems under unknown peridodic DoS jamming attacks[R]. 2013 Proceedings of the SIAM Conference on Control and its Applications, 2013.

[20] M. Zhu and S. Martinez. On distributed constrained formation control in operator-vehicle adversarial networks[J]. Automatica, 2013,49(12):3571-3582.

[21] M. Zhu and S. Martinez. On attack-resilient distributed formation control in operator-vehicle networks[J]. SIAM Journal on Control and Optimization, 2014,52(5):3176-3202.

[22] S. Amin, G. A. Schwartz and S. S. Sastry. Security of interdependent and identical networked control systems[J]. Automatica, 2013,49(1):186-192.

[23] M. Zhu and S. Martinez. On the performance analysis of resilient networked control systems under replay attacks[J]. IEEE

Transactions on Automatic Control, 2014:59(3):804-808.

[24] A. Cavoukian. Smart Meters in Europe: Privacy by Design at its Best. Information and Privacy Commissioner, Ontario, Canada, 2012.

[25] CA Senate Bill 1476. California Public Utilities Commission, 2010.

[26] C. Cottrill and P. Thakuriah. Privacy in context: An evaluation of policy-based approaches to location privacy protection[J]. International Journal of Law and Information Technology, 2014,22(2):178-207.

[27] http://www.markey.senate.gov/news/press-releases.

[28] C. Efthymiou and G. Kalogridis. Smart grid privacy via anonymization of smart metering data[R]. 2010 First IEEE International Conference on Smart Grid Communications, 2010:238-243.

[29] A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet and D. Irwin. Private memoirs of a smart meter[R]. Proceedings of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building, New York, NY, USA, 2010.

[30] J.-M. Bohli, C. Sorge and O. Ugus. A privacy model for smart metering[R]. IEEE International Conference on Communications Workshops, 2010:1-5.

[31] T. Jeske. Privacy-preserving smart metering without a trusted-third-party[R]. In J. Lopez and P. Samarati, editors, SECRYPT, 2011:114-123.

[32] R. Petrlic. A privacy-preserving concept for smart grids.[R] In Proceedings of Sicherheit in vernetzten Systemen, 2010:B1-B14.

[33] M. Jawurek, M. Johns and K. Rieck. Smart metering depseudonymization[R]. In Annual Computer Security Applications Conference, 2011:227-236.

[34] S. Ruj, A. Nayak and I. Stojmenovic. A security architecture for data aggregation and access control in smart grids[J]. Arxiv preprint arXiv:1111.2011:2619.

[35] M. Lemay, G. Gross, C. A. Gunter and S. Garg. Unified architecture for large-scale attested metering[R]. In Hawaii International Conference on System Sciences, 2007:115.

[36] F. Li, B. Luo and P. Liu. Secure information aggregation for smart grids using homomorphic encryption[R]. 2010 First IEEE International Conference on Smart Grid Communications, 2010:327-332.

[37] K. Kursawe, G. Danezis and M. Kohlweiss. Privacy-friendly aggregation for the smart-grid[R]. International Symposium on Privacy Enhancing Technologies, 2011:175-191.

[38] F. Garcia and B. Jacobs. Privacy-friendly energy-metering via homomorphic encryption[R]. Proceedings of the 6th International Workshop on Security and Trust Management, 2010:226-238.

[39] E. Shi, T.-H. H. Chan, E. G. Rieffel, R. Chow and D. Song. Privacy-preserving aggregation of time-series data[R]. Network and Distributed System Symposium, 2011.

[40] V. Rastogi and S. Nath. Differentially private aggregation of distributed time-series with transformation and encryption[R]. Proceedings of the 2010 International Conference on Management of Data, 2010:735-746.

[41] A. Rial and G. Danezis. Privacy-preserving smart metering[R]. Proceedings of the 10th annual ACM workshop on Privacy in the electronic society, 2011:49-60, .

[42] A. Molina-Markham, G. Danezis, K. Fu, P. Shenoy and D. Irwin. Designing privacy-preserving smart meters with low-cost microcontrollers[R]. Proceedings of the 16th International Conference on Financial Cryptography and Data Security, 2012,2.

[43] D. Varodayan and A. Khisti. Smart meter privacy using a rechargeable battery: Minimizing the rate of information leakage[J]. Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing,2011,5:1932-1935.

[44] J. Dreier and F. Kerschbaum. Practical privacy-preserving multiparty linear programming based on problem transformation[R]. 2011 IEEE Third International Conference on Privacy, Security, Risk and Trust, 2011:916-924.

[45] A. R. Borden, D. K. Molzahn, B. C. Leiseutre and P. Ramanathan. Power system structure and confidentiality preserving transformation of optimal power flow problem[R]. Fifty-first Annual Allerton Conference, 2013:1021-1028.

[46] A. R. Borden, D. K. Molzahn, P. Ramanathan and B. C. Lesieutre.

Confidentiality-preserving optimal power flow for cloud computing[R]. Fiftieth Annual Allerton Conference, 2012:1300-1307 .

[47] C. Dwork. Differential privacy[R]. In 3rd Intertional Colloquium on Automata, Languages and Programming,2006:1-12.

[48] C. Dwork and A. Roth. The algorithm foundations of differential privacy[J]. Foundations and Trends in Theoretical Computer Science, 2014,9(2-4):211-407.

[49] C. Dwork. Differential Privacy: A Survey of Results[J]. Theory and Applications of Models of Computation, 2008:1-19.

[50] Q. Geng and P. Viswanath. The optimal mechanism in differential privacy[R]. In 2014 IEEE International Symposium on Information Theory, 2014:2371-2375.

[51] C. E. Shannon. Communication theory of secrecy systems[J]. Bell System Technical Journal, 1949,28(4):656715.

[52] S. Goldwasser and S. Micali. Probabilistic encryption[J]. Journal of Computer and System Sciences, 1984,28(2):270-299.

[53] M. T. Hale and M. Egerstedt. Differentially private cloud-based multi-agent optimization with constraints[R]. In American Control Conference, 2015:1235-1240.

[54] Z. Huang, S. Mitra and G. Dullerud. Differentially private iterative synchronous consensus[R]. In Proceedings of the 2012 ACM workshop on Privacy in the electronic society, 2012:81-90.

[55] J. Le Ny and G. J. Pappas. Differentially private filtering[J]. IEEE Transactions on Automatic Control, 2014,59(2):341—354.

[56] C. Wang, K. Ren and J. Wang. Secure and practical outsourcing of linear programming cloud computing[R]. In 31st IEEE International Conference on Computer Communications,2011:820—828.

[57] Y. Lu and M. Zhu. Game-theoretic distributed control with information-theoretic security guarantees[C]. 5th IFAC Workshop on Distributed Estimation and Control in Networked Systems, 2015,48(22):264-269.

[58] Y. Lu and M. Zhu. Secure cloud computing algorithms for discrete constrained potential games[C]. 5th IFAC Workshop on Distributed Estimation and Control in Networked Systems,2015,48(22):180-185.

[59] A. Shamir. How to share a secret[J]. Communications of the ACM, 1979,22(11):612—613.

[60] Y. Lu and M. Zhu. On confidentiality preserving monitoring of linear dynamic networks against inference attacks[R]. 2015 American Control Conference, 2015,7:359-364.

[61] G. Carl, G. Kesidis, R. R. Brooks and S. Rai. Denial-of-service attack-detection techniques[J]. IEEE Internet Computing, 2006,10(1):82-89.

[62] Y. Mo and B. Sinopoli. Secure control against replay attacks[R]. Allerton Conference on Communication, Control, and Computing, 2009:911-918.

[63] J. Liu, Y. Xiao, S. Li and W. Liang. Cyber security and privacy issues in smart grids[J]. IEEE Communications Surveys & Tutorials, 2012,14(4):981-997.

[64] Y. Mo, H. H. Kim, K. Brancik and D. Dickinson. Cyber-physical security of a smart grid infrastructure[J]. Proceedings of the IEEE, 2012,100(1):195-209.

[65] Y. Lindell and B. Pinkas. Secure multiparty computation for privacy-preserving data mining[J]. Journal of Privacy and Confidentiality, 2009,1(1):59-98.

[66] L. Mazare and B. Warinschi. Separating trace mapping and reactive simulatability soundness: the case of adaptive corruption[J]. Foundations and Applications of Security Analysis, 2009:193-210, .

[67] Q. Chai and G. Gong. Verifiable symmetric searchable encryption for semi-honest-but-curious cloud servers[R]. 2012 IEEE International Conference on Communications,2012(6):917-922.

[68] Y. Lindell and B. Pinkas. An efficient protocol for secure two-party computation in the presence of malicious adversaries[J]. International Conference on Advances in Cryptology, 2008,28(2):52-78.

[69] B. Barak and Y. Lindell. Strict polynomial-time in simulation and extraction[J]. SIAM Journal on Computing, 2002,33(4):783-818.

[70] A. Russell and H. Wang. How to fool an unbounded adversary with a short key[J]. IEEE Transactions on Information Theory, 2002,2332(3):133-148.

[71] Symantec Corp. Internet security threat report, 2015,20(4):15.

信息物理系统中的传感器信息完整性攻击

莫一林，韩　铎，谢立华

新加坡南洋理工大学 电机与电子工程学院

摘要：信息物理系统是一个将传感、通信、控制与计算和物理环境进行有机结合的复杂系统。本文探讨了针对信息物理系统传感器数据的信息完整性攻击，并回顾了近十年来控制领域在此方面的主要研究成果。

关键词：信息物理系统；传感器；信息完整性攻击

1　引言

信息物理系统（Cyber-Physical System）是一个将传感、通信、控制与计算和物理环境进行有机结合的复杂系统。它在航空航天、过程控制、能源、医疗、制造以及交通等众多领域得到了广泛应用。近些年来计算机技术的快速发展将有力地推动信息系统和物理系统之间的进一步融合，并大幅度提高信息物理系统的适用性和功能性。自动驾驶汽车、智能电网和智能家居等新型信息物理系统的出现，让我们周围的物理空间变得更加智能。但与此同时，信息世界与物理世界的紧密结合也对研究者提出了很多新的挑战。

信息物理系统的安全性是衡量其系统性能的最重要的考量之一。对大型信息物理系统，如电网、交通网络等的攻击可能会导致严重的经济损失（如大面积停电、信号灯紊乱等），甚至会危及国民以及国家安全（如铁路系统失控）。很多不同的组织都可以通过攻击信息物理系统获益：一般的个体攻击者可以攻击电网操纵电价，进而获得经济利益；恐怖组织或敌对国家可以利用对信息物理系统的攻击威胁政府。技术的不断进步以及信息世界与物理世界的紧密结合，将为攻击者提供更多的攻击手段，如2010年发现的“震网”病毒（Stuxnet）对伊朗的核提纯设备造成了巨大的破坏[1-2]。由此说明，信息物理系统的安全性已经成为一个非常紧迫的课题。本文主要探讨针对信息物理系统传感器数据的信息完整性攻击（Integrity Attack），并回顾了近十年的主要研究成果。

2　问题描述

假设信息物理系统的状态演化遵守以下的线性时不变系统模型：

$$x(k+1)=Ax(k)+w(k). \qquad (1)$$

其中 $x(k)\in\mathbb{R}^n$ 为n维状态变量，$w(k)\in\mathbb{R}^n$ 为过程噪声（Process Noise），$A\in\mathbb{R}^{n\times n}$ 为系统矩阵。为了获得系统的状态，假设系统中有m个传感器，每个传感器的观测服从以下的线性模型：

$$y_i(k)=C_i x(k)+v_i(k). \quad (2)$$

其中 $y_i(k)\in\mathbb{R}^{p_i}$ 为第i个传感器的真实观测值，$C_i\in\mathbb{R}^{p_i\times n}$ 为第i个传感器的观测矩阵，$v_i(k)\in\mathbb{R}^{p_i}$ 为测量噪声（Measurement Noise）。如无特殊说明，假设每个传感器的测量为标量，即 $p_i=1$。定义 $\mathcal{S}\triangleq\{1,\ldots,m\}$ 为所有传感器的集合。

等式描述了传感器在正常运行时遵循的模型。本文主要考虑针对传感器的信息完整性攻击，即攻击者通过篡改传感器的数据，实现对系统的破坏。在此攻击下，新的传感器模型变为：

$$z_i(k)=y_i(k)+a_i(k). \quad (3)$$

其中 $z_i(k)\in\mathbb{R}^{p_i}$ 为被篡改后的第i个传感器的数据，$a_i(k)$ 为攻击者在第i个传感器上引入的偏差。在本文中我们假设 $a_i(k)$ 遵循以下的模型：

（1）对于未受到攻击的传感器，其 $a_i(k)$=0。对于受到攻击的传感器，$a_i(k)$ 可以取任意值。

（2）受到攻击的传感器的集合不随着时间的推移而改变。

（3）整个系统中最多只有l个传感器受到攻击，被攻击的传感器的集合记为 $\mathcal{A}$，其补集记为 $\overline{\mathcal{A}}$，表示信息物理系统自身并不知道受到攻击的传感器的集合。

与一般的测量噪声 $v_i(k)$ 相比，偏差 $a_i(k)$ 具有以下的特点：

（1）任意性。一般假设线性系统的测量噪声具有某种统计特性（如假设 $v_i(k)$ 为独立同分布的高斯噪声），或者假设测量噪声只能在某个有界集合中取值。与之相反，我们对 $a_i(k)$ 没有任何约束。攻击者可以根据自己的目标以及信息物理系统的模型，设计最佳的攻击 $a_i(k)$。

（2）稀疏性。一般而言，信息物理系统中的所有传感器都会受到测量噪声的影响。然而我们假设只有l 个传感器会遭到攻击。

假设 $\mathcal{I}=\{i_1,\ldots,i_j\}\subset\mathcal{S}$ 为一指标集，定义以下变量：

$$y_{\mathcal{I}}(k)\triangleq\begin{bmatrix}y_{i_1}(k)\\ \vdots\\ y_{i_j}(k)\end{bmatrix},z_{\mathcal{I}}(k)\triangleq\begin{bmatrix}z_{i_1}(k)\\ \vdots\\ z_{i_j}(k)\end{bmatrix},C_{\mathcal{I}}\triangleq\begin{bmatrix}C_{i_1}\\ \vdots\\ C_{i_j}\end{bmatrix},$$
$$a_{\mathcal{I}}(k)\triangleq\begin{bmatrix}a_{i_1}(k)\\ \vdots\\ a_{i_j}(k)\end{bmatrix},v_{\mathcal{I}}(k)\triangleq\begin{bmatrix}v_{i_1}(k)\\ \vdots\\ v_{i_j}(k)\end{bmatrix} \quad (4)$$

为了简化符号，定义 $y(k)\triangleq y_{\mathcal{S}}(k),z(k)\triangleq z_{\mathcal{S}}(k),C\triangleq C_{\mathcal{S}},a(k)\triangleq a_{\mathcal{S}}(k),v(k)\triangleq v_{\mathcal{S}}(k)$。

以上介绍的信息物理系统的模型为动态模型。实际中常用的系统模型也包括静态系统模型（如在电力系统状态估计中所使用的模型[3]）。由于静态模型不考虑系统的演化，我们可以将系统的状态记为 $x\in\mathbb{R}^n$。每个传感器只收集一次数据。假设真实的第 i 个传感器读数为 y_i，被修改后的读数为 z_i，则第 i 个传感器的模型可以写为：

$$z_i=y_i+a_i=C_i x+v_i+a_i \quad (5)$$

类似于动态系统，我们可以相应地定义 $y_{\mathcal{I}},z_{\mathcal{I}},C_{\mathcal{I}},a_{\mathcal{I}},v_{\mathcal{I}}$。

基于状态演化模型，传感器模型以及攻击模型，我们主要关心以下问题：

（1）攻击检测与辨识：判断系统是否受到攻击（攻击检测），即判断是否存在 $a_i(k)\neq 0$，以及界定遭到攻击的传感器的集合（攻击辨识）。

（2）安全状态估计：如何通过 $z_i(k)$ 来估计系统的状态 $x_i(k)$。

2 攻击检测与辨识

本章主要考虑如何检测和辨识传感器信息完整性攻击。首先我们从攻击者的角度，考虑攻击的可检测性以及可辨识性。大致上，如果一个受到攻击的系统的输出和一个正常系统的输出“相同”，则意味着攻击是不可被检测的，因为任何检测手段都无法通过系统的输出来区分系统是否受到攻击。同理，如果两个针对不同传感器集合

$\mathcal{A}$ 和 $\mathcal{A}'$ 的攻击，所产生的输出“相同”，则意味着被攻击的传感器的集合是不可被辨识的，因为无法区分其究竟是 $\mathcal{A}$ 还是 $\mathcal{A}'$。

对于静态系统，我们有如下的定义：

定义1：一个针对静态系统的攻击 $a \neq 0$ 是不可检测的（undetectable）或隐蔽的（stealthy）[4]，当且仅当存在 Δx，如下等式成立：

$$a = C\Delta x. \tag{6}$$

假设攻击 a 是不可检测的，则：

$$Cx + v + a = C(x + \Delta x) + v. \tag{7}$$

换而言之，任何攻击检测器均无法区分以下的两种情况：

（1）系统正常运行，其状态为 $x + \Delta x$。

（2）系统受到攻击，其状态为 x，且攻击者的输入为 a。

站在攻击者的角度，假设恶意传感器的集合为 $\mathcal{A}$，则当且仅当 $C_{\overline{\mathcal{A}}}$ 不满足列满秩条件时，攻击者可以发起隐蔽攻击[5]。我们定义一个指标集 $\mathcal{I}$ 为不可检测的集合，如果 $C_{\overline{\mathcal{A}}}$ 列不满秩。可以看出，不可检测的集合 $\mathcal{I}$ 的大小决定了系统的安全程度。如果不可检测的集合 $\mathcal{I}$ 的基数很大，则攻击者需要攻击大量传感器才可以实现隐蔽攻击。反之，如果 $\mathcal{I}$ 基数很小，则攻击者只需要攻击少量传感器，即可保证攻击的隐蔽性。基于这种考量，在文献[6]中，作者提出了安全指标（security index）的概念。传感器 i 的安全指标被定义为包含 i 的最小的不可检测集合的基数。假设一个传感器的安全指标较小，则意味着这个传感器对系统而言非常重要，需要加强其安全性（如使用更强的加密算法）。

对于动态系统，可以看出系统的输出 $z(k)$ 是由初始值 $x(0)$，噪声 w，v，以及攻击 a 决定的。因此，我们可以将 $z(k)$ 记作 $z(x(0), w, v, a, k)$。

定义2：一个针对动态系统的攻击 $a \neq 0$ 是不可检测的（undetectable）或隐蔽的（stealthy），当且仅当存在 $x(0)$ 以及 $x'(0)$，如下等式对所有 k 成立：

$$z(x(0), w, v, a, k) = z(x'(0), w, v, 0, k). \tag{8}$$

一个针对动态系统的攻击 $a \neq 0$ 是不可辨识的（unidentifiable），当且仅当存在 $x(0)$，$x'(0)$，以及攻击 $a' \neq a$，如下等式对所有 k 成立：

$$z(x(0), w, v, a, k) = z(x'(0), w, v, a', k). \tag{9}$$

由于我们所考虑的信息物理系统为线性系统，以上的条件可以简化为：

定理1 一个针对动态系统的攻击 $a \neq 0$ 是不可检测的，当且仅当存在 $x(0)$，如下等式对所有 k 成立：

$$z(x(0), 0, 0, a, k) = 0. \tag{10}$$

一个针对动态系统的攻击 $a \neq 0$ 是不可辨识的，当且仅当存在攻击 $a' \neq a$，且 $a - a'$ 不可检测。

假定受到攻击的传感器的集合为 $\mathcal{A}$，在文献[7-8]中，作者证明了当且仅当 $(A, C_{\overline{\mathcal{A}}})$ 不可观时，攻击者可以发起隐蔽攻击。同时，作者提出可以设计如下的估计器以及基于残差的检测器，来检测非隐蔽攻击：

$$\hat{x}(k+1) = Ax(k) + Kr(k+1) \tag{11}$$

$$r(k+1) = z(k+1) - CA\hat{x}(k) \tag{12}$$

其中 K 为增益矩阵，且 $A - KCA$ 稳定。对于无噪声系统，作者证明了如果攻击不存在，则 $r(k) \to 0$ 收敛为0。因此，可以通过 $r(k)$ 的大小判断系统是否受到攻击。

当系统中存在噪声时，检测器中的 $r(k)$ 并不收敛为0，而是收敛为一稳定的高斯过程（stationary Gaussian process）。因此，由于噪声的存在，检测器很难检测一个非常小的攻击 a。另一方面，一个隐蔽攻击对系统造成的伤害也可能是有限的（如攻击 $a(k)$ 可能渐进收敛为0）。针对以上的两个考量，在文献[9-11]中，作者提出了以下概念：

定义3：一个针对动态系统、估计器以及检测

器的攻击 $a \neq 0$ 是可行的（feasible），如果以下条件成立：

对于所有的 k，$\| P_r^{-1/2} r(k) \| \leq 1$，其中 P_r 为 $r(k)$ 的协方差矩阵。

一个攻击是完美攻击（perfect attack），如果它是可行的，且以下条件成立：

$\| \hat{x}(k) - x(k) \| \to \infty$ 即估计误差趋向于无穷大。

假定被攻击的传感器的集合为 $\mathcal{A}$，在文献[10]中，作者证明了完美攻击存在，当且仅当存在 x，如下条件成立：

（1）x为A矩阵的一个不稳定的特征向量。

（2）$C_{\bar{\mathcal{A}}} x = 0$。

（3）x 属于系统 $x(k+1) = (A - KCA)x(k) - K\Gamma u(k)$ 的可达空间。其中 Γ 为一对角矩阵。其对角元素满足：

$$\Gamma_{ii} = \begin{cases} 0 & i \notin \mathcal{A} \\ 1 & i \in \mathcal{A} \end{cases}. \qquad (13)$$

对于一般的可行攻击，在文献[9,11]中，作者提出利用椭圆微积分（ellipsoidal calculus）来计算攻击所能造成的估计误差。

以上的研究主要集中于隐蔽（或可行）的攻击。在文献[8]中，作者考虑了如何辨识受到攻击的传感器的集合。作者证明了辨识问题是一个NP难问题。一般而言，需要为每一个可能的恶意传感器的集合建立一个残差生成器（见文献[12]），或者通过求解一个l_0优化问题来实现攻击辨识。在文献[13]中，作者证明了对于没有噪声的系统，当系统的A，C矩阵满足特定条件时，可以将l_0优化问题转化为l_1凸优化问题来同时实现攻击辨识以及状态估计。

3 安全状态估计

本章主要考虑在存在恶意的传感器数据的情况下的状态问题。

我们首先考虑静态系统的状态估计问题。在某些特定条件下，我们可以找到“最优”估计器。在文献[14-15]中，作者考虑了当状态 x 为标量时的状态估计问题。文中，作者考虑了比线性模型更一般的模型，即假设系统状态 x 以及真实的测量值 y 满足某一已知的概率分布。作者证明了如果大于等于一半的传感器是恶意的，则最优的状态估计为x的期望，而与收到的观测 z 无关。另一方面，针对小于一半的传感器是恶意的情况，作者提出了局部估计器（Local Estimator）的概念：

假设 $\mathcal{I}$ 为一指标集。一个静态估计器 $\hat{x} = \varphi_{\mathcal{I}}(z)$ 被称为是局部估计器，如果估计结果 $\hat{x}$ 与指标集 $\mathcal{I}$ 中的传感器的观测结果无关。即对任意 $i \in \mathcal{I}$，改变 z_i 并不影响 $\hat{x}$ 的值。

在定义了局部估计器后，作者证明了最小均方误差估计器具有以下的形式：

$$\hat{x} = g(z) = \min_{|\mathcal{I}|=l} \left[\max_{|\mathcal{J}|=l, \mathcal{J} \cap \mathcal{I} = \varnothing} \varphi_{\mathcal{J} \cup \mathcal{I}}(z) \right]. \qquad (14)$$

其中 $\varphi_{\mathcal{J} \cup \mathcal{I}}(z)$ 为局部估计器。

在文献[16]中，作者考虑了当状态 x 为向量时的状态估计问题。作者假设测量噪声 v 是有界的，即满足 $\| G^{-1} v \| \leq \delta$，其中$G$为一可逆矩阵。作者考虑了设计估计器 $\hat{x} = g(z)$ 来最小化最差情况下的估计误差。作者证明了如果存在一个基数为$2l$ 的指标集 $\mathcal{K}$，使得 $C_{\bar{\mathcal{K}}}$ 不满足列满秩的性质，则最差情况下的观测误差为无穷大。另一方面，如果这样的指标集不存在，则最优估计问题可以转化为求一个集合的切比雪夫中心的问题，并且可以利用线性矩阵不等式求解。

以上最优的估计器都存在计算复杂度高的问题，因此难以应用于大规模的系统。在文献[17]中，作者提出了一类基于凸优化的状态估计器：

$$\hat{x} = g(z) = \arg\min_{\hat{x}} \sum_{i=1}^{m} f_i(z_i - C_i x). \qquad (15)$$

其中 f_i 对称、非负的凸函数。这类估计器的优点在于计算复杂度较低，可以用于求解大规模的问题。作者证明了如果以下两个条件成立，则估计器是安全的：

（1）对所有 x 以及 f_i，以下极限有界：

$$\lim_{t\to\infty}\frac{f_i(tC_ix)}{t}=H_i(x)<\infty \tag{16}$$

（2）对所有 x 以及所有基数为 l 的指标集 $\mathcal{I}$，以下不等式成立：

$$\sum_{i\in\mathcal{I}}H_i(x)<\sum_{i\notin\mathcal{I}}H_i(x) \tag{17}$$

同时，作者证明估计器是安全的的必要条件为：

（1）对所有 x 以及 f_i，以下极限有界：

$$\lim_{t\to\infty}\frac{f_i(tC_ix)}{t}=H_i(x)<\infty \tag{18}$$

（2）对所有 x 以及所有基数为 l 的指标集 $\mathcal{I}$，以下不等式成立：

$$\sum_{i\in\mathcal{I}}H_i(x)\le\sum_{i\notin\mathcal{I}}H_i(x) \tag{19}$$

可以看出，以上的充分和必要条件之间只存在一个小的差别，即小于号变成了小于等于号。

下面我们研究动态估计问题。一种常见的方法是采用滚动时域估计（Moving Horizon Estimation）的方法，即截取一段历史数据 $Z(k:k+N\text{-}1)=\begin{bmatrix}z(k) & \cdots & z(k+N-1)\end{bmatrix}$ 来估计当前时刻的状态 $x(k)$，这样可以将动态估计的问题转化为静态估计的问题。在文献[13]中，作者考虑了无噪声（$w=0,v=0$）情况下的动态估计问题。假定以下不等式对所有非零 x 均成立：

$$|\mathrm{supp}(Cx)\cup\mathrm{supp}(CAx)\cup\cdots\cup\mathrm{supp}(CA^{N-1}x)|>2l, \tag{20}$$

其中 $supp(z)$ 代表 z 中非零元素对应的指标集。若成立，则以下的 l_0 优化问题可以准确地求解出系统的初始状态：

$$\hat{x}(0)=\arg\min_{\hat{x}}\left\|Z(0:N-1)-\Phi_N(x(0))\right\|_0, \tag{21}$$

其中，$\|X\|_0$ 代表矩阵 X 中非零行的个数，$\Phi_N(x)$ 定义如下：

$$\Phi_N(x)=\begin{bmatrix}Cx & CAx & \cdots & CA^{N-1}x\end{bmatrix}. \tag{22}$$

由于系统没有噪声，可以通过初始状态准确地计算任意时刻的系统状态。l_0 优化本质上是一个组合优化的问题，因此计算复杂度较高，不易应用于大规模的系统。在文献[13]中，作者还提出利用压缩感知的方法，来求解以下凸优化问题，以降低计算复杂度：

$$\hat{x}(0)=\arg\min_{\hat{x}}\left\|Z(0:N-1)-\Phi_N(x(0))\right\|_{l1/lr}, \tag{23}$$

其中一个矩阵的 l_1/l_r 范数被定义为矩阵每个行向量的 l_r 范数的和。

定义 $(\Phi_N(x))_i$ 为 $\Phi_N(x)$ 的第 i 行向量。作者证明了如果对任意非零 x 以及基数为 l 的指标集 $\mathcal{I}$，以下不等式成立：

$$\sum_{i\in\mathcal{I}}\left\|(\Phi_N(x))_i\right\|_r<\sum_{i\notin\mathcal{I}}\left\|(\Phi_N(x))_i\right\|_r, \tag{24}$$

则优化问题和的解相同，即我们可以通过凸优化来准确求解系统的初始状态：

备注：可以发现不等式与非常相似。事实上，我们可以将优化问题看成是的一个特例，之后利用的安全性的充分条件导出不等式。

在文献[18]中，作者将以上的方法推广到了存在有界噪声的系统。作者提出可以通过求解以下的优化问题，来生成一个对 $\hat{x}(k)$ 的估计：

$$\hat{x}(k)=\arg\min_{\hat{x}}\left\|Z(k:k+N-1)-\Phi_N(x(k))+\Omega\right\|_0$$
$$s.t.\quad|\Omega|\prec\Delta. \tag{25}$$

其中 $|\Omega|\prec\Delta$ 代表 Ω 中的每一个元素的绝对值小于对应的 Δ 中的元素。矩阵 Δ 的大小取决于系统噪声的特性。作者证明了如果不等式成立，则生成的状态估计与实际状态之间的误差是有界的。

以上的动态估计器均利用了滚动时域的方法，将动态估计问题转化为静态问题求解。图1显示了滚动时域类的动态估计器的信息流。可以看出，这类方法的缺陷是只能利用有限时间内的数据，而不能使用所有的历史数据。

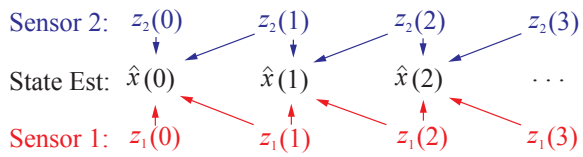


图1　基于滚动时域的动态估计器的信息流示意图

其中我们假设滚动窗口的大小 N=2。

针对以上的问题，在文献[19]中，作者提出了利用局部估计器（Local Estimator）将线性高斯系统（Linear Gaussian System）的动态估计问题转化为静态估计问题。针对每个传感器，作者提出设计以下的局部估计器：

$$\hat{x}_i(k) = Ax_i(k) + L_i[z_i(k+1) - C_i Ax_i(k)], \quad (26)$$

其中 $\hat{x}_i(k)$ 为第 i 个局部估计器的状态估计。可以看出 $\hat{x}_i(k)$ 只与第 i 个传感器的测量值 z_i 有关。

假设稳态的卡尔曼滤波器（Steady-State Kalman Filter）可以写为如下形式：

$$\hat{x}(k) = Ax(k) + K[z(k+1) - CAx(k)], \quad (27)$$

其中 K 为稳态卡尔曼增益（Steady-State Kalman Gain）。作者证明了如果设计局部估计器的增益 L_i 使得所有 $A - L_i C_i A$ 矩阵与 $A - KCA$ 矩阵的特征值重合，则稳态的卡尔曼滤波器可以被分解成如下形式：

$$\hat{x}(k) = \sum_{i=1}^{m} F_i x_i(k). \quad (28)$$

作者又提出利用如下的LASSO优化问题来生成状态估计 $\hat{x}_s(k)$：

$$\begin{aligned} \min \quad & \frac{1}{2}\hat{\mu}(k)^T \tilde{W}^{-1}\hat{\mu}(k) + \gamma\left\|\hat{v}(k)\right\|_1 \\ s.t. \quad & \hat{x}_i(k) = \hat{x}_s(k) + \mu_i(k) + v_i(k), \forall i \end{aligned} \quad (29)$$

作者证明了当系统没有受到攻击时，$\hat{x}_s(k)$ 有很大概率等于最优的卡尔曼估计 $\hat{x}(k)$。另一方面，当少于一半的传感器受到攻击时，$\hat{x}_s(k)$ 的估计误差依然有界。图2显示了基于局部估计器的动态估计器的信息流。可以看出，每个传感器的所有历史观测值都完全地保存在局部估计值中。

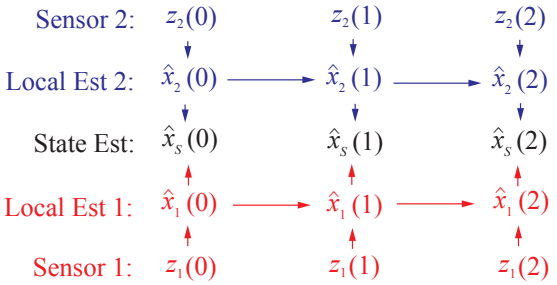


图2　基于局部估计器的动态估计器的信息流示意图

4　结论与展望

本文主要回顾了控制领域针对信息完整性攻击的一些研究成果，主要包括了攻击检测、攻击辨识以及安全状态估计。可以看到，目前的研究主要集中在利用控制系统模型，通过传感器数据之间的关联来检测、辨识攻击以及估计系统的状态。另一方面，针对信息物理系统的信息层面的建模非常粗糙，并且没有很好地利用信息层面的消息（例如，可以通过分析网络层数据包来检测传感器是否受到攻击）。基于控制理论的安全研究未来应与传统的信息安全相结合，从而可以实现对信息物理系统的多方位的保护。

参 考 文 献

[1] D. P. Fidler. Was Stuxnet an Act of War? Decoding a Cyberattack[J]. IEEE Secur. Priv. Mag., 2011. 9(4):56-59.

[2] T. Chen. Stuxnet, the real start of cyber warfare? Editor’s Note[J]. IEEE Netw., 2010,24(6):2-3.

[3] A. Abur, A. Exposito. Power system state estimation: theory and implementation. CRC Press: 2004.

[4] Y. Liu, P. Ning, and M. K. Reiter. False data injection attacks against state estimation in electric power grids[J]. ACM Trans. Inf. Syst. Secur., 2011,14(1):1-33.

[5] Y. Mo, T. H. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli. Cyber – Physical Security of a Smart Grid Infrastructure[J]. Proc. IEEE, 2011,100(1):1-15.

[6] J. M. Hendrickx, K. H. Johansson, R. M. Jungers, H. Sandberg, and

K. C. Sou. Efficient Computations of a Security Index for False Data Attacks in Power Networks[J]. IEEE Trans. Automat. Contr., 2014,59(12):3194-3208.

[7] F. Pasqualetti, A. Bicchi, and F. Bullo. Consensus computation in unreliable networks: A system theoretic approach[J]. IEEE Trans. Automat. Contr., 2012,57, (1):90-104.

[8] F. Pasqualetti, F. Dorfler, and F. Bullo. Attack Detection and Identification in Cyber-Physical Systems[J]. IEEE Trans. Automat. Contr., 2013,58(11):2715-2729.

[9] Y. Mo, E. Garone, A. Casavola, and B. Sinopoli. False data injection attacks against state estimation in wireless sensor networks[R]. in 49th IEEE Conf. Decis. Control, 2010:5967-5972.

[10] Y. Mo and B. Sinopoli. False data injection attacks in control systems[R]. in IEEE Conference on Decision and Control, 2010.

[11] Y. Mo and B. Sinopoli. On the Performance Degradation of Cyber-Physical Systems under Stealthy Integrity Attacks. IEEE Trans. Automat. Contr., p. to be appeared.

[12] M.-A. Massoumnia, G. C. Verghese, and A. S. Willsky. Failure detection and identification[J]. IEEE Trans. Automat. Contr., 1989,34(3):316-321.

[13] Y. Mo and B. Sinopoli. Robust estimation in the presence of integrity attacks[R]. in Proceedings of the IEEE Conference on Decision and Control, 2013:6085-6090.

[14] Y. Mo and B. Sinopoli. Secure Estimation in the Presence of Integrity Attacks[J]. IEEE Trans. Automat. Contr.,2015,60(4):1145-1151.

[15] Y. Mo and R. M. Murray. Multi-dimensional state estimation in adversarial environment[R]. in 2015 34th Chinese Control Conference (CCC), 201:4761-4766.

[16] D. Han, Y. Mo, and L. Xie. Convex Optimization Based State Estimation against Sparse Integrity Attacks[R]. in 2016 35th Chinese Control Conference (CCC), 2016, Available online: http://yilinmo.github.io/public/papers/acc16-1.pdf

[17] H. Fawzi, P. Tabuada, and S. Diggavi. Secure Estimation and Control for Cyber-Physical Systems Under Adversarial Attacks[J]. IEEE Trans. Automat. Contr., 2014,59(6):1454-1467.

[18] M. Pajic, J. Weimer, N. Bezzo, P. Tabuada, O. Sokolsky, I. Lee, and G. J. Pappas. Robustness of attack-resilient state estimators[R]. in 2014 ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS), 2014:163-174.

[19] Y. Mo and E. Garone. Secure Dynamic State Estimation via Local Estimators[R]. in IEEE Conference on Decision and Control, 2016, Available online: http://yilinmo.github.io/public/papers/cdc16-1.pdf.

作者简介

莫一林　现为新加坡南洋理工大学电机与电子工程学院助理教授。他于2007年在清华大学自动化系获得本科学位。2012年在卡内基梅隆大学获得电子与计算机工程博士学位。他曾作为博士后在卡内基梅隆大学（2013）以及加州理工学院（2013-2015）进行研究工作。他的研究兴趣包括安全控制系统的设计以及网络化控制系统，及其在传感器网络与智能电网中的应用。

韩　铎　2015年毕业于香港科技大学，获得电子系博士学位；2011年毕业于香港城市大学，获得工学学士学位（一等荣誉）。2014年作为访问学者在美国加州理工学院从事研究工作；2015年至今于新加坡南洋理工大学从事博士后工作。主要研究方向包括：网络化系统安全，估计理论，传感器网络优化等。

谢立华　新加坡南洋理工大学电子系教授。1992年毕业于The University of Newcastle, Australia, 获得博士学位，1983年和1986年于南京理工大学获本科学位和硕士学位。IEEE Fellow 和 IFAC Fellow，研究方向为鲁棒控制、传感器网络、网络控制系统，估计理论和信号处理。

网络化控制系统安全问题研究现状与挑战

张　恒[1]，何建平[2]，程　鹏[3]，王文海[3]，陈积明[3]

1. 淮海工学院理学院，江苏 连云港，222001

2. 维多利亚大学 电子与计算机工程学院，加拿大维多利亚，V8W 3P6

3. 浙江大学 控制科学与工程学院，浙江 杭州，310027

摘要：计算、通信、控制等信息技术深度融合的工业4.0时代的到来，给网络化控制系统安全问题研究带来了新的机遇和挑战。网络化控制系统安全的研究目的在于建立完整的系统安全防御体系，确保系统安全高效可靠的运行。本文就网络化控制系统安全问题研究最新国内外研究成果、现状及面临的困难与挑战进行概述，并指出和总结了仍未解决但急需解决的研究问题。

关键词：网络化控制；攻击；系统安全

1　概述

信息技术的飞速发展引领人类进入了以数字化、网络化和智能化为特征的工业4.0时代，并孕育出智慧工厂、智能交通、智能电网等各种新型智能化信息系统，显著地提高并改变了人类社会的生活、生产和管理方式。新型信息系统通过信息感知、泛在计算和管理调控，实现物理空间、信息空间的互联互通和深度融合。新型信息系统的本质是网络化控制系统（Networked Control Systems，简称NCS），它是由物理对象、传感器、估计器、控制器、执行器和网络媒介构成。网络化控制是信息化系统实现实时、稳定、优化运行的关键技术支撑[1]。典型的NCS的结构如图1所示。

工业4.0时代对网络化控制的高度信息化和智能化的要求，需要NCS技术具有更高的开放性，这就直接导致了NCS具有更高的潜在安全威胁。近期发生的NCS重大安全事件有：

（1）2010年，“震网”病毒（Stuxnet）利用工业控制系统漏洞入侵伊朗布尔什核电站，导致1/5的离心机报废，核反应堆长时间无法运营。

（2）2011年，美国伊利诺伊州城市供水系统，由于数据采集和监控系统被入侵，大量供水泵被烧毁。

（3）2012年，破坏力巨大的“火焰”病毒（Flame）在中东地区大范围传播，对石油工业等重要控制系统的正常运行造成了很大的冲击。

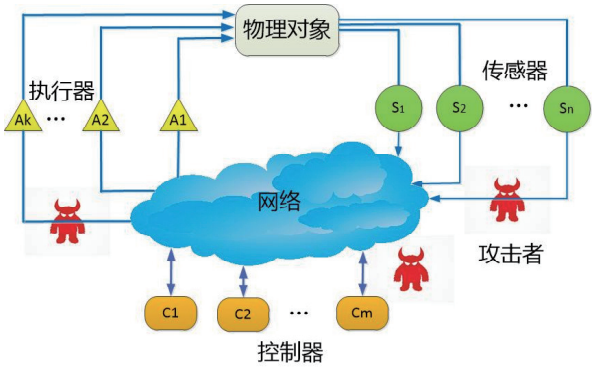


图1　NCS系统结构图

（4）2014年，安全厂商F-Secure发现Havex病毒，该病毒通过入侵SCADA和工控系统中使用的工业控制软件，有能力禁用水电大坝，使核电站过载，甚至可以做到按一下键盘就能关闭一个国家的电网。

（5）2015年底，乌克兰的变电站控制系统持续遭到网络攻击，至少三个区域约140万居民失去了电力供应，大规模停电3-6小时。

根据全球工业控制信息安全权威机构美国工业控制系统网络应急响应小组（the Industrial Control Systems Cyber Emergency Response Team，简称ICS-CERT）报告，工控系统安全事件由2012财年197起到2015财年295起，呈现了快速上升趋势[2]。截至2016年6月，中国国家信息安全漏洞共享平台（China National Vulnerability Database，简称CNVD）也已累计发布840条工控系统安全漏洞。由此可见，已经广泛应用于工业、军事、交通、能源等关系国计民生各个行业和关键基础设施的NCS一旦受到攻击，不仅会造成巨大的经济损失，而且会对民众的生命安全和国家安全造成重大威胁。因此，网络化控制系统安全课题受到了研究者们的广泛关注和深入研究[1,3-21]。

网络空间与物理空间深度融合的特点为NCS安全带来了许多新的研究问题和挑战。例如，如何刻画攻击与系统状态之间的关系、如何对恶意攻击进行有效检测、如何处理针对闭环控制的恶意攻击、如何对抗以物理进程为目标的恶意攻击等。现有的计算机安全技术还没有足够的能力保证NCS安全。因此，这些新的研究问题都对NCS系统安全运行提出了全新的理论挑战和技术需求，并成为现代工业发展与应用亟待解决的重大研究课题。

2　研究热点与成果

NCS安全涉及控制理论、网络通信技术和计算机技术等多个学科交叉的挑战性问题，已成为当前信息领域研究的科学前沿问题，国内外研究者已经开展了大量相关研究，并取得了一定的研究成果。

2.1　典型攻击模型

面向NCS系统的典型攻击包括拒绝服务攻击（Denial-of-Service attack，简称DoS attack）[5-7]，重放攻击（Replay attack）[8]，数据注入攻击（Data injection attack）[9]等。

DoS攻击是通过大量合法或伪造的请求占用大量网络和系统资源，实现系统无法正常工作的目的。具体攻击方式包括物理层的拥塞攻击，链路层的碰撞攻击，网络层的指示错误、黑洞攻击，传输层的泛洪攻击等。根据DoS攻击造成的随机丢包规律，研究人员通常将该攻击描述为独立同分布的随机变量序列[5-7]。

重放攻击是攻击者记录系统元件之间在一个时段内的通信数据，然后选择另一时段重放这些数据[8,9]。骇人听闻的震网病毒就是利用了重放攻击原理，通过播放21秒级联保护系统的传感器正常情况下的数据实现离心机工作异常，从而造成核电系统的毁灭性破坏[9]。基于攻击者记录的系统元件通信数据和攻击起始时间，可以建立攻击时间序列模型[8]。

数据注入攻击是攻击者通过发送错误信息给相应的接收端，破坏通信数据的完整性和准确性[1]。这里的错误信息包括错误的测量值、错误的发送时间、错误的用户ID等。攻击者获得系统元件之间的通信秘钥或者入侵传感器、控制器，可以实现数据注入攻击。在正常工作状态下的系统演化方程基础上，加上由攻击引起的测量数据、控制数据等变化值，即可获得攻击状态下的系统演化方程。值得注意的是这里的攻击引起的变化值有可能是常值、随机值或者有界值。

2.2　攻击特征与系统性能内在联系

刻画攻击与NCS系统控制性能之间的耦合关系

在安全问题研究中起着至关重要的作用。深刻理解二者的耦合关系有助于准确设计入侵检测方法和构建可靠的安全防御机制。

Zhang等人分别建立了能量受限的DoS攻击策略与系统状态估计性能、最优控制性能的函数关系，并且给出了攻击对于估计和控制性能影响的量化评估[5,6]。Amin等人研究了传感器与估计器之间的测量数据传输信道、控制器与执行器之间的控制数据传输信道同时遭受DoS攻击时，通过独立随机序列模型刻画攻击对数据传输的影响，进而得到攻击变量序列与线性二次高斯控制代价函数之间的对应关系[7]。

Mo等人对估计器到控制器传输的测量数据受到重放攻击时，系统状态估计和控制性能的变化进行了分析[11]。Zhu等人考虑了重复播放控制器到执行器传输数据的重放攻击，研究了该攻击对的系统性能的影响，进而设计了滚动控制率降低攻击对系统性能的影响[8]。

Teixeira等人对资源受限的数据注入攻击下的系统控制性能进行了深入研究，通过定义的安全集描述攻击对系统性能的影响，并且在四容水箱控制平台验证攻击参数与控制性能的对应关系[10]。Liu等人则分析了攻击能力约束下的数据注入对电网状态估计的影响[12]。

2.3 攻击入侵检测机制

针对不同的攻击，研究人员设计了攻击检测机制。Zhang等人指出数据接收率（Packet Reception Rate，PRR）是反映系统元件之间的通信是否受到DoS攻击的常规检测指标[5]。Carl等人总结了针对DoS攻击的常规检测方法，这些方法在传感器网络中都是非常典型的[13]。x^2-检验是最常用的检测重放攻击和数据注入攻击的方法[11,14]。Pasqualetti等人针对线性定常连续系统攻击检测问题，分别设计了检测攻击的集中式和分布式滤波器[15]。该滤波器可以实现对重放攻击、数据注入攻击等典型攻击的检测。针对数据注入测量值和控制值的攻击形式，Weerakkody等人基于物理水印技术提出了一种新的入侵检测方法，并通过选择合适的水印自由度参数可以获得最大化的检测率[9]。

2.4 系统防御机制

系统防御机制研究包括安全与系统实时性能权衡、安全状态估计、安全控制等方面。

恶意攻击的存在对NCS实时控制性能造成显著的影响，而使用信息加密等安全防御机制则必然会降低系统实时控制性能[3,4]。也就是说，安全防御机制和实时控制性能是一对矛盾体。Gupta等人基于路径跟踪问题考虑NCS安全对系统性能的影响，通过将系统安全特征映射到额外的系统延时，显示系统安全和实时控制之间的权衡关系[3]。Zeng和Chow在文献[4]中研究了如何权衡信息加密水平与系统实时控制性能。作者利用快速跟踪平均误差刻画系统实时控制水平，基于密钥长度定义信息加密水平，进而构建了性能—安全权衡模型。通过协同进化算法选择最优的安全参数和系统参数，实现了性能—安全协同优化。

状态估计是了解NCS运行状况的一个最基本途径，也是系统反馈控制算法设计的重要依据。例如，在电网系统中需要估计网络拓扑和潮流分布等状态信息，用以掌握电网系统运行状况[12]，而对无人机UAV的反馈控制更是基于对其位置、速度等状态变量的估计[21]。各种攻击行为会对系统状态估计产生明显的影响，研究人员从不同的角度对其展开研究。其中包括面向一般线性系统的弹性状态估计[16]，针对电网的安全状态估计[17]，针对无人操控地面小车的巡航安全的弹性状态估计[18]、弹性自适应状态估计[19]等。

安全控制技术是实现攻击环境下NCS系统可靠运行的关键。针对DoS攻击，Amin等人构建了攻击下的最优线性二次高斯控制模型，并且利用

半正定规划的最优解获得了最优安全控制策略[7]。Gupta等人构建DoS攻击与控制器之间的零和博弈模型，并且获得了博弈场景下的控制平衡点和攻击策略[20]。Zhu等人设计了滚动时域控制算法来抵御重放攻击，并且分析了系统控制性能衰退情况[8]。而在文献[21]中，Zhu等人设计分布式控制算法，使车载网可以在数据注入攻击控制信号条件下依然可以保持队形。

3　开放问题及挑战

控制、通信、计算技术的进一步深度融合，将推动形成组件高度异构、拓扑复杂多变的多维度开放式NCS，这对系统的安全性提出了新的挑战和更高要求，主要包括以下几个方面：

（1）高维异构系统与复杂模态攻击的关联建模问题。目前，针对工业应用场景下的NCS系统高维异构特性，以及不断升级的复杂模态攻击，缺乏合理的数学模型描述系统与攻击之间的相互作用规律。

（2）资源受限的系统优化防御问题。不同于传统的信息系统能量供给充足、计算和存储能力较强，NCS设计中通常需要考虑能量、计算、存储等有限的资源。如何优化配置有限的资源实现系统安全防御目标是极具挑战的研究课题。

（3）系统组件的信任管理问题。系统的组件特别是传感器节点容易受到攻击威胁，造成物理设备失效、被劫持等，严重影响系统可靠运行，而目前针对NCS系统组件构建安全认证和信任管理体系的研究非常缺乏。

（4）复杂模态攻击的高效精准入侵检测问题。日益升级攻击的模态复杂、时空多变等特性，以及系统资源受限，给高效精准入侵检测机制的设计带来巨大挑战。

（5）大规模系统安全性度量问题。在构建安全度量指标时，需要综合考虑NCS的系统高实时性、高可靠性、高稳定性等需求以及系统规模等因素。而在具体应用场景中，离散子系统和连续子系统混合构成完整的大系统，也对系统安全度量指标构建带来困难。

（6）系统安全控制与优化问题。在现有NCS控制机制基础上，结合复杂模态攻击与系统运行的关联建模分析，设计安全可靠的优化控制技术，依然是具有挑战的核心工作。

4　结语

探索和研究网络化控制系统安全是一项关乎国家安全的重要课题，具有重要的现实意义和应用价值。本文概述了目前关于控制系统研究的主要研究热点，分别总结了攻击建模、攻击特征与系统性能内在联系、攻击入侵检测机制、攻击防御机制等方面取得了一些重要研究成果。此外，本文还指出该课题仍然面临并亟待解决的难题。对网络化控制系统安全理论与关键技术体系的深入研究，必将有力地提升系统安全防御能力，保障国家和公共安全。

参 考 文 献

[1] A. A. Cardenas, S. Amin, S. S. Sastry. Secure control: Towards survivable cyber-physical systems[R]. In Proceedings of IEEE ICDCS Workshops, 2008:495-500.

[2] Industrial Control Systems Cyber Emergency Response Team. ICS-CERT year in review, School of Computer Science, Carleton University, 2015.

[3] R. A. Gupta, A. A. Masoud, and M.-Y. Chow. A delay-tolerant potential field-based network implementation of an integrated navigation system[J]. IEEE Transactions on Industrial Electronics, 2010, 57(2):769-783.

[4] W. Zeng, and M.- Y. Chow. Optimal tradeoff between performance and security in networked control systems based on coevolutionary algorithms[J]. IEEE Transactions on Industrial Electronics, 2012, 59(7):3016-3025.

[5] H. Zhang, P. Cheng, L. Shi, and J. Chen. Optimal DoS Attack Policy With Energy Constraint[J]. IEEE Transactions on Automatic Control, 2015,60(11):3203-3208.

[6] H. Zhang, P. Cheng, L. Shi, and J. Chen. Optimal DoS Attack Scheduling in Wireless Networked Control System[J] IEEE Transactions on Control System Technology, 2016, 24(3):843-852.

[7] S. Amin, A. A. Cardenas, S. S. Sastry. Safe and secure networked control systems under denial-of-service attacks[J]. Hybrid Systems: Computation and Control, 2009:31-45.

[8] M. Zhu, S. Martínez. On the performance analysis of resilient networked control systems under replay attacks[J]. IEEE Transactions on Automatic Control, 2014, 59(3):804-808.

[9] S. Weerakkody, Y. Mo, B. Sinopoli. Detecting integrity attacks on control systems using robust physical watermarking[R]. In Proceedings of IEEE Conference on Decision and Control, 2014:3757-3764.

[10] A. Teixeira, I. Shames, H. Sandberg, K.H. Johansson. A secure control framework for resource-limited adversaries[J]. Automatica, 2015, 51:135-148.

[11] Y. Mo, B. Sinopoli. Secure control against replay attacks[R]. In Proceedings of 47th Annual Allerton Conference on Communication, Control, and Computing, 2009:911-918.

[12] Y. Liu, P. Ning, M. K. Reiter. False data injection attacks against state estimation in electric power grids[J]. ACM Transactions on Information and System Security, 2011, 14(1):13.

[13] G. Carl, G. Kesidis, R. R. Brooks, S. Rai. Denial-of-service attack-detection techniques[J]. IEEE Internet Computing, 2006, 10(1):82-89.

[14] F. Miao, M. Pajic, G. J. Pappas. Stochastic game approach for replay attack detection[R]. In Proceedings of 52nd IEEE Conference on Decision and Control, 2013:1854-1859.

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

[16] J. Weimer, N. Bezzo, M. Pajic, O. Sokolsky, I. Lee. Attack-resilient minimum mean squared error estimation[R]. In Proceedings of American Control Conference. 2014: 1114-1119.

[17] G. Dán, H. Sandberg. Stealth attacks and protection schemes for state estimators in power systems[R]. In Proceedings of IEEE International Conference on Smart Grid Communications, 2010:214-219.

[18] M. Pajic, J. Weimer, N. Bezzo, P. Tabuada, O. Sokolsky, I. Lee, G.J. Pappas. Robustness of attack-resilient state estimators[R]. In Proceedings of ACM/IEEE International Conference on Cyber-Physical Systems, 2014:163-174.

[19] N. Bezzo, J.Weimer, M. Pajic, O. Sokolsky, G. J. Pappas, I. Lee. Attack resilient state estimation for autonomous robotic systems[R]. In Proceedings of IEEE/RSJ International Conference on Intelligent Robots and Systems, 2014:3692-3698.

[20] A. Gupta, C. Langbort, T. Ba?ar. Optimal control in the presence of an intelligent jammer with limited actions[R]. In Proceedings of IEEE Conference on Decision and Control, 2010:1096-1101.

[21] M. Zhu, S. Martínez. On attack-resilient distributed formation control in operator-vehicle networks[J]. SIAM Journal on Control and Optimization, 2014, 52(5):3176-3202.

作者简介

张恒 2015年获浙江大学工学博士学位，现为淮海工学院校聘副教授。2016年5月聘为连云港市数学会副秘书长，系统优化与决策专业委员会主任。目前主要从事网络化控制系统安全与优化理论研究，在IEEE Trans. on Automatic Control、IEEE Trans. on Control System Technology等IEEE汇刊和IEEE CDC、ACC、IFAC等控制领域顶级会议发表多篇网络化系统状态估计与控制安全问题研究论文，发表学术论著1部，担任Peer-to-Peer Networking and Applications（Springer，SCI期刊）客座编委和包括IEEE Trans. on Automatic Control、IEEE Trans. on Control of Network Systems、IEEE Trans. on Information Forensics & Security等多个学术期刊的审稿人。

程鹏 浙江大学控制学院教授、博士生导师。主要研究领域为工业控制系统安全、网络化系统估计与控制、信息物理融合系统等。先后承担国家自然科学基金重大/重点项目，科技部863计划、支撑计划项目等国家级项目10余项，并担任国家重点研发计划"内生安全的主动防御工控系统防护技术研究"课题技术负责人。成果在ACM MobiSys, ACM MobiHoc、IEEE INFOCOM和IEEE TAC、IEEE TDSC、Automatica等发表论文50余篇。获IEEE ICCC'14 Best Pape Award、IEEE INFOCOM'14 Best Demo Award，2014年教育部科技进步一等奖，以及日本学术振兴会JSPS Fellowship等荣誉。担任IEEE Trans. Control of Network Systems，Wireless Networks等国际期刊编委，并任IEEE TCNS 信息物理融合系统安全控制特刊特邀编委。

控制系统安全的理论与应用研究进展

苗　菲

宾夕法尼亚大学　电子系统工程系

摘要：信息物理系统（Cyber-Physical Systems，CPS）的攻击实例使控制系统安全问题日益受到重视。本文通过介绍实验成功的攻击模型，分析了现有系统存在的安全隐患，并重点介绍了对控制系统攻击的检测与辨识、弹性状态估计器及控制器等方向的研究进展。在此基础之上提出了未来的研究方向。

关键词：信息物理系统（CPS）；安全控制；应用研究

1　引言

信息物理系统（Cyber-Physical Systems，CPS）是一个综合计算、网络和物理环境的复杂系统，通过计算、通信和控制技术融合与协作，实现大型工程系统的实时感知、动态控制和一体化设计，使系统更加可靠、高效、实时协同，具有重要而广泛的应用前景。信息物理系统的分布式特点为物理系统带来了风险分散、易扩展与易维护等好处；但与此同时，又使信息、控制系统安全（Security）方面的隐患容易扩展，进而影响整个物理系统，特别是保障人们日常生活的基础设施系统，如供电、供水、石油运输、交通运输等系统，以及与人们生命安全有密切联系的系统，如自动驾驶车、智能医疗设备等。一旦这些系统受到外界的恶意攻击，其造成的损失将不可估计。基础设施不能正常运行会造成大量的经济损失也会给居民的生活带来不便，而自动驾驶车、智能医疗设备在被攻击情况下执行的错误运行指令甚至会威胁使用者的生命安全。因此，从信息物理系统融合的特点出发，降低控制系统被攻击的可能性及考虑潜在的攻击风险的控制系统设计是信息物理系统亟待解决的问题。

2000年，澳大利亚昆士兰的Maroochy的无线电通讯设备遭到攻击，导致污水大规模泄漏[1]；2010年，伊朗布什尔核电站遭到Stuxnet（“震网”）的攻击[2]。这些事件的发生使得控制系统的安全问题受到了广泛关注。作为一个新兴的研究领域，从理论上分析攻击模型，到模拟针对特定系统的攻击实验；从理论分析系统在不同攻击模型下的稳定性，到根据特定控制器设计进行的实验，硬件系统、控制理论、计算机软件等多领域的科研工作者进行了不同层面的研究与合作。本文主要列举了控制理论与工程方向的几个科研团队在理论与实验方面的工作，并提出几个未来研究方向的设想。

2　信息物理系统（CPS）的攻击模型

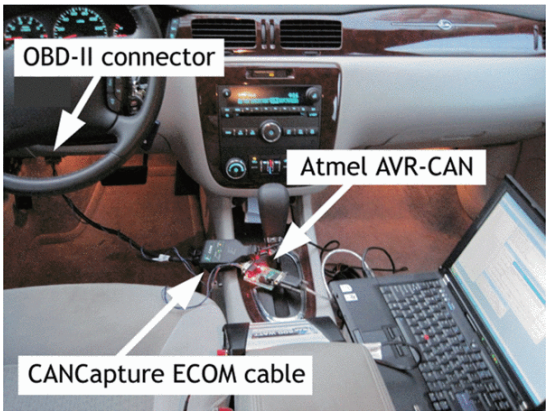
控制系统安全的研究离不开对攻击模型及现实中攻击方法的探索，根据不同攻击方式的特点提出相应的系统性预防及解决方案。对于信息物理系统的攻击可以针对系统的不同层面及组成部分，如从系统的硬件层上进行结构修改以达到修

改硬件功能的目的，此外还有物理部件如传感器、执行器的直接破坏，通讯层的窃听及数据篡改，控制器代码的修改等问题。

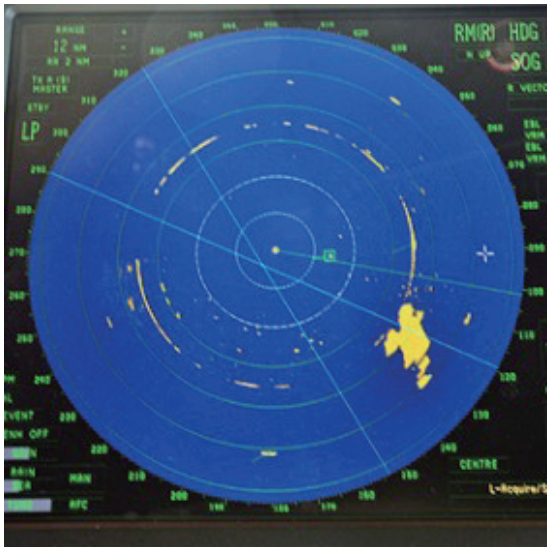
其中，直接针对物理系统的攻击和针对通讯层面的攻击可能产生等效的破坏结果。例如，分布式控制的传感器网络（如分布式控制的智能电网系统），其网络结构复杂、节点数量大，当一些节点遭到物理性破坏或切断了与其他部分的通讯后，由于缺少相应的测量信息，对电力系统的状态估计误差会增加。无论是直接对传感器物理层面进行的攻击还是通过通信过程对测量数据的修改，都属于具有一定系统模型知识的攻击，它不同于一般的系统故障或环境干扰，这类攻击能够巧妙利用系统的模型知识，通过错误检测系统的攻击，从而在不知不觉中使状态估计器的误差逐渐偏离正确值，进而使物理系统功能瘫痪[14]。这对于大规模网络控制系统是极其危险的。

大规模的信息物理系统如智能电网，不便于进行攻击模型的实验检测，但一些单机系统如车辆、游轮等，为科研工作者提供了实际可检测的实验系统。美国华盛顿大学的安全控制课题组设计了关于车辆的传感器、控制器、执行器，作为可攻击性实验平台，如图1（a）所示。实验表明，现有的未考虑控制系统可能受到攻击的车辆控制系统设计并不能满足安全性能的要求[3]。2013年，德州大学奥斯汀分校的GPS技术研究团队通过自主设计的价值2000美元的硬件，向导航系统传递虚假的GPS信号，导致一辆游艇偏离预定航线[4]，这将十年前关于攻击GPS系统的理论[5]变成了现实，并证明了不加密的民用GPS系统被攻击的可行性。被攻击后的游艇的控制台如图1（b）所示。

这些对于现有系统进行的可攻击性实验表明，控制系统安全问题并不仅仅存在于理论层面，在日常生活中也可能会遇到。随着自动驾驶车、智能可穿戴设备、智能医疗器件等越来越多的信息物理系统及其互联而成的复杂系统的发展和使用，在出现攻击实例后才考虑控制系统的安全已远远不能满足人们的需求。科研工作者已经认识到了这一问题的重要性，并从控制系统设计的初始就开始考虑整个系统今后可能面临的各种攻击及安全隐患，以尽早检测攻击及系统的运行错误，及时响应受到攻击环境下的弹性控制行为，尽量确保整个系统的安全性。



（a）用于进行车辆控制系统攻击实验的平台



（b）GPS信息被攻击篡改后的游艇控制台

图1 进行信息物理系统攻击模型实验的平台举例

3 保证控制系统安全的方法

设计安全的控制系统主要涉及两个层面的挑

战。第一个层面是设计能够针对控制系统环境的攻击，如对传感器、控制器、通信层攻击的弹性控制系统结构和机制。第二个层面是保证生成控制算法的代码过程的安全，即保证控制系统的代码本身不被篡改，使所设计的各项功能能够正确地被执行。第二个层面的工作主要通过正规方法、形式验证等理论工具来实现。这篇文章主要举例介绍基于第一个层面的近期工作。

3.1　对控制系统攻击的检测和辨识

为保证通信内容不被截断、窃听、篡改所进行的加密解密方法的研究一直是信息安全领域的重要课题。然而对于大规模的传感器网络系统而言，对所有的通信都进行加密会增加通讯开销，降低整个网络的通信效率，这并不是一个高效实用的方法。因此，仅靠原有的信息安全方法已不能保证当今不断发展、规模日益扩大的控制系统的安全。针对信息物理系统的融合性特点，设计新的错误辨识、弹性状态估计器、兼顾控制器的优化性能及对攻击的检测率等方向的研究就成为了当今的热点课题。

在没有进行全网的通信加密、系统的传感器和执行器网络可能被选择性攻击的情况下，对于线性时不变系统这一控制系统最基本模型的错误检测和被攻击部分的辨识是建立在系统的可观测性和可控性基础之上[9]。设计弹性的状态估计器，可以保证在符合特定数量的测量传感器信息正确的情况下，状态估计的误差小于预期阈值；增加关键节点的冗余传感器，使状态估计器在部分节点被破坏或通信被切断的情况下，仍然有足够的测量信息来进行计算，并将状态估计值提供给控制器以计算相应的控制命令[6]。

相对于对每条通信数据都单独进行编码的高开销加密方式而言，将传感器测量信息在进行通信传输前进行整体编码，能够检测出原本可以成功通过统计错误检测器的被修改过的传感器测量值，而且具有能够实时生成编码矩阵、在智能攻击变换对传感器通信信道插入值的情况下随时间而变的编码矩阵的特点[10]。博弈论方法在系统可能面临多种不同类型的攻击及采用相应的安全控制措施的问题上也有着广泛的应用[8,11]，这是由系统对外界环境（攻击模型）的知识有限、对环境的判断具有不确定性的特点决定的。基于不同的控制系统及可能遇到的攻击系统模型及系统的先验知识，系统与外界环境的竞争或合作关系等，需要应用不同的博弈论模型。

3.2　弹性状态估计器及控制器

当传感器被攻击时，无论是对单个传感器测量值的修改，还是对传感器网络与状态估计器、控制器之间的通信信道的攻击，最直接的影响就是状态估计器只能根据被修改过的测量值估计系统的状态，而对系统状态的错误估计会进一步导致控制器计算出错误的执行器指令。因此，设计弹性状态估计器是降低传感器及其通信信道被攻击对系统造成的整体影响至关重要的一步。美国宾夕法尼亚大学的PRECISE LAB 课题组设计了在一半以上的传感器测量值未被修改的情况下的弹性控制器，并证明了其估计误差与测量噪声造成的误差相同[7]。关于鲁棒及弹性状态估计器的实验是用图2所示的LandShark无人车实验平台进行检验的。针对大规模传感器网络的高效、可辨识，而被攻击的传感器或通信信道的弹性状态估计器的研究也获得了进展[12]。

3.3　未来的研究方向

尽管目前控制系统安全是信息物理系统的热点研究领域，但仍然有几个相关方向的问题亟待解决。第一个问题是基于非线性系统在存在被攻击的潜在风险情况下的弹性状态估计器和弹性控制器。已有的理论模型主要研究了线性系统的安全控制问题，但非线性系统的安全控制基础理论

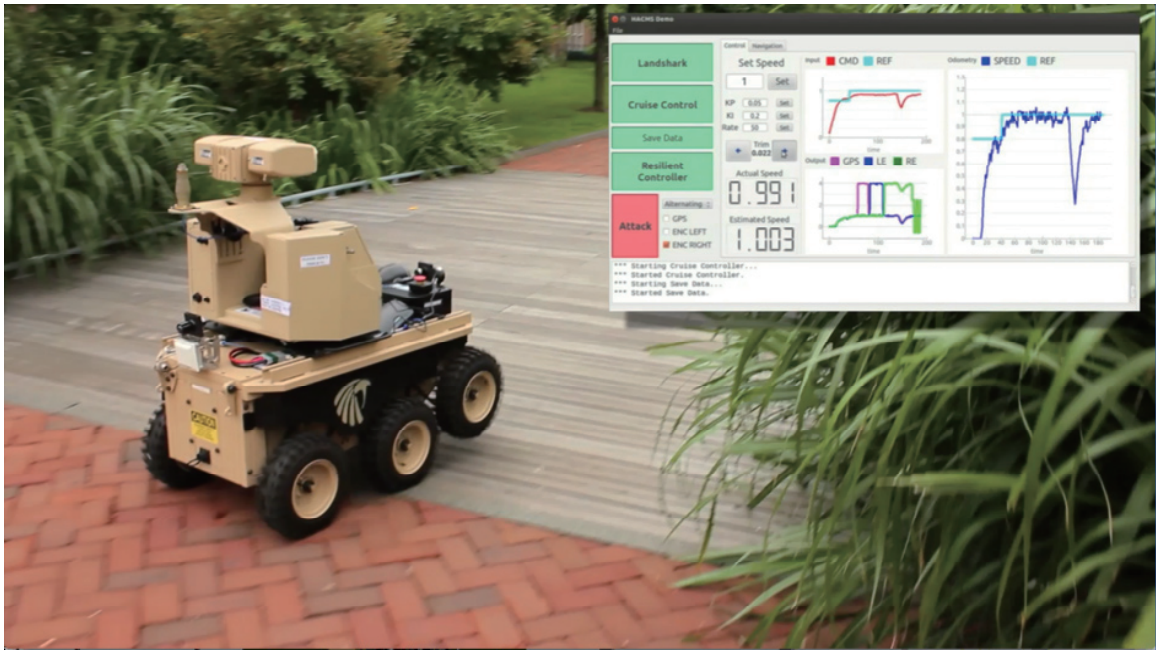


图2　宾夕法尼亚大学PRECISE LAB 进行控制系统安全研究的LandShark 无人车实验平台

研究还不够完善。第二个方向是基于多机器人协作系统在分布式控制的情况下，既保证系统运行的优化性能，又在协同策略中考虑到可能来自于外部甚至于一个团队内部不可信任的个体的错误传感器信息，是还未被充分研究的课题。第三个方向是针对智能城市这类大规模非同质系统在不同种类的传感器，在不同通信频率、不同状态估计误差要求、不同控制功能等系统设计要求下，特定系统组成部分受到攻击时，系统对于攻击的诊断辨识及弹性响应的相应措施。

4　总结展望

控制系统的安全问题是信息物理系统快速发展的工业4.0时代的重要研究课题之一，积极开展这方面的研究对在新的科技发展潮流中占据国际领先水平有着重要作用。以我国在控制理论研究方向的优势，今后主要的研究应聚焦在基于非线性、大规模非同质网络模型的理论研究，并结合自动驾驶车、智能城市等新型信息物理系统发展过程中存在的应用层面的问题，研发从系统设计层面就考虑到安全隐患的新型系统，从而在新一轮科技发展潮流中作出贡献。

参 考 文 献

[1] Jill Slay and Michael Miller. Lessons learned from the maroochy water breach[R]. In Critical Infrast. Protection, 2007:73-82.

[2] J. P. Farwell and R. Rohozinski. Stuxnet and the future of cyber war[J]. Survival, 2011, 53(1):23-40.

[3] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage. Experimental security analysis of a modern automobile[R]. In 2010 IEEE Symposium on Security and Privacy (SP),2010:447-462.

[4] “Spoofers" Use Fake GPS Signals to Knock a Yacht Off Course[J]. MIT Technology Review, 2013(8):14.

[5] J. S. Warner and R. G. Johnston. A simple demonstration that the global positioning system (gps) is vulnerable to spoofing[J]. Journal of Security Administration, 2002, 25(2):19-27.

[6] G. D′ an and H. Sandberg. Stealth attacks and protection schemes for state estimators in power systems[R]. in 2010 First IEEE International Conference on Smart Grid Communications (SmartGridComm), 2010:214-219.

[7] M. Pajic, J. Weimer, N. Bezzo, P. Tabuada, O. Sokolsky, I. Lee,and G. Pappas. Robustness of attack-resilient state estimators[R]. in 2014 ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS), 2014:163-174.

[8] Mohammadhossein Manshaei, Quanyan Zhu, Tansu Alpcan,Tamer Basar, and Jean-Pierre Hubaux. Game theory meets net work security and privacy[J]. ACM Comput. Surv.,2013, 45(3):25:1-25:39.

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

[10] Fei Miao, Quanyan Zhu, Miroslav Pajic and George J. Pappas. Coding Schemes for Securing Cyber-Physical Systems Against Stealthy Data Injectoin Attacks. Accepted[J]. In IEEE Transactions on Control of Network Systems (TCNS), 2016.

[11] F. Miao, M. Pajic, and G. Pappas, Stochastic game approach for replay attack detection[R]. in IEEE 52nd Annual Conference on Decision and Control (CDC), 2013, 12:1854-1859.

[12] Yasser Shoukry, Michelle Chong, Masashi Wakiaki, Pierluigi Nuzzo, Alberto Sangiovanni-Vincentelli, Sanjit A. Seshia, Joao. P. Hespanha, and Paulo Tabuada. SMT-Based Observer Design for Cyber Physical Systems under Sensor Attacks[R]. In Proceedings of the International Conference on Cyber-Physical Systems (ICCPS), 2016(4).

[13] G. Dan and H. Sandberg, Stealth Attacks and Protection Schemes for State Estimators in Power Systems, Smart Grid Communications (SmartGridComm)[R]. In 2010 First IEEE International Conference on, Gaithersburg, MD, 2010:214-219.

[14] Y. Liu, P. Ning, and M. K. Reiter, False data injection attacks against state estimation in electric power grids[R]. in Proceedings of the 16th ACM Conference on Computer and Communications Security. ACM, 2009:21-32.

作者简介

苗菲　2010年6月毕业于上海交通大学电子信息与电气工程学院自动化系，获工学学士学位和金融学第二专业学士学位，在校期间曾获得国家奖学金、上海市优秀学生等荣誉。2010年9月起进入美国宾夕法尼亚大学电子系统工程系攻读博士学位，于2016年5月获得博士学位及统计学硕士学位，并继续博士后研究工作。博士期间的主要研究方向为信息物理系统（CPS），主要的课题包括智能交通系统，控制系统安全及网络控制。曾在2015年4月获得CPS领域国际顶级会议6th ACM/IEEE International Conference on Cyber-Physical Systems（ICCPS，CPSWeek）的最佳论文候选。其博士毕业论文“Data-Driven Dynamic Robust Resource Allocation: Application to Efficient Transportation”获得宾夕法尼亚大学电子系统工程系2016年度最佳博士毕业论文奖。

关于举办2016中国智能车大会暨国家智能车发展论坛的通知

为了促进智能车基础理论研究、成果原始创新和高技术开发，增强我国智能车自主研发技术水平和实际应用能力，促进智能车技术产业化应用，推动其在能源、交通等领域的深入应用和产业转型升级，10月13日-10月16日，由中国自动化学会和国家自然科学基金委联合主办的2016中国智能车大会将在江苏常熟拉开帷幕，同期将会举行第八届“中国智能车未来挑战赛”，本赛事也是2016年“一带一路”无人驾驶车横跨中国科研试验的安全测试环节，着重考核无人驾驶车辆的4S性能（即安全性（Safety）、舒适性（Smoothness）、敏捷性（Sharpness）和智能性（Smartness））。

（详情请登录学会官网：www.caa.org.cn）

智能电网数据注入攻击与防御综述

邓瑞龙，梁 浩

阿尔伯塔大学 电气与计算机工程系，加拿大 埃德蒙顿

摘要：电力网络是一个大型的、复杂的、互联的基础设施，负责将电能从发电站输送到千家万户。随着计算机网络以及信息与通信技术（Information and Communications Technology，ICT）的引入，传统的电网系统正逐步向智能电网和信息物理系统（Cyber-Physical System，CPS）升级。智能电网由SCADA（Supervisory Control and Data Acquisition）系统持续监控和操作，以维持正常的运行状态，并利用坏数据检测（Bad Data Detection，BDD）过滤由于仪表故障而引入的错误测量数据。最新研究表明，一种仔细合成的数据注入（False Data Injection，FDI）攻击能够绕过坏数据检测，并能在状态估计引入任意误差而不被发现。通过修改状态变量，数据注入攻击能够误导控制中心作出错误决策，进而对电网系统发出有害的控制命令，影响电力市场的正常操作。自从数据注入攻击被提出后，人们针对如何防御该攻击对智能电网状态估计的影响进行了持续的研究。这篇综述全面地概括了相关文献。具体地，我们先从攻击者的角度探究如何构造数据注入攻击的问题；然后从系统管理员的角度探究如何防御数据注入攻击；基于以上概括，最后从数据注入攻击与防御的角度提出未来的研究方向与可能存在的挑战。

关键词：智能电网；信息安全；状态估计；数据注入；攻击防御

1 引言

电网系统是一个庞大的、互联的、复杂的基础设施，能够将电能从发电站输送到千家万户。现有的电网系统由SCADA（Supervisory Control and Data Acquisition）系统持续监控和操作，以维持正常的运行状态[1]。随着计算机网络系统以及信息与通信技术（Information and Communications Technology，ICT）的引入，电网系统正逐步向智能电网和信息物理系统（Cyber-Physical System，CPS）升级[2]。电网系统变得更开放，能够通过外部网络信息接入，如电力公司与智能电表之间的双向通信以及基于互联网的办公网络等。然而，现有的SCADA系统协议并不具备先进的数据加密能力，这就意味着它并不能直接保护通信网络中的数据流信息[3]。同时，广泛分布在不同地域的基础设施是相互依赖的，这就需要通信以维持电网系统的稳定。因此，电网系统的信息化集成，在带来发展的同时，也引入了信息安全方面的弱点，甚至被认为是对电网系统可靠运行的主要威胁[4]。潜在的协作式和复杂信息攻击也随着外部网络信息接入而引入了电网系统，使智能电网对信息攻击的防御变得不可或缺。

现实中已经出现了对SCADA系统恶意攻击的实例。澳大利亚Maroochy地区一名员工通过破坏污水处理厂的SCADA系统，将一百万升未经处理的污水恶意排放到当地地下水通道[5]。更令人恐惧的是，一种已经被设计出来的、名为Stuxnet的病毒，用于夺取对可编程逻辑控制器等特定模块的控制，并很有可能破坏这些模块所控制的物理装

置[6]。2003年，一种名为Slammer的蠕虫病毒破坏了某个离线核电站的安全控制系统，攻击了另一个电力公司的SCADA系统，还中断了其从某通信公司为SCADA网络租用的带宽[7]。最近一次针对智能电网SCADA系统的信息攻击发生在2015年12月23日，侵入乌克兰三个区域配电网系统的远程信息[8]。该攻击主要通过钓鱼电子邮件侵入、安装恶意电脑固件、阻塞电话网络等手段，造成大面积停电，对大约225,000户居民带来直接影响。随后据CNN报道，在美国的电网系统中也发现了类似的恶意代码和漏洞。

为了防御信息攻击，学术界和工业界都开展了大量研究。具体地，针对信息攻击制定了一系列的国际标准，如《NERC关键基础设施保护（Critical Infrastructure Protection，CIP）》（第五版）[9]、《NIST SP 800-53联邦信息系统与组织的安全与隐私控制》[10]、《NIST IR 7628智能电网信息安全指导准则》[11]。CIP第五版中定义了能量管理系统（Energy Management System，EMS）中电子安全周界的概念，即周界内的SCADA系统关键信息组件是被安全保护的。传统的安全措施如防火墙、杀毒软件、运行记录、视频监控等主要用于构建安全周界。这些安全措施能够防御普通的、个体的、简单的信息攻击。如何构建信息安全对策以防御更系统、更先进的信息攻击（如对乌克兰电网系统的攻击）仍然需要更多的研究。

可用性、完整性、机密性是信息与通信系统中最基本的信息安全要求。从电网系统的角度出发，智能电网的信息安全主要包括以下两方面[12]：

（1）数据与命令的可用性。拒绝服务（Denial-of-Service，DoS）攻击是一种资源消耗型攻击，包括持续快速向服务器发送请求或直接阻塞通信信道等手段。如果同时阻塞多个智能电表，就能发动分布式拒绝服务（Distributed DoS，DDoS）攻击。由于数据与命令的可用性对于电网系统的监测与控制至关重要，DoS或DDoS攻击能够破坏电网系统的正常运行。

（2）数据与命令的完整性。信息的完整性对于智能电网的监测与控制至关重要，包括数据信息收集和控制命令传达等环节。信息完整性攻击能够改变智能电网的状态估计，从而影响电力市场的运行和操作。其不仅会造成收益损失，另一方面，错误的控制命令（如打开断路器）还有可能对电网系统造成毁灭性的影响。

完整性攻击对电网系统造成的后果较为严重，同时也很难检测，因此是智能电网信息安全领域研究的重点。

电网系统主要包括发电、输电、配电、用电等环节，以及各环节与控制中心之间的双向通信。电网系统通过通信网络和远程终端设备（Remote Terminal Unit，RTU），如智能电表、传感器、执行器等收集仪表测量数据，包括输电线上的电力潮流和各节点的功率注入等。控制中心配有SCADA系统，功能包括状态估计、坏数据检测、机组组合、经济调度、故障诊断、潮流优化、负载预测等。SCADA系统基于仪表测量数据估计电网系统的状态变量，包括各节点的相位角等。控制中心利用该估计的状态对电网系统进行操作和控制，准确的状态估计对于维持智能电网的正常运行状态至关重要。为了确保状态估计的准确性，现有的SCADA系统利用坏数据检测（Bad Data Detection，BDD）过滤由于仪表故障引入的错误测量数据。

然而，最近的一项研究显示，一种仔细合成的数据注入（False Data Injection，FDI）攻击能够绕过坏数据检测，并能在状态估计引入任意误差而不被发现[13]。如要发动数据注入攻击，攻击者需要具备篡改仪表测量数据的能力，既可以直接通过操控远程终端设备本身，也可以间接通过操控远程终端设备与控制中心之间的通信数据。通过修改状态变量，数据注入攻击能够误导控制中心作出错误决策，进而对电网系统发出有害的控制

命令，这样不仅会影响电力市场的正常操作，还有可能造成电网系统大规模停电等。

2 相关文献

数据注入攻击的概念最早由Liu等人于2009年提出[13]。这类攻击被认为是针对智能电网状态估计的一种新型信息攻击。此后，人们针对怎样构造以及如何防御该攻击进行了持续研究。电网系统对数据注入攻击的弱点主要通过两种安全指标来量化，分别用于针对两种不同类型的数据注入攻击，即稀疏攻击和最小量值攻击[14]。Teixeira等人[15]将一种安全指标用于说明线性攻击策略针对交流（非线性）潮流模型的局限性。此外，他们还进一步提出了一种特定目标约束下合成秘密欺骗攻击的通用方法[16]。有关怎样构造数据注入攻击的更多参考文献详见[17,18]。

数据注入攻击可以对智能电网运行产生不同程度的影响。Dan等人考虑了攻击者篡改仪表测量数据所需的攻击成本，同时提出了贪婪算法用于预算有限情况下针对数据注入攻击的完全防御和部分防御[19]。作为一种特殊的数据注入攻击，负载重分布（Load Redistribution，LR）攻击的概念最早于2011年提出[20]。针对智能电网状态估计的数据注入攻击可以分为两种不同的模式，这两种模式将对电力市场产生不同的影响[21]。攻击者可以发动数据注入攻击得到持续的资金套利，如通过选择一对节点进行虚拟投标等手段[22]。同时，对实时电力市场发动数据注入攻击可以使某一节点上的发电商额外获利[23]。此外，通过伪造假的电力传输拥塞模式，数据注入攻击能够操纵任意目标节点上的实时电价[24]。有关数据注入攻击如何影响电力市场的更多参考文献详见[25,26]。

为防御数据注入攻击，直流（线性）状态估计可用于检测数据注入攻击[27]。Kim等人研究了如何基于线性测量模型构造数据注入攻击，并提出了通过保护一小部分仪表测量数据或部署安全的相位测量装置（Phasor Measurement Unit，PMU）的防御对策[28]。同样，对直流潮流近似下难以察觉的数据完整性攻击，可以通过部署安全的相位测量装置来进行防御[29]。有关怎样构造以及如何防御数据注入攻击的更多参考文献详见文献[30-33]。此外，Bi等人提出了通过保护一组关键状态变量的对策以防御数据注入攻击[34]。为了达到该目的，他们先仔细选出了需要保护的最小数量的仪表测量数据，并把该问题刻画成博弈论中的Steiner树模型。此外，通过同时考虑保护仪表测量数据和转化的拓扑信息，混合的防御对策在文献[35]中被提出。有关如何防御数据注入攻击的更多参考文献详见文献[36-38]。

3 构造数据注入攻击

掌握电网系统相关信息的攻击者能够成功地发动数据注入攻击，绕过现有的坏数据检测并往状态估计引入任意误差而不被发现[13]。其中，有两种攻击场景比较切合实际，一种是攻击者只能篡改某些仪表的测量数据，另一种是攻击者的攻击资源有限。研究结果表明，在两种场景下，攻击者都能有效地构造数据注入攻击并任意修改状态变量的估计值。面对潜在的数据注入攻击威胁，现有的智能电网保护机制还有待加强。

针对智能电网状态估计的安全指标可以用于量化攻击者发动秘密欺骗攻击所需的最小成本，同时保证不触发坏数据预警[14]，可以利用凸优化方法评估更复杂的攻击，同时考虑模型误差和多目标攻击。研究结果表明，仪表测量数据的冗余性能够在一定程度上提高安全指标，如增加攻击向量的量值，但攻击向量仍可以相对稀疏。

特定目标约束下的秘密欺骗攻击可以使用文献[16]中提出的通用方法进行合成，该方法还可以模拟攻击者只掌握电网系统有限信息的场景，如局部模型或过时（扰动的）模型等。研究结果表明，如果攻击者能够掌握更准确的电网系统模型，

就能够发动更剧烈地秘密欺骗攻击而不被发现。

针对智能电网状态估计的数据注入攻击可以分为两种不同的模式[21]。一是强攻击模式，是指篡改足够多的仪表测量数据，使系统管理员难以观察电网系统的状态。对于强攻击模式，可以利用图论方法找出一组最少的仪表测量数据使电网系统状态不可见。该问题可以表示成子模块图函数最小化问题，并在多项式时间内求解。二是弱攻击模式，是指攻击者只能篡改一小部分仪表的测量数据。该问题可以从决策论的角度求解。研究结果表明，最大化智能电网状态估计误差与最小化数据注入攻击被检测出的概率之间存在折中。

4　防御数据注入攻击

直流状态估计可以用于数据注入攻击[27]的检测。方法一是保护一组基本的测量数据，方法二是独立验证一组有策略地选出的状态变量。研究结果表明，保护基本的测量数据对于数据注入攻击的检测既是充分的也是必要的。

考虑到攻击者篡改仪表测量数据所需要的攻击成本，贪婪算法可以用于预算有限情况下针对数据注入攻击的完全防御和部分防御[19]。完全防御是指攻击者没有任何可能发动数据注入攻击。由于电网系统中存在相当多的仪表测量数据，想要一夜之间保护所有的仪表测量数据是不可能的。同时由于预算有限不足以支持完全防御，系统管理员会考虑优先保护一部分仪表测量数据以最大限度地改进电网系统安全指标。相应的保护策略可以用贪婪算法启发式地求解。

弱攻击模式下的数据注入可以从决策论的角度进行检测[21]。而从系统管理员的角度，可以使用基于大量历史数据的似然率测试（Generalized Likelihood Ratio Test，GLRT）方法来检测数据注入攻击，在利用先验信息的同时，结合贝叶斯公式保护并追踪电网系统可能的状态。研究结果表明，与两种传统的坏数据检测技术相比，这种通用的似然率测试方法是渐近最优的，表现在其误阱率的衰变率是最快的。

针对在直流潮流近似下难以察觉的数据完整性攻击，可以使用文献[29]中提出的一种有效算法来找出所有的稀疏攻击，然后针对该信息通过部署安全的相位测量装置进行防御。可以证明，只需最小数量的相位测量装置部署在一组有策略地选出的节点上即可防御该类数据注入攻击。

5　展望

根据IEEE 2030标准[39]，智能电网的系统框架是基于以下三个互联的子系统：①电力系统，包括发电、输电、配电、用电等环节；②通信系统，包括不同组件之间的互联与信息交换；③信息系统，包括数据信息的存储与计算，用于电网系统运行与管理决策。为了保护智能电网免受信息攻击，需要在通信系统与信息系统均部署安全措施。具体地，为通信系统设计先进的通信协议以改进通信链路对信息攻击的免疫能力。为保护数据的完整性，信息系统也需要先进的算法以检测出坏数据并消除其影响。尽管智能电网数据注入攻击与防御等话题已经在学术研究领域引起了极大关注，但仍存在许多有待解决的问题值得进一步探究。未来的研究方向与可能存在的挑战，主要包括以下几个方面：

（1）分布式的数据注入攻击与防御。现有研究大都只关注集中式的数据注入攻击与防御，而基于分布式求解的工作很少。然而，集中式的数据注入攻击要求攻击者掌握整个电网系统的拓扑结构和参数配置。另外，对于大规模的电网系统，集中式的防御对策由于算法复杂度的影响，可能导致不完全或效率低的坏数据检测结果。因此，基于分布式的数据注入攻击与防御将变得不可或缺。

（2）基于博弈论的信息安全策略。在相关文献中，攻击者与防御者之间的相互作用还未得到

充分研究。简单而言，两者之间的相互关系可以建模成一个静态的零和博弈。防御者为先手，通过部署防御资源尽可能地保护电网系统免受数据注入攻击；而攻击者为后手，寻找电网系统最薄弱的环节发动数据注入攻击。有趣的是攻击者可能完全知道、部分知道或不知道防御者的策略，但防御者作为先手事先却是完全不知道攻击者的策略。该信息不对称性对数据注入攻击与防御的影响有待研究。另外，考虑多攻击者多防御者的场景，可以利用分层博弈模型，如Stackelberg博弈来刻画相对复杂的相互作用。而且，如果从更实际的角度出发，把攻防双方的相互作用看成一个连续过程而不仅仅是单次事件，则可以利用动态博弈模型，如马尔科夫博弈来刻画状态演变过程。

（3）资源有效的防御优化。绝大部分现有工作都假设某些仪表的测量数据能够被绝对保护。换句话说，攻击者无论多强都不能篡改某些仪表的测量数据。这样的假设对于实际系统来说并不可行。一个更符合实际的假设是攻击者能否篡改某些仪表的测量数据取决于防御者在仪表上所部署防御资源的多少。从这个角度出发，一个扩展方向是设计资源有效的防御对策保护电网系统免受数据注入攻击。另一个扩展方向是决定保护哪些仪表的测量数据以及在这些仪表上部署多少的防御资源。

6 结语

综上所述，在过去的几年里，数据注入攻击被认为是威胁智能电网状态估计的一种新型信息攻击，针对数据注入攻击与防御的研究已经成为智能电网信息安全领域积极活跃却又充满挑战的话题。这篇综述一方面从攻击者的角度探究如何构造数据注入攻击的问题，另一方面从系统管理员的角度探究如何防御数据注入攻击。基于以上概括，同时提出了未来的研究方向，包括分布式的数据注入攻击与防御、基于博弈论的信息安全策略以及资源有效的防御优化等。

参 考 文 献

[1] A. Abur and A. G. Exposito. Power System State Estimation: Theory and Implementation[M]. Boca Raton:CRC Press Inc., 2004.

[2] X. Fang, S. Misra, G. Xue, & D. Yang. Smart grid—the new and improved power grid: A survey[J]. IEEE Communications Surveys Tutorials, 2012,14(4):944-980.

[3] J. Weiss. Protecting Industrial Control Systems from Electronic Threats[M]. New York, NY, USA: Momentum Press, 2010.

[4] W. Wang & Z. Lu. Cyber security in the smart grid: Survey and challenges[J]. Computer Networks, 2013,57(5):1344-1371.

[5] J. Slay & M. Miller. Lesson learned from the Maroochy water breach, in Critical Infrastructure Protection, E. Goetz and S. Shenoi, Eds., ed Boston, MA, USA: Springer, 2008:73-82.

[6] N. Falliere, et al. W32.Stuxnet Dossier v.1.4, Symantec Corporation, Cupertino, CA, USA, 2011.

[7] K. Poulsen. Slammer worm crashed Ohio nuke plant network[R]. in SecurityFocus, ed. Mountain View, CA, USA: Symantec Corporate Offices, 2003.

[9] Electricity Information Sharing and Analysis Center, Analysis of the Cyber Attack on the Ukrainian Power Grid, 2016.

[10] CIP Standards. http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

[11] NIST Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations, 2013

[12] NIST IR 7628, Guidelines for Smart Grid Cyber Security, 2010.

[13] Y. Mo, T. H. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, B. Sinopoli. Cyber-Physical Security of a Smart Grid Infrastructure[J]. Proceedings of the IEEE,2012,100(1):195-209.

[14] Y. Liu, P. Ning & M. K. Reiter. False data injection attacks against state estimation in electric power grids[R]. in Proc. ACM CCS, 2009:21-32.

[15] H. Sandberg, A. Teixeira, & K. Johansson. On security indices for state estimators in power networks[R]. in Preprints of the First Workshop on Secure Control Systems, CPSWEEK, 2010.

[16] A. Teixeira, G. Dan, H. Sandberg, & K. H. Johansson. A cyber security study of a SCADA energy management system: Stealthy deception attacks on the state estimator[C]. in IFAC World Congress, 2011,18(1):271-277.

[17] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson & S. S. Sastry. Cyber security analysis of state estimators in electric power

systems[R]. in Proc. IEEE CDC, 2010: 5991-5998.

[18] G. Hug & J. A. Giampapa. Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks[J]. IEEE Transactions on Smart Grid, 2012,3 (3):1362-1370.

[19] M. Ozay, I. Esnaola, F. T. Yarman Vural, S. R. Kulkarni & H. V. Poor. Sparse attack construction and state estimation in the smart grid: Centralized and distributed models[J]. IEEE Journal on Selected Areas in Communications, 2013,31(7):1306-1318.

[20] G. Dan & H. Sandberg. Stealth attacks and protection schemes for state estimators in power systems[R]. in Proc. IEEE SmartGridComm, 2010:214-219.

[21] Y. Yuan, Z. Li, & K. Ren. Modeling load redistribution attacks in power systems[J]. IEEE Transactions on Smart Grid, 2011,2(2):382-390.

[22] O. Kosut, L. Jia, R. J. Thomas & L. Tong. Malicious data attacks on the smart grid[J]. IEEE Transactions on Smart Grid, 2011,2(4):645-658.

[23] L. Xie, Y. Mo & B. Sinopoli. Integrity data attacks in power market operations[J]. IEEE Transactions on Smart Grid, 2011,2(4):659-666.

[24] L. Jia, R. J. Thomas & L. Tong. Impacts of malicious data on real-time price of electricity market operations[R]. in Proc. IEEE HICSS, 2012:1907-1914.

[25] S. Bi & Y. J. Zhang. False-data injection attack to control real-time price in electricity market[R]. in Proc. IEEE Globecom, 2013:772-777.

[26] M. Esmalifalak, Z. Han &d L. Song, Effect of stealthy bad data injection on network congestion in market based power system[R]. in Proc. IEEE WCNC, 2012:2468-2472.

[27] J. Lin, W. Yu, X. Yang, G. Xu & W. Zhao. On false data injection attacks against distributed energy routing in smart grid[R] in Proc. IEEE/ACM ICCPS, 2012:183-192.

[28] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt & T. J. Overbye. Detecting false data injection attacks on DC state estimation[R]. in Preprints of the First Workshop on Secure Control Systems, CPSWEEK, 2010.

[29] T. T. Kim & H. V. Poor. Strategic protection against data injection attacks on power grids[J]. IEEE Transactions on Smart Grid, 2011,2(2):326-333.

[30] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar & K. Poolla. Smart grid data integrity attacks[J]. IEEE Transactions on Smart Grid, 2013,4(3):1244-1253.

[31] S. Cui, Z. Han, S. Kar, T. T. Kim, H. V. Poor, & A. Tajer. Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions[J]. IEEE Signal Processing Magazine, 2012,29(5):106–115.

[32] Y. Huang, M. Esmalifalak, H. Nguyen, R. Zheng, Z. Han, H. Li & L. Song. Bad data injection in smart grid: Attack and defense mechanisms[J]. IEEE Communications Magazine, 2013,51(1)27-33.

[33] M. Esmalifalak, G. Shi, Z. Han & L. Song. Bad data injection attack and defense in electricity market using game theory study[J]. IEEE Transactions on Smart Grid, 2013,4(1):160-169.

[34] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang & W. Zhao. On false data-injection attacks against power system state estimation: Modeling and countermeasures[J]. IEEE Transactions on Parallel and Distributed Systems, 2014,25(3)717-729.

[35] S. Bi & Y. J. Zhang. Graphical methods for defense against false-data injection attacks on power system state estimation[J]. IEEE Transactions on Smart Grid, 2014,5(3):1216–1227.

[36] S. Bi & Y. J. Zhang. Using covert topological information for defense against malicious attacks on dc state estimation[J]. IEEE Journal on Selected Areas in Communications, 2014,32(7):1471-1485.

[37] F. Pasqualetti, R. Carli & F. Bullo. Distributed estimation via iterative projections with application to power network monitoring[J]. Automatica,2012,48(5):747-758.

[38] O. Vukovic, K. C. Sou, G. Dan & H. Sandberg. Network-aware mitigation of data integrity attacks on power system state estimation[J]. IEEE Journal on Selected Areas in Communications,2012,30(6):1108-1118.

[39] V. Kekatos & G. Giannakis. Distributed robust power system state estimation[J]. IEEE Transactions on Power Systems, 2013,28(2):1617-1626.

[40] IEEE Std 2030-2011, Guide for smart grid interoperability of energy technology and information technology operation with the electric power system, and end-use applications and loads, 2011.

作者简介

邓瑞龙　加拿大阿尔伯塔大学电气与计算机工程系博士后，研究方向包括智能电网通信、控制与安全等。

梁　浩　加拿大阿尔伯塔大学电气与计算机工程系助理教授，博士生导师，研究方向包括智能电网通信、控制与安全等。

智能电网中通信组网的网络安全综述

秦　湛，任　奎

纽约州立大学布法罗分校 计算机科学与工程学院，布法罗 纽约 14260

摘要：近年来，随着智能电网的发展与推广，一系列关于通信组网安全性的研究被发表，并受到关注。不同于其他的大规模分布式网络，智能电网中的通信组网具有不对称、多层次、多样性的通信需求。已有的安全技术并不能完全适用于智能电网中的应用。在这篇综述中，我们首先总结并分析了通信组网的结构特点，提出并结合其安全需求。随后对现有的网络安全机制进行了总结与讨论，对包括DoS攻击检测与防御、安全通信协议、匿名通信等多种技术的应用进行了分析。

关键词：智能电网；安全；密码学；拒绝服务攻击

1　引言

智能电网，是下一代电网建设中的核心概念与技术。其通过将现代化输电网络与网络通信技术进行整合，以信号侦测收集整个分布式系统中的电力供应与使用状况，从而优化调整电力生产与配送，达到节约能源、降低损耗、提升整体电网安全与可靠性的目的。智能电网中对电力配送网络以及通信网络的整合，并不仅仅是对现有电力自动化控制系统的技术升级。跨网络的整合，必须打破现有电力系统中的闭环控制系统，才能引入以分布式智能系统为代表的新兴通信网络技术[1]。智能电网中的高速双向通信使数以百万计的各种电力设备构成了新的动态交互式结构网络，并实现了智能电表基础建设（Advanced Metering Infrastructure）以及电力需求响应（Demand Response）等一系列崭新的电力管理功能。

与此同时，我们不应忽视，这些新功能、新技术的实现离不开对通信组网的高度依赖。而这种依赖也将以往针对传统电网的安全威胁与攻击扩展到了网络通信这一新的维度中。智能电网中通信组网的攻击将会带来多种潜在威胁：小到用户数据的篡改与泄露，大到复杂电力传输系统的连锁故障等[2]。智能电网中的通信组网作为一个网络系统个体，相比传统的分布式网络系统，其所面对的安全威胁规模更大、种类更多，所导致的后果也更加严重，对现有通信组网的升级也将带来更多新的潜在系统安全威胁。因此，本文首先将对与智能电网中的通信组网的安全问题构建系统模型，并对通信组网的实际安全需求与技术挑战进行分析。在此基础上，进一步介绍并总结现有的智能电网中通信组网的多种解决方案，分析其优缺点。

2　通信组网的结构与特点

各个地区的发电厂，大范围的配送网络，以及数以百万计的终端用户构成了电力输配网络这个极具复杂性的基础设施网络系统。根据广泛使用的系统模型，智能电网的结构一般分为七个模

块：发电设施、传输、分配、用户端、市场、服务以及维护。如图1所示，前四个模块构成了双向的电力与信息网络；后三个模块构成了电力管理与调配后台系统[3]。为了连接这些不同的模块，智能电网需要构建一个由骨干网以及大量局域网构成的多层次的高度分布式通信网络[4]：根据智能电网监测网络的不同，智能电网的通信组网可以分为两部分：一是电力状态监测网络构成的主干网，该网络具有局域范围内节点数量少。可横跨多个智能电网模块，带宽与计算能力强的特点。主干网架设主要分为结合现有电力网络铺设通信网络的进行建设，或是独立于已有电力网络的额外通信网络进行建设的两种方式。二是由个人用户监测网络构成的局域网，该网络的特点是临时节点数量多，带宽与计算能力弱。不仅如此，局域网络还需要同时兼容有线与无线通信网络以实现广域上的大规模分布式通讯系统。综上所述，面对一个这样复杂的多层次的高度分布式通信网络，首先必须对网络中不同模块的特点进行分析，才能提出一个全面的网络安全解决方案。

从结构复杂度的层面分析，智能电网中的通信组网具有类似于互联网的网络通信复杂度。然而，上述两个复杂网络之间仍具有许多不同之处：

首先是网络延迟与带宽需求的不同。与互联网不同，智能电网中的通信组网对数据包的传输有着更高的要求。举例来说，在互联网通信中针对下载、多媒体流、即时通信等不同服务的延迟性，最高要求（即时通信、在线游戏等）也可以在100毫秒左右。然而在电力调配的不同应用中，对于数据延迟的要求往往限制在几毫秒之内。因此，智能电网中的通信组网相较互联网具有更严格的即时性要求。对于网络攻击，如DoS攻击等的防御性要求也就更加高。相反，对于网络带宽的要求，通信组网的要求则要比互联网低。在智能电网数据流中，需要高带宽的应用往往较为少见。因此网络延迟较带宽在通信组网中更加重要。

其次是网络结构的不同。互联网要求支持任意两端的点对点通信，而智能电网的双向通信往往只存在于同一层级的中心节点与分节点之间。由此导致的不同网络流量模型也会对基于流量分析的防御机制带来影响。

综上所述，我们可以看出，与互联网相比，智能电网的通信组网虽然同样是一种大规模的通

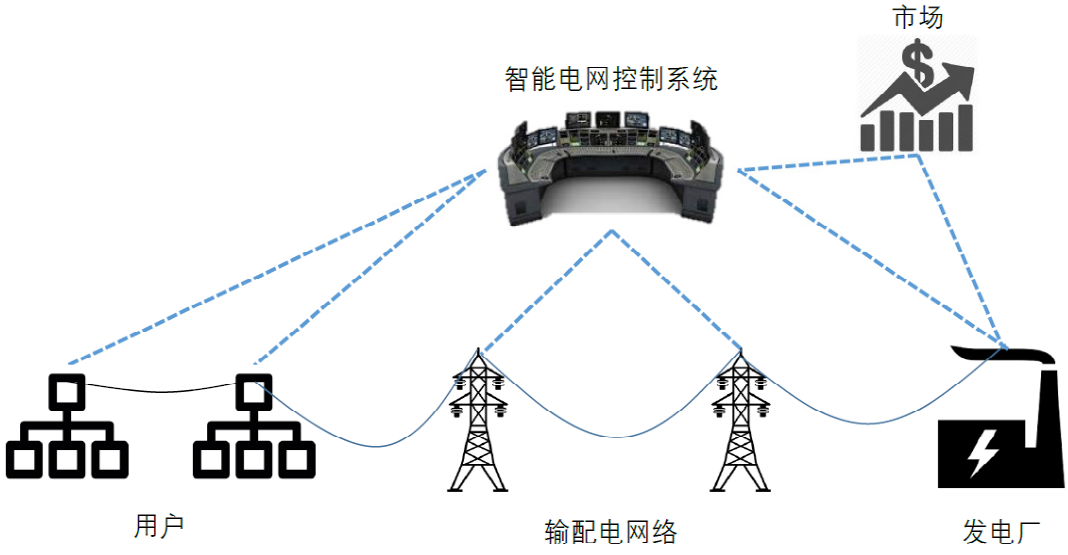


图1　智能电网网络结构（虚线表示通信网络，实线表示输电网络）

信网络，但与一般网络相比，其系统架构、功能需求等方面却不尽相同。在这种情况下，现有的基于互联网架构设计的网络安全防御机制并不能简单的搬移、应用到通信组网中。在这种情况下，重新分析通信组网的安全需求、设计相应的通信安全机制显得尤为重要。

3　通信组网的安全需求与威胁

智能网络通信组网是基于不同任务与应用的功能型网络。在提出一个全面的网络安全解决方案之前，需要明确的是通信网络的一般性安全需求。这里，我们将美国国家标准技术研究所（NIST）对下一代智能电网安全的定义作为标准。如图2所示，智能电网的安全需求可以分为三个方面：可用性、完整性以及保密性。可用性要求通信组网可以提供对数据的及时、可靠的访问。完整性要求通信组网可以避免数据被不当的更改与删除，从而提供数据的可验证性。保密性要求通信组网保证重要数据不被泄露，并提供有效的数据访问管理。以上三种安全需求的描述较为概括。具体到实际应用中，我们可以将通信组网的网络通信安全具体地对应到以下三个方面：网络攻击的侦测与防御性、数据认证与访问控制以及安全通信协议。

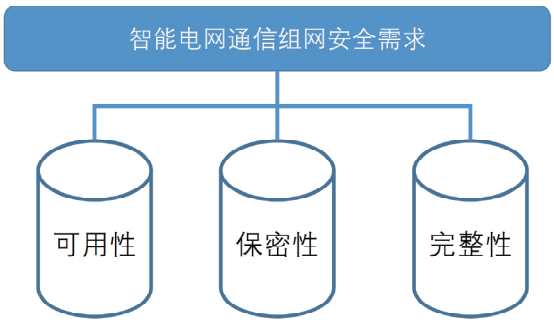


图2　智能电网通信组网的安全需求

通过比较通信组网与互联网在以上三方面的安全需求，我们可以得出以下结论：在网络攻击的侦测与防御性方面，互联网主要侧重于关键服务器与路由节点，而通信组网则对网络中每一个节点都有这样的安全性需求。其次，在数据认证与访问控制方面，互联网侧重于点对点通信数据的认证，其中的访问控制只局限于小范围内，而对通信组网内的所有数据流均需要严格的认证与访问控制。最后，对于互联网来说，大部分的数据通信是没有保密性要求的，而在智能电网中，绝大部分的数据具有较高的敏感性与保密性要求。

在通信组网中，潜在的安全威胁与攻击根据针对上述不同的安全需求，我们可以对应地分为三个类别。针对可用性的攻击：又被称为DoS攻击，目的是延迟、阻碍或破坏网络的正常通信。对于网络延迟性要求较高的输配电网络来说，对于这类攻击的防御显得尤为重要。针对完整性的攻击：攻击者通过非法篡改网络中的通信网络中数据包来达到攻击系统的目的。针对保密性的攻击：攻击者通过非法访问网络中的数据来攻击系统。

针对上述三种攻击，近年来已经有一系列的研究被提出[5-10,19-22]。具体的技术细节这里不再过多赘述，有兴趣的读者请阅读相应参考文献。这里，我们简要讨论一下通信组网的结构特点与相对应攻击的关系。首先，正如上文所述，通信组网中输配电网络以及数据采集与监控系统（SCADA）对延迟性的高要求，导致实现DoS攻击防御具有较高的技术挑战。不仅如此，由此带来的对计算效率的要求也限制了一些具有较高复杂度的加密算法的应用。其次，在数据采集的用户端对于保密性与完整性往往具有较高要求，因此这一部分的安全机制研究往往侧重于加密算法以及安全协议方向。

4　当前的解决方案

这里，我们简要介绍一些当前通信组网安全

机制的解决方案。我们主要将其分为两类：一是保护可用性的防御机制，如侦测网络流量以及防御DoS攻击等；二是保护完整性与保密性的防御机制，如基于密码技术的安全保护以及非密码技术的安全保护。

4.1 保护可用性的防御机制

由于智能电网中通信组网部分模块对于延迟性的高要求，DoS攻击常常对网络的可用性具有极大的影响。因此，对应用已有的DoS攻击防御技术，如网络流量监测、数据包过滤等技术，提出了更高的要求。类似于互联网中对DoS攻击的防御，通信组网中的防御机制也可以分为两个部分：攻击检测以及攻击缓解。在攻击检测方面，通信组网同时具有有线与无线网络，因此基于物理层的信号强度检测[11]以及基于数据包的传输层检测均可以有效发现DoS攻击[12]。绝大多数的攻击检测机制数据被动检测，现有的检测方法可以直接应用于通信组网中。需要注意的是某些分布式设备只能提供有限的计算能力。因此，基于抽样方法的攻击检测更加适用于这种情况。

在攻击缓解方面，绝大部分基于互联网的防御机制均适用于通信组网，如传输速率限制、包过滤、网络重配置等技术[13]。除了传统基于网络层的攻击缓解技术，由于无线网络同样存在于通信组网中，基于物理层的统计缓解同样适用于智能电网。针对小范围无线网络的攻击缓解技术主要基于协调式与非协调式的抗干扰技术。协调式的抗干扰技术要求收发端具有预先设定的秘钥。虽然非协调式可以提供更强的安全性，随之而来的是更高的网络延迟。因此在特定的网络环境下（如对延迟敏感不高的用户端局域网），会适用于不同的无线攻击缓解技术。

除了DoS攻击之外，作者在文献[21-22]中对于注入式攻击进行了研究。在这种攻击中，攻击者恶意上传错误的数据从而达到破坏电网系统的作用。在文献[22]中，作者提出可以用一种极大极小攻击防御模型，检测分析错误数据注入式攻击的出现。在文献[21]中，作者提出了一种三层模型用以检测对系统伤害程度最高的错误数据。这一模型将错误数据的量化检测转化为等价的单层混合整数最优解问题，为计算功能有限条件下的注入式攻击防御提出了可行的解决方案。

4.2 保护完整性与保密性的机制

保密性与完整性对智能电网在现实中的推广十分重要，尤其是对于用户端的消费者来说，通信组网中的数据传输必须提供可信赖的安全性以保护用户的隐私。如图3所示，在通信组网中，除了为维护输配电网络的所监测的数据流外，智能电网中大部分的监测数据都具有较高的敏感性。为了达到保密性与完整性，文献[14]提出了一种基于压缩技术的加密方法，使用户端可以高速上传当前的监测数据，与此同时数据监测点（Access Point）可以验证用户的身份信息。在文献[15]中，作者引入了可信第三方来保证用户上传数据的匿名性。在文献[16]中，为了保护上传数据的完整性，语义检测、安全证书等多种技术用来构成一个完整的安全协议。在文献[19]中，作者提出了一种保护用户隐私的电力使用控制系统，它利用第三方云计算平台实现复杂计算的外包。保护用户隐私的同时，在简单移动设备上实现电能使用控制的功能。

然而基于密码学的保护机制并不能完全保护用户的数据隐私。举例来说，由于智能电网中电力输送网络与数据网络同时存在，即使用户的消费数据通过密码加密传输，攻击者通过监测电力输送网络中的变化也可以得知用户的实际电力消费。通过这些数据，攻击者可以有效地得到用户的生活习惯等隐私信息。为了保护用户的隐私，不同于基于密码学的技术，文献[18]提出将用户分为若干小组，从而将单个用户的数据隐藏在整个

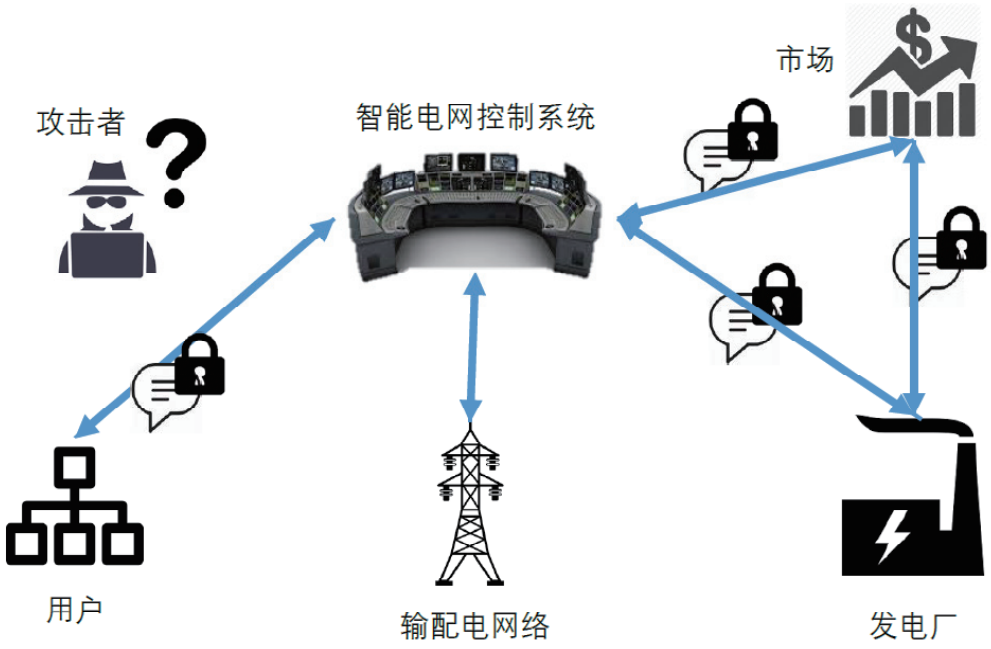


图3　通信组网结构与的保密性需求

小组的数据和中。然而这种简单的方法并不能完全抵御类似的攻击，因为攻击者还是有可能单独监测用户的电力使用数据。为了解决这一问题，通过在实际中引入一个额外的电池，使得用差分隐私技术在智能电网的应用中，保护用户使用电量成为可能。在文献[17]中，作者对当前在智能电网中利用可充电电池保护电力消费量的技术进行了总结与分析，并进一步提出了通过考虑平衡电池剩余电量来实现长时间隐私保护的研究方向。

同时，传统的完整性检测技术，如哈希函数（如SHA-1）、数字签名（如RSA或ECC）等技术，仍然适用于通信组网中。这些技术通过语义检查（通过检查数据语义的正确性）、安全证书（可信第三方的数字签名）、可信线路（数据来自于封闭的通信线路）等方法，对所收集的数据进行真实与完整性验证。在多层级的智能电网中，这样的数据完整性验证构成了一个完整的信任链。确认所上传数据的完整度需要先确认输入数据的完整度，确认输入数据的完整度需要先确认产生数据过程的完整度。与在互联网中的应用相比，智能电网在用户端对这些密码技术在计算复杂度以及通信复杂度上有着更严格的要求。与此相反，在智能电网的某些模块内的通信中，如输配电通信网络，对保密性的要求反而很低（图3）。在实际设计中需要针对不同部分通信组网提供相对应的安全性解决方案。

5　结束语

作为下一代智能电网中不可或缺的组成部分，通信组网是一个由多层级节点构成的大规模的分布式通信网络，其中不同的网络模块与层级在网络安全方面有着不同的要求。在本文中，我们提出了针对通信组网普遍性的安全模型，并在可用性、完整性以及保密性方面对通信组网的安全需求进行了讨论。通过对比互联网，智能电网中的安全组网具有不同的网络结构以及相应的安全性要求。同时，我们总结并简述了当前基于网络与密码技术的安全机制。作为一个新的研究领域，智能电网中通信组网尚未有一套成熟完整的

安全机制。然而，随着智能电网的逐步推广与实现，通信组网的安全机制必然会吸引更多的关注，成为下一个研究热点。

参 考 文 献

[1] H. Farhangi. The path of the smart grid[J]. IEEE Power and Energy Mag., 2010(8):18-28.

[2] A. R. Metke, R. L. Ekl. Smart grid security technology[R]. in Proc. of Innovative Smart Grid Technologies Conference Europe (ISGT), 2010.

[3] W. Wang, Y. Xu, M. Khanna, A survey on the communication architectures in the smart grid, Computer Networks, 2011(55):3604-3629.

[4] Office of the National Coordinator for Smart Grid Interoperability, NIST framework and roadmap for smart grid interoperability standards, release 1.0, NIST Special Publication 1108 (2010) 1-145.

[5] O. Kosut, L. Jia, L. Tong, Improving detectors for false data attacks on power system state estimation, in Proc. of 44th Annual Conference on Information Sciences and Systems (CISS ' 10), 2010.

[6] Z. Lu, W. Wang, C. Wang. From jammer to gambler: Modeling and detection of jamming attacks against time-critical traffic[R]. in: Proc. of IEEE INFOCOM 2011, 2011.

[7] D. Jin, D. M.Nicol, G. Yan. An event buffer flooding attack in dnp3 controlled scada systems[R]. in Proceedings of the 2011 Winter Simulation Conference, 2011.

[8] L. Jia, R. J. Thomas, L. Tong. Malicious data attack on realtime electricity market[R]. in Proc. of IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2011:5952-5955.

[9] L. Sankar, S. Kar, R. Tandon, H. V. Poor. Competitive privacy in the smart grid: An information-theoretic approach[R]. in: Proc. of IEEE Conference on Smart Grid Communications, 2011.

[10] F. Pasqualetti, R. Carli, F. Bullo. A distributed method for state estimation and false data detection in power networks[R]. in: Proc. of IEEE Conference on Smart Grid Communications, 2011.

[11] J. Yang, Y. Chen, W. Trappe, J. Cheng. Determining the number of attacks and localizing multiple adversaries in wireless spoofing attacks[R]. in Proc. of IEEE INFOCOM ' 09, 2009.

[12] A. Hamieh, J. Ben-Othman. Detection of jamming attacks in wireless ad hoc networks using error distribution[R]. in Proc. of IEEE ICC' 09, 2009.

[13] T. Peng, C. Leckie, and K. Ramamohanarao. Survey of network-based defense mechanisms countering the DoS and DDoS problems[J]. ACM Computing Surveys (CSUR). 2007,39(1):3.

[14] K. Moslehi, and R. Kumar. A Reliability Perspective of the Smart Grid[J]. IEEE Trans. Smart Grid. 2010,1(1):57-64.

[15] C. Efthymiou, and G. Kalogridis. Smart grid privacy via anonymization of smart metering data. Smart Grid Communications (SmartGridComm)[R]. 2010 First IEEE International Conference on. IEEE, 2010.

[16] A. Wagner, et al. Linked Data for a Privacy-aware Smart Grid.GI Jahrestagung . 2010(1).

[17] Z. Zhang, et al. Cost-friendly Differential Privacy for Smart Meters: Exploiting the Dual Roles of the Noise

[J]. IEEE Trans. Smart Grid. 2016,1(1):75-82.

[18] R. Sushmita and N. Amiya, A decentralized security framework for data aggregation and access control in smart grids[J]. IEEE Transactions on Smart Grid, 2013,4(1):196-205.

[19] H. Chun, K. Ren, and W. Jiang. Outsourceable Privacy-Preserving Power Usage Control in a Smart Grid. IFIP Annual Conference on Data and Applications Security and Privacy[R]. Springer International Publishing, 2015.

[20] X. Liu, et al. Optimal budget deployment strategy against power grid interdiction[R]. INFOCOM, 2013 Proceedings IEEE. IEEE, 2013.

[21] Y. Yuan, Z. Li, and K. Ren. Quantitative analysis of load redistribution attacks in power systems[J]. IEEE Transactions on Parallel and Distributed Systems. 2012,23(9):1731-1738.

[22] Y. Yuan, Z. Li, and K. Ren. Modeling load redistribution attacks in power systems[J]. IEEE Transactions on Smart Grid. 2011,2(2):382-390.

Cybersecurity for Communication Network in Smart Grid: Survey

Qin Zhan, Ren Kui

Computer Science and Engineering, State University of New York at Buffalo,

Buffalo, NY 14260, United States

Abstract: Nowadays, as the developing of smart grid, there are a series of works studying the security mechanisms for communication network in smart grid. Different from the existing large-scale distributed network like Internet, communication network in smart grid has the network features like asymmetric, multi-hierarchical, various latency tolerance etc. It is not suitable to apply existing cybersecurity techniques in most scenarios in smart grid's applications. In this paper, we first introduce and formulate the system architecture of the communication network in smart grid. After that, we present the security goals of this network system and the corresponding threats to it. The existing works in this area are also summarized along with an analysis of their pros and cons.

Key words: Smart Grid; Security; Cryptography; DoS Attack

第36届中国控制会议（CCC2017）征文通知

第36届中国控制会议（CCC2017）将于2017年7月26-28日在辽宁大连举办。中国控制会议由中国自动化学会控制理论专业委员（TCCT）发起，现已成为控制理论与技术领域的国际性学术会议。会议旨在为系统、控制及其自动化领域的国内外学者与技术人员提供一个学术交流平台，展示最新的理论与技术成果。会议采用大会报告、专题研讨会、会前专题讲座、分组报告和张贴论文等形式进行交流。会议的工作语言为中文和英文。会议英文论文进入IEEE Xplore数据库，并由EI收录。

（详情请登录学会官网：www.caa.org.cn）

弹性分布式能量管理研究

段　杰，周武元

美国北卡罗来纳州立大学 Advance Diagnosis，Automation and Control实验室

摘要：间歇式可再生能源、电动汽车等新型负荷和各种储能设备的广泛应用给电网运行和控制带来了新的机遇和挑战，分布式能量管理系统是解决大规模复杂电力系统优化调度的有效途径。相比于传统集中式能量管理，分布式控制结构的特点是控制中心的作用被取消了，元件由对应的局部控制器来控制，元件之间相互协调和相互影响，共同决定整个系统的功能和行为特征。但也正是由于没有控制中心的监控作用，智能设备之间的信息交互安全性缺乏保障，使其很有可能被攻击者利用，这给电力系统的稳定和用户安全造成了潜在的威胁。本文介绍了美国北卡罗来纳州立大学Advance Diagnosis，Automation and Control （ADAC）实验室提出的分布式能量管理算法，并针对信息交流安全问题，提出了一种基于“邻里守望”（neighborhood watch）原理的分布式弹性控制模型，保证分布式能量管理系统在遭到恶意信息的干扰下也能得到最优的运行计划。

关键词：能量管理系统；分布式控制；信息攻击；弹性电网

1　前言

近年来，在世界范围内的节能减排浪潮和信息技术快速发展的推动下，电力系统正发生着深刻的变革。间歇式可再生能源、电动汽车等新型负荷和各种储能设备的并网优化调度成为电力工业界和学术界关注的焦点[1]。为了保证大规模分布式电源并网之后高效稳定的运行，电网通常由能量管理系统对电源和负荷进行智能控制和自动调度决策[2]。传统电力系统的能量管理主要是集中式控制，其控制结构如图1所示。在集中式控制方式下，控制中心与各个电气设备通信，掌握反映电力系统状态的各种信息，控制中心经过优化计算后决定系统的功率运行点，向各个电气设备发出调度指令指导系统的运行[3]。

随着并入电网中的分布式电源和储能装置数量的增多，传统的集中式控制面临显著的瓶颈[4-5]：①随着分布式电源的增加，对中央控制器的计算能力要求也更加严格；②对通信能力也有较高要求，一旦中心单元故障，整个系统便面临瘫痪的风险，如果某条通信线路故障，相应的电气设备

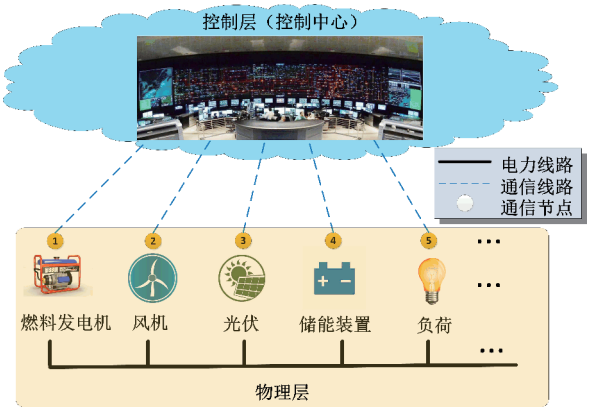


图1　能量管理系统的集中式控制结构

则不能被中央控制器控制；③每个设备需要向中央控制器提供自己的重要信息，如负荷曲线、新能源出力和发电机耗量成本，这些重要信息如果泄露则会直接损害自身的经济利益。

正因为集中式控制具有上述提及的缺点，分布式控制逐渐成为一个研究热点[6-9]。分布式控制结构如图2所示。在分布式控制方式下，控制中心的作用被取消，元件都由对应的局部控制器来控制，元件之间相互协调和相互影响，共同决定整个系统的功能和行为特征。这意味着在分布式能量管理系统中，每个物理实体不再仅仅是被动地完成电能转化和执行的装置，而是装备了“大脑”的智能体，具有一定的计算、存储和通信能力，能够对系统实现信息采取和自主行为控制。

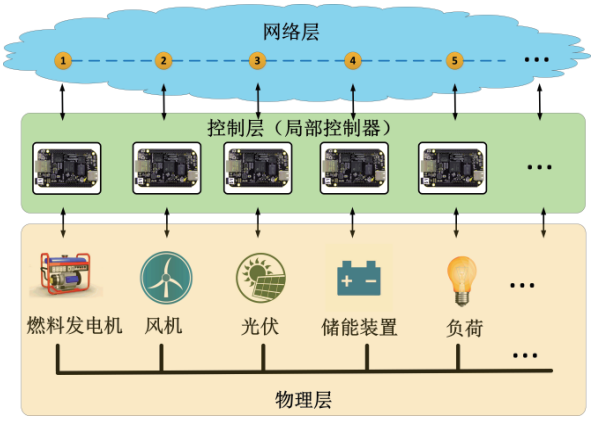


图2　能量管理系统的分布式控制结构

随着电网中数字化和信息化程度不断提高，电力一次系统和信息系统的融合越来越紧密，传统的电力系统正转化为电力物理信息融合系统（Cyber-Physical System，CPS）。但是高级信息技术的引入对电力系统的可靠性和安全性也带来了潜在的负面影响[10-11]。2010年出现的首个针对控制系统的计算机病毒“Stuxnet”，让人们清楚地认识到受到物理隔离保护的控制系统也可能受到网络攻击的威胁[12]。2015年乌克兰电网受到网络攻击，导致该国约70万居民家中停电数小时，这更是第一例由于网络攻击造成的电力系统大停电事件[13]。因此，电网中的信息物理安全风险控制机制成为急需研究的重要问题。

在分布式能量管理系统中，信息物理安全问题显得尤其突出[14-15]。分布式控制成功应用的前提条件是装备了“大脑”的智能设备的控制权得到正确使用，智能设备之间相互分享正确信息并正确决定所控设备的运行方式。但是分布式控制缺少一个中央控制器，从系统搜集各类信息对电网设备的状态进行监控、分析和诊断，因此智能设备之间信息交互的安全性缺乏保障，使其很有可能被攻击者利用。图3表示了分布式能量管理系统的部分局部控制器受到恶意攻击时的情形。

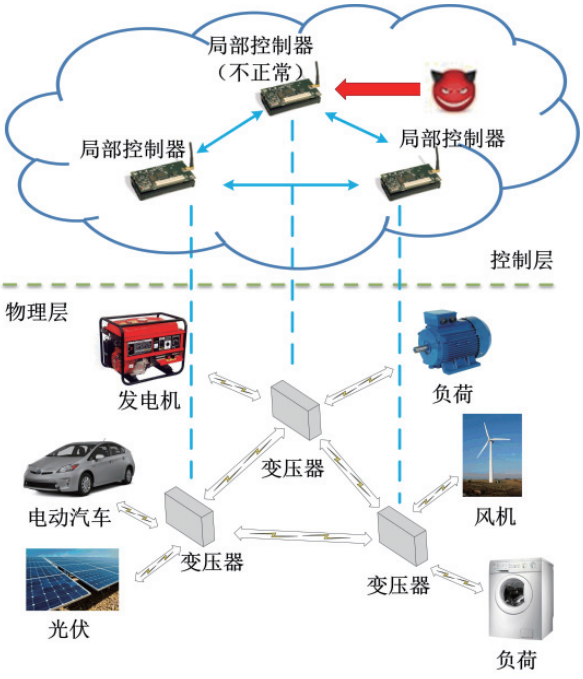


图3　分布式能量管理系统的部分局部控制器受到恶意攻击示意图

如图3所示，当系统的部分局部控制器受到恶意攻击时，其他正常局部控制器接收的部分或者全部信息可能会受到恶意篡改。虚假信息的直接结果是，正常局部控制器的调度决策被误导而得到非最优解甚至错误的功率运行点，给电力系统的稳定和用户安全造成潜在的威胁。如某个电源

设备通过通信网络向邻近用户发布虚假的低成本发电信息，使得周围的大量智能负荷，如电动汽车、智能热水器和智能空调等同时使用，造成系统过负荷。因此，在分布式控制结构下有效识别并抵御恶意攻击，让系统在受到恶意攻击时仍能够保持正常性能，最大限度减低由攻击引发的破坏，是未来实现分布式能量管理大规模应用的关键技术之一。

2　分布式能量管理算法

美国北卡罗来纳州立大学ADAC实验室提出了一种全新的分布式微网能量管理算法，用于优化分布式电源的日前出力计划[16-17]。算法以全局经济性为目标，基于可再生能源及负荷日前预测和实时电价，在满足系统物理约束条件的前提下，优化各分布式电源的基本调度曲线。其主要特点包括：

（1）控制结构为完全分布式，不存在控制中心，优化问题计算量分摊到各个局部控制器中，适用于大规模、复杂的分布式系统。

（2）虽然每个局部控制器只优化自己控制的分布式电源，但目标函数是全系统的运行成本。该分布式算法优化结果与集中式优化结果相同，能够达到系统全局最优。

（3）在通信失效下具有更好的鲁棒性，只要整个系统的通信网络拓扑保持联通状态，即没有孤立节点，则单条甚至多条通信线路的故障不会影响算法结果。

（4）在信息交互过程中，邻近局部控制器不需要分享用电负荷、发电耗量成本以及可再生能源出力情况等个人隐私信息，以避免信息泄露后被不法分子截获、篡改甚至用于其他非法途径。

2.1　微网分布式控制结构

算法考虑微网中包含柴油发电机、风电和光伏等分布式电源，储能装置和负荷系统，具有灵活的运行特性，可以并网或者脱网运行，微网结构可以如图4所示[17]。其中分布式电源风电和光伏出力主要取决于自然环境，属于不可调度机组，分布式电源柴油发电机和储能装置属于可调度机组。能量管理系统需要预测风电、光伏和负荷的出力，并根据预测出力情况、燃料机组油耗等制定可调度机组的调度计划。

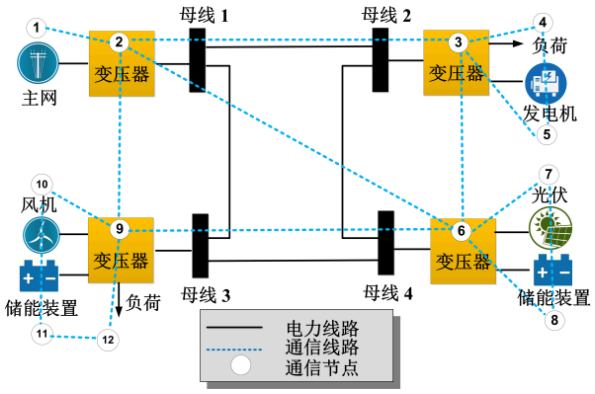


图4　微网分布式控制结构

在分布式控制结构中，每个电气设备均嵌入了局部控制器作为所控设备的“大脑”，对设备进行监控、信息采集和智能控制。局部控制器之间通过通信线路相互连接，进而实现信息在系统内的流动和分享。每个电气设备成为具有网络信息能力和自主控制能力的智能行为体，如同一个能够获取周围环境信息而执行单独任务的联网机器人一样，同时，这些“机器人”的行为是依赖于物理设备本身的性质并且以系统运行最优化为目标的。

2.2　能量管理优化模型

在微网的优化调度中，储能装置能够在电网负荷低谷期间将电能吸收并储存起来，在电网负荷高峰期间把电能释放出来，以满足用电高峰的需求，因此微网的能量管理是一个多步优化问题。

算法以小时为时间尺度，目标函数是T时间段内系统运行成本最低，运行成本考虑了燃料机组的能耗成本以及微网与主网之间的能量交互成

本。为了保证系统安全稳定地运行，算法考虑的物理约束条件包括：①功率平衡约束；②燃料机组最大发电能力约束；③燃料机组爬坡速率约束；④储能设备容量约束；⑤储能设备爬坡速率约束；⑥微网与主网之间允许交互的最大功率约束。其优化模型可以记为：

$$\min_{\mathbf{u}(t),t=1,\ldots,T}\left(J=\sum_{t=1}^{T}C\left(\mathbf{x}(t),\mathbf{u}(t),\mathbf{w}(t)\right)\right),\quad(1)$$
$$\text{s.t.}\quad \mathbf{g}(\mathbf{X},\mathbf{U},\mathbf{W})=0,\mathbf{h}(\mathbf{X},\mathbf{U},\mathbf{W})\le 0.$$

式中，x（t）表示系统的状态向量；u（t）表示系统的可控输入向量，包括储能装置的充放电计划、燃料出力计划和从主网的购电计划；w（t）表示系统的不可控输入向量，包括间歇式电源出力、负荷大小和电网电价。系统的功率平衡约束条件可以用等式方程组表示，其他物理约束条件可由不等式方程组表示。

2.3 分布式信息交流

在能量管理优化过程中，需要知道系统的全局信息，如系统的增量成本信息和系统功率不平衡值。在集中式控制结构下，控制中心可以收集系统各部分信息获得以上信息的确切值。但是，在分布式控制结构下，每个局部控制器仅能与邻近其他节点通信，获得有限范围内的局部信息。因此，在没有控制中心负责传递全局信息的情况下，局部控制器需要利用邻近节点提供的有效信息，估计系统全局信息，并保证信息估计值能够反映系统的真实情况。

算法建立了一个一致性网络[18]用于系统全局信息的估计。在一致性网络中，相邻局部控制器之间分享系统增量成本信息的估计值和自己节点的功率不平衡值。通过迭代作用逐渐实现各节点增量成本趋于一致，而且每个节点的功率不平衡估计值与系统功率不平衡实际值相等。每个局部控制器利用从一致性网络中获得的增量成本估计值以及功率不平衡估计值调整所控可调度机组的出力计划，进而实现系统的运行成本最优。图5表示每个局部控制器在一致性网络中实现的功能。

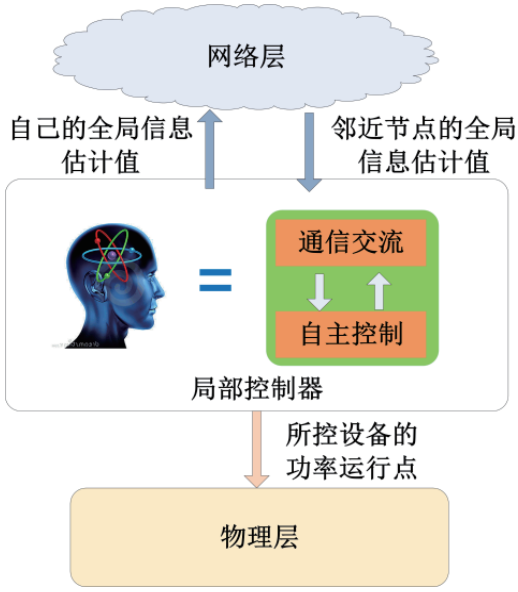


图5 局部控制器在一致性网络中实现的功能

3 分布式弹性控制

分布式能量管理容易受到恶意局部控制器所传递的错误信息的影响。一方面，分布式控制结构要求每个局部控制器与邻近节点相互协调和相互影响，共同决定系统的最优功率运行点；另一方面，分布式控制结构缺乏一个控制中心对系统中每个设备的状态进行监控、分析和诊断。因此，任意一个局部控制器向邻近节点传递的错误信息都会对系统的功率运行点产生影响，甚至影响电力系统的稳定运行。

我们提出了一种基于“邻里守望”[19]（neighbourhood watch）原理的分布式弹性控制模型[15,20]。其主要特点有：

（1）控制结构为完全分布式，每个局部控制器依靠自己储存的局部信息历史数据，判断邻近节点分享信息的正确性。局部控制器之间相互监督和制约，遏制信息分享过程中潜在的恶意行为。

（2）在用来估计系统全局信息的一致性网络

中引入反馈回路，以降低和消除错误信息对能量管理优化结果的影响。根据邻里守望的监督结果动态调节一致性网络的迭代权重因子，使正常局部控制器即使在通信网络中有错误信息存在的情况下仍能正确估计系统全局信息，进而计算得到所控分布式电源功率运行点的最优值。

3.1　邻里守望概念

顾名思义，邻里守望是指邻居间有组织的巡逻，并相互协助看护整个社区。运用到分布式能量管理系统中，是指在制定能量计划的过程中，局部控制器不仅要将自己的局部信息分享给邻近节点，而且要判断邻近节点分享信息的正确性，检测邻近节点状态是否正常。

如图6所示，假设一个系统有三个局部控制器在相互分享信息，局部控制器1需要监测邻近节点2和3的状态，同理，局部控制器2需要检测邻近节点1和3的状态，局部控制器3需要检测邻近节点1和2的状态。如果某个局部控制器侦查到正在传递错误信息的恶意控制器，不仅自己要抵御错误信息的影响，而且要将恶意的局部控制器信息通知其他相邻的节点，使系统即使在遭到不正常或者恶意的干扰下也能排除影响得到最优的运行计划。

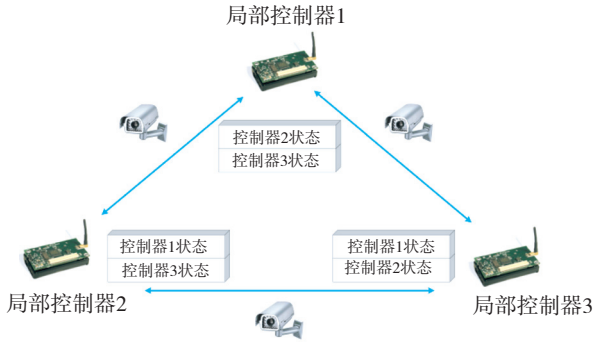


图6　分布式控制结构中的邻里守望模型

3.2　分布式弹性控制流程

对于局部控制器来说，在分布式能量管理的每一次迭代优化过程中，需要对邻近节点完成四个步骤的弹性控制，以保证即使通信网络中有错误信息的存在也不会影响系统最优化运行结果的计算。

3.2.1　错误信息甄别

在每一次迭代优化开始之前，局部控制器利用与邻近节点交流得到的历史信息数据，估计邻近节点即将分享的信息的条件期望值。在优化迭代过程中，局部控制器接收邻近节点分享的信息，将它与条件期望值作对比，判断该次信息的正确性。如果真实值与条件期望值足够接近，则认为邻近节点在此次迭代过程中传递了正确信息；反之，则认为邻近节点传递的信息被干扰或者恶意篡改。

3.2.2　声誉度管理

为了对各个局部控制器的行为进行有效约束，引入声誉度（reputation）的概念[21]，作为反映局部控制器历史行为的度量。根据每一次优化迭代中信息甄别的结果，局部控制器统计邻近节点传递正确信息的累计次数，将正确信息的累计次数转换成该邻近节点的声誉度。简单来说，如果邻近节点持续传递错误信息，那么该节点的声誉度会迅速下降；反之，则该节点的声誉度会维持在一个较高的状态。每个局部控制器对每个邻近节点单独计算声誉度，将所有邻近节点的声誉度用一个本地声誉度向量管理。

3.2.3　恶意控制器鉴定

在局部控制器的本地声誉度向量中，如果表征某邻近节点的声誉度值降到系统规定的恶意控制器阈值以下，那么对应邻近节点则被鉴定为恶意节点，该节点对应的控制器则被鉴定为恶意控制器。当控制器被鉴定为恶意控制器之后，该恶意控制器的状态就会被告知给其他正常的邻近节点，同时，该恶意控制器分享的信息也会被视为无用信息而在一致性网络中隔离。

当然，在实际应用中可以引入定时重置机制，给定一个迭代次数值循环重置声誉度，可以避免恶意控制器假借正常服务迅速提高声誉度后再开始无顾虑地破坏能量管理优化过程，也可以让因为偶然因素被错误隔离的正常控制器在一定迭代次数后重新加入系统优化过程。

3.2.4　一致性网络权重更新

根据邻近节点的声誉度动态调整一致性网络中的迭代权重因子，声誉度低的邻近节点对应迭代权重下降，其目的是削弱恶意控制器对其他节点的影响，使正常节点能够快速准确估计出系统全局信息。图7表示分布式弹性控制的框图，其中从声誉度向量输出端指向一致性网络输入端的反馈控制，表征了一致性网络权重更新的作用。

4　结束语

能量管理系统的基本功能是优化分布式电源发电计划、安排储能系统充放电、管理可控负荷、维持系统运行稳定。与集中式能量管理系统相比，分布式控制结构具有良好的可扩展性，适用于分布式电源、储能装置和可控负荷数量的急剧增多的复杂智能电网系统。同时，分布式控制结构在通信失效下具有更好的鲁棒性，可以实现分布式电源即插即用的功能，也有利于帮助保护各节点用电负荷、发电耗量成本以及可再生能源出力情况等个人隐私。因此，分布式控制将逐渐成为电网能量管理控制结构的发展方向，也将会对未来复杂大规模电网运行的便利性和高效性起到重要重要。

虽然分布式能量管理系统具有广阔的应用前景，但是，它的研究并不是一蹴而就的，目前分布式能量管理依然面临一系列的挑战，主要有以下几个方面。

可再生能源如风电、光伏出力，受自然环境的影响，具有间歇性、波动性和可预测性差的特点。在分布式优化算法的设计中需要考虑这些随机因素对调度决策的影响。

分布式控制结构依赖于局部控制器之间的相互交流，共同决定系统的功能和行为特征，通信拓扑结构的设计对通信交流效果的影响较大。因此，需要设计有效的通信拓扑结构，减少局部控制器之间的交流次数和时间。

为了使能量管理系统的决策更加真实地反映电力系统运行情况，分布式能量管理的约束条件可以进一步考虑线路损耗、电压约束、可靠性约束等，目标函数可以进一步考虑电池衰减成本、通信成本等，这对优化算法提出了更高的要求。

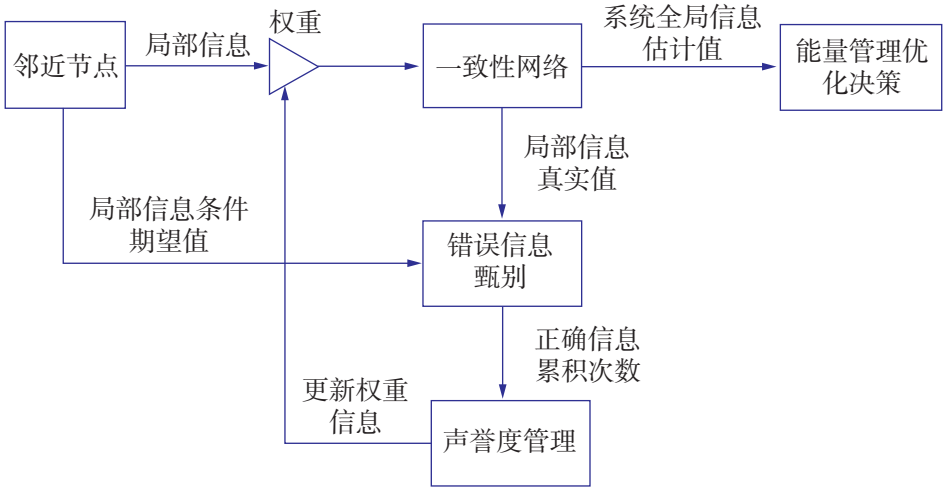


图7　分布式弹性控制框图

可靠且兼容与通信网络是能量管理系统的基础，通信可能会存在延时、超时失败等问题，从而会影响分布式能量管理系统的执行。同时，通信网络的共享和易接近等特点，使其存在安全隐患。因此，分布式能量管理系统的通信安全也是一个值得研究的问题。

参 考 文 献

[1] H. Farhangi, The path of the smart grid [J]. IEEE power and energy magazine, 2010, 8(1): 18-28

[2] Basu A K, Chowdhury S P, Chowdhury S, et al. Microgrids: Energy management by strategic deployment of DERs—A comprehensive survey [J]. Renewable and Sustainable Energy Reviews, 2011, 15(9): 4348-4356.

[3] Alippi C, Anastasi G, Di Francesco M, et al. Energy management in wireless sensor networks with energy-hungry sensors [J]. IEEE Instrumentation & Measurement Magazine, 2009, 12(2): 16-23.

[4] Zhang Z, Chow M-Y. Convergence analysis of the incremental cost consensus algorithm under different communication network topologies in a smart grid [J]. IEEE Transactions on Power Systems, 2012, 27(4): 1761-1769.

[5] Rahbari-Asr N, Ojha U, Zhang Z, et al. Incremental welfare consensus algorithm for cooperative distributed generation/demand response in smart grid [J]. IEEE Transactions on Smart Grid, 2014, 5(6): 2836-2845.

[6] Erseghe T. A distributed and scalable processing method based upon admm [J]. IEEE Signal Processing Letters, 2012, 19(9): 563-576.

[7] Hug G, Kar S, Wu C. Consensus+ innovations approach for distributed multiagent coordination in a microgrid [J]. IEEE Transactions on Smart Grid, 2015, 6(4): 1893-1903.

[8] Yang S, Tan S, Xu J-X. Consensus based approach for economic dispatch problem in a smart grid [J]. IEEE Transactions on Power Systems, 2013, 28(4): 4416-4426.

[9] Zhang Y, Rahbari-Asr N, Duan J, et al. Day-ahead Smart Grid Cooperative Distributed Energy Scheduling with Renewable and Storage Integration [J]. IEEE Transactions on Sustainable Energy, 2016, in press

[10] Sridhar S, Hahn A, Govindarasu M. Cyber–physical system security for the electric power grid [J]. Proceedings of the IEEE, 2012, 100(1): 210-224..

[11] Mo Y, Kim T H-J, Brancik K, et al. Cyber–physical security of a smart grid infrastructure [J]. Proceedings of the IEEE, 2012, 100(1): 195-209.

[12] Langner R. Stuxnet: Dissecting a cyberwarfare weapon [J]. IEEE Security & Privacy, 2011, 9(3): 49-51.

[13] North American Electric Reliability Corporation, Analysis of the Cyber Attack on the Ukrainian Power Grid [R], 2016.

[14] Duan J, Zeng W, Chow M-Y. Economic impact of data integrity attacks on distributed DC optimal power flow algorithm[C]. 47th North American Power Symposium (NAPS), 2015: 1-7.

[15] Zeng W, Zhang Y, Chow M-Y. Resilient Distributed Energy Management Subject to Unexpected Misbehaving Generation Units[J]. IEEE Transactions on Industrial Informatics, 2016, in press.

[16] Rahbari-Asr N, Zhang Y, Chow M-Y. Consensus-based distributed scheduling for cooperative operation of distributed energy resources and storage devices in smart grids [J]. IET Generation, Transmission & Distribution, 2016, 10 (5): 1268-1277.

[17] Rahbari-Asr N, Zhang Y, Chow M-Y. Cooperative distributed scheduling for storage devices in microgrids using dynamic KKT multipliers and consensus networks [C]. 2015 IEEE Power & Energy Society General Meeting, 2015: 1–5.

[18] Olfati-Saber R, Fax JA, Murray RM. Consensus and cooperation in networked multi-agent systems[J]. Proceedings of the IEEE, 2007, 95(1): 215-233.

[19] Rouf I, Mustafa H, Xu M, et al. Neighborhood watch: security and privacy analysis of automatic meter reading systems [C]. Proceedings of the 2012 ACM conference on Computer and communications security, 2012: 462–473.

[20] Zeng W, Chow M-Y, A reputation-based secure distributed control methodology in D-NCS [J]. IEEE Transactions on Industrial Electronics, 2014, 61(11): 6294-6303.

[21] He D, Chen C, Chan S, et al. ReTrust: Attack-resistant and lightweight trust management for medical sensor networks [J]. IEEE Transactions on Information Technology in Biomedicine, 2012, 16 (4): 623-632.

作者简介

段　杰　美国北卡罗来纳州立大学博士研究生，研究领域包括分布式控制、能量管理优化调度和弹性电力物理信息融合系统。

周武元　美国北卡罗来纳州立大学教授、IEEE fellow。最新研究兴趣包括分布式控制和管理理论，主要应用领域在智能电网、电池和机器人系统。曾担任IEEE Transaction on Industrial Electronics杂志主编（Editor-in-Chief）和浙江大学“长江学者”特聘教授。目前担任美国北卡罗来纳州立大学ADAC 实验室主任和IEEE Transaction on Industrial Informatics 杂志共同主编（Co-Editor-in-Chief）。

工业控制系统信息安全防护中的风险评估方法及技术

周纯杰，张　琦，秦元庆

华中科技大学 自动化学院

摘要：工业控制系统信息安全风险评估是工业控制系统信息安全防护的基础和关键。本文分别从定量评估、定性评估和定量定性相结合的评估三个研究方向，对工业控制系统信息安全主流的风险评估方法进行了概括描述，分析各种方法的优缺点，以帮助工业控制系统风险评估的实施者了解、选择以及改进信息安全风险评估方法。本文总结了工业控制系统信息安全风险评估目前存在的问题以及面临的挑战，为工业控制系统信息安全的研究人员提供研究方向。

关键词：工业控制系统；信息安全；信息攻击；风险评估

1　引言

工业控制系统在国民经济和人民日常生活中发挥着重要作用，是国家关键基础设施和各类工业生产的大脑和中枢神经。随着物联网的普及和两化融合的推进，工业控制系统也朝着网络化和智能化的方向发展，工业控制系统面临着信息安全的问题。近年来，由网络攻击引起的工业控制系统安全事故频发，并呈逐年增加的趋势，工业控制系统信息安全的严峻形势引起了社会的高度关注。

基于风险的安全防护及控制是业界的共识，工业控制系统信息安全风险评估是解决工业控制系统信息安全问题的关键。工业控制系统处于不同的生命周期，其信息安全风险评估的作用也是不同的。信息安全风险评估的目的是分析系统潜在的威胁来源，评估系统脆弱性的严重程度，为工业控制系统的设计实施人员提供决策信息，以便有针对性地对系统的脆弱性进行安全加固。

对传统IT系统信息安全风险评估的研究有很多，并形成了很多较为成熟的解决方案，但是由于工业控制系统自身的特点，导致针对传统IT系统的信息安全风险评估方法无法直接运用到工业控制系统上。其原因就是工业控制系统与传统IT系统的信息安全风险内容不同，工业控制系统受到入侵攻击会威胁到人民的身体健康和生命安全，破坏生态环境，对企业生产等造成经济损失，甚至会对国家经济、形象造成负面影响。另外，工业控制系统信息安全风险传播的方式与传统IT系统也不同。这些对于传统IT系统的信息安全风险评估的实施都提出了巨大的挑战。

本文对近年来工业控制系统的风险评估方法进行分析，帮助工业控制系统风险评估的实施者

基金项目：国家自然科学基金重点项目（61433006）；国家自然科学基金面上项目（61272204）

了解、选择、改进信息安全评估方法。本文还提出了工业控制系统信息安全风险评估存在的问题以及面临的挑战，也为工业控制系统信息安全的研究人员提供研究方向。

2　工业控制系统信息安全风险评估

工业控制系统的信息安全风险评估主要分析工业控制系统的潜在威胁来源以及系统脆弱性的严重程度，对工业控制系统的信息安全防护非常重要，工业与信息化部安全协调司副司长杨春艳指出“信息安全漏洞分析和风险评估工作不可或缺”[1]。利用信息安全风险评估提供的信息，结合系统的功能性需求与非功能性需求，工业控制系统的设计者可以权衡安全性与实施成本，实现最优的系统设计。根据计算方法的不同，工业控制系统信息安全静态风险评估可以分成定量风险评估、定性风险评估以及定性定量相结合风险评估。

2.1　定量风险评估

工业控制系统的定量风险评估，是工业控制信息安全领域的研究热点，有很多研究成果。这类定量风险评估中的风险量化以经济损失为主，考虑与风险相关的因素有：威胁来源、攻击概率、系统脆弱性、攻击者攻击能力、系统自身特点等。

攻击树和漏洞树都是传统IT系统的信息安全分析的常用方法，很多关于工业控制系统信息安全风险评估的研究都是基于这些方法。黄慧萍等人[2]提出一种基于攻击树的工业控制系统信息安全风险评估方法。该方法运用攻击树对工业控制系统进行信息攻击建模，然后利用概率风险评估技术计算叶节点、根节点和各攻击序列发生的概率，结合攻击目标实现后所造成的损失，即可计算得出根节点的风险值。该方法可以计算各个节点遭受信息攻击风险的概率大小，还可以得出系统攻击树中风险最大的攻击路径，有助于风险管理者找到工业控制系统中的信息安全薄弱环节和最有可能被攻击者利用的攻击路径和方式，从而重点采取防御措施。此外，本文计算攻击概率时考虑了攻击成本，为攻击概率分析提供了新颖的思路。Sandip C. Patel等人[3]提出一种基于漏洞树的SCADA系统信息安全风险评估方法。该方法在漏洞树的基础上进行拓展，添加威胁影响指数和信息漏洞指数。前者描述信息攻击产生的经济损失的多少，后者描述系统漏洞的多少。

还有很多关于工业控制系统信息安全风险评估的研究针对工业控制系统各自的特点提出有针对性的评估方法。M. A. McQueen等人[4]提出Compromise Graph对攻击能力以及系统漏洞的严重程度进行建模，并利用该模型对安全措施实施后SCADA系统信息安全风险降低量进行量化。工业控制系统的风险评估应当考虑攻击者的攻击能力，该方法的主要贡献是在评估过程中考虑了攻击者的攻击能力，并提供了一种量化攻击者的攻击能力的方法。Yu Jiaxi等人[5]利用信息安全脆弱性指数描述电力工业信息安全脆弱性严重程度，并给出量化方法，该方法主要考虑电力系统信息安全事件以及安全事故之间的因果关系。而 Matthew H. Henry 等人[6]则从信息攻击与系统组建之间的影响关系入手，提出网络安全风险模型 （Network Security Risk Model）来描述信息攻击与系统组建之间的影响关系，并利用网络安全风险模型对过程控制系统进行信息安全风险评估。此外，该文章还提出如何利用风险评估结果进一步进行风险管理。Woo 等人[7]提出一种基于最优潮流算法（Optimal Power Flow）和潮流跟踪算法（Power Flow Tracing）的电力SCADA系统的信息安全风险的量化方法。该方法利用最优潮流算法估计最小发电成本，利用潮流跟踪算法计算停电成本。将电力系统的信息安全风险量化成经济损失。J. D. Markovic-Petrovic等人[8]利用年预期损失（Annual

Loss Expectancy）量化 SCADA 系统的信息安全风险。风险评估量化过程考虑资产价值、曝光度以及安全事件的年发生率。

定量风险评估是用直观数据表达评估结果，其优点是科学、严密、客观，缺点是需要量化的数据非常多，如果存在难以获取的数据，或者是难以量化的数据，定量信息安全风险评估的应用范围将大大受限。

2.2 定性风险评估

针对定量风险评估的缺点，很多专家学者将研究重心转移到了定性风险评估上，定性风险评估用来评估某些数据难以获取或者难以量化的工业控制系统的信息安全风险。

OCTAVE (Operationally Critical Threat，Asset，and Vulnerability Evaluation) 是由美国卡耐基·梅隆大学软件工程研究所下属的CERT协调中心开发的用以定义一种系统的、组织范围内的评估信息安全风险的方法[9]，常被用于IT系统的信息安全风险评估。工业控制系统的很多关于信息安全风险评估的研究都是基于OCTAVE评估方法。张闻等人[10]参考OCTAVE信息安全风险评估方法，以国家和国家电网公司的两个风险评估指南为依据，从资产重要程度、威胁以及脆弱性的严重程度分析电力系统的信息安全风险，提出电力系统的信息安全风险计算公式，表示风险大小、资产价值、脆弱性严重程度、威胁严重程度。资产价值、脆弱性严重程度以及威胁严重程度均采取专家打分制。通过该方法可以有效地发现安全问题和缺陷，及时弥补安全漏洞，确保系统稳定运行。卢慧康等人[11]在评估资产重要程度、威胁以及脆弱性的严重程度的基础上，额外考虑了安全措施的有效性，考虑的更加全面。

与OCTAVE风险评估方法类似，CORAS是一个为安全关键系统设计的基于模型的风险评估方法[12]，基于ISO/IEC 31000风险管理标准[13]。CORAS风险评估方法也可以应用于工业控制系统的信息安全风险评估。Guillermo A. Francia等人[14]将CORAS风险评估方法用于SCADA系统的信息安全风险评估。该文章首先分析资产的重要等级，然后分析潜在攻击以及系统脆弱性，最后利用CORAS建模语言构建SCADA系统的威胁图，该威胁图是由安全专家以及利益相关人集体讨论得出的。

此外，围绕NIST（National Institute of Standards and Technology）提出风险评估框架[15]和澳大利亚的风险管理标准AS/NZS 4360:2004[16]，也有很多工业控制系统风险评估的应用研究。Song，Jae-G等人[17]提出针对核电站的信息安全风险评估方法，该方法主要分为系统识别与建模、资产分析、威胁分析、脆弱性分析四个步骤。Beggs Christopher等人[18]提出一个基于专家小组打分的SCADA 系统信息安全风险评估框架。此外，该文章还提出了攻击者攻击能力评估方法，与文献[4]相比，该文献考虑的内容更加全面细致，包括攻击者是否具有高级信息通讯技术、是否具有高级黑客工具和技术、是否具有SCADA系统知识储备、侦察能力大小、资金储备、攻击动机等。

有很多的工业控制系统信息安全风险评估方法是在攻击树、博弈模型、Petri网等信息系统常用风险评估技术的基础上，结合具体工业控制系统的特点提出有针对性的信息安全风险评估方法。Eric J. Byres 等人[19]利用攻击树计算SCADA系统的信息安全风险。该方法的思路是从攻击者的角度对SCADA系统进行信息安全风险评估，针对每一种潜在的攻击手段，分别利用专家打分制评估其攻击难度、影响程度以及被检测的概率，最终合成系统的总信息安全风险。Siru Ni等人[20]提出一种基于OMR（Object-Message-Role）形式模型的嵌入式系统的信息安全风险评估方法。OMR形式模型可以描述系统功能和安全性之间的关系。利用OMR形式模型可以定性分析信息攻击的可能性大

小和危害程度，进而获得嵌入式系统的信息安全风险。Hewett Rattikorn等人[21]建立博弈模型对智能电网的SCADA系统进行信息安全风险分析。该文章将入侵过程看作是攻击者与防御者的非合作连续完全信息非零和博弈，建立博弈树来对信息攻击进行成本收益分析。对于攻击后果的量化，该文章采用的是传统IT系统机密性、完整性和可用性评估指标。M. H. Henry等人[22]提出一种基于Petri网的SCADA系统信息安全风险评估方法。该文章中将风险定义为攻击者对控制系统的掌控程度。除了系统风险，该方法还可以识别会产生严重后果的攻击行为。F. Baiardi 等人[23]提出一种多层超图建模方法，该模型可以对关键基础设施组件之间的依赖关系进行建模，利用该模型进行关键基础设施信息安全风险评估。该文章在计算系统风险的时候，与文献[19]同样将攻击的难易程度考虑在内。

定性风险评的优点是在信息缺少或者难以量化时，仍可进行风险评估，但其评估结果含糊，需依赖评估者的主观性，因此对主要评估者的要求较高。

2.3　定性定量相结合风险评估

针对定量风险评估和定性风险评估的各自缺点，并结合各自优点，定性定量相结合的工业控制系统信息安全风险评估方法成为近年来的研究热点。定性定量相结合的评估方法主要以模糊综合评价法为主。Li Yang 等人[24]提出一种因素状态空间（Factor State Space）与模糊综合评价法（Fuzzy Comprehensive Evaluation Method）相结合的油气SCADA系统信息安全评估方法。主要思路是把整个油气SCADA系统安全性分解成调度管理中心安全性、区域管理中心安全性、区域控制中心、站点控制中心安全性和通信系统安全性五个评价指标，每个评价又由硬件安全性、软件安全性、物理环境安全性和安全管理能力四个指标构成，最后利用模糊综合评价法计算系统风险。陈连栋等人[25]提出了一种针对电力系统的信息安全风险评估方法，使用的方法也是模糊综合评价法，与其他模糊综合评价法不同的是，该方法使用BP神经网络代替专家打分，减少了主观成分和人为因素对测试的影响。马国庆等人[26]在上述风险评估的基础上，又结合了熵权法，实现数据处理的全自动化，不需要人为确定各指标的权重系数，不存在评估结果因人而异的缺点。林云威等人[27]将模糊综合评价法和D-S证据理论相结合，对评估结果进行合成，降低主观因素的影响。

此外，还有一些其他定性定量的分析方法应用于工业控制系统信息安全风险评估中。王旭等人[28]从资产重要程度、威胁以及脆弱性的严重程度三个方面评估电力系统的信息安全风险，该评估方法利用二维风险矩阵法，评估信息安全风险，将定性的过程定量化，通过风险矩阵法评估信息安全风险，不仅能够考虑风险影响的程度以及风险发生的概率，还能降低主观的不确定性。张伟等人[29]针对电力企业的云计算环境提出灰色关联定量分析方法，首先建立电力云计算应用的信息安全评价指标体系，将电力云计算应用的信息风险分解成数据管理、基础设施安全、信息安全、运营管理、风险管理、发布管理和安全架构七个评价指标，最后利用灰色关联分析方法计算系统信息安全风险。Roy Arpan等人[30]提出一种基于攻击对策树的定性定量相结合的SCADA系统信息安全评估方法，其信息安全评估过程分为定性分析和概率分析。此外，该文章还提出了一种利用多目标优化寻求最优安全策略的方法。

3　风险评估存在的问题以及面临的挑战

工业控制系统的信息安全风险评估，主要存

在忽视企业管理漏洞、后果难以客观量化、评估结果主观性强等问题。

工业控制系统的信息安全风险评估是一个综合管理、技术等多层面的系统工程。目前对风险评估方法的研究大多只考虑了系统的技术层面的脆弱性，而没有考虑管理层面的脆弱性。近年来，越来越多的攻击利用社会工程学，以及企业管理层面的漏洞对系统进行攻击，这些攻击被称为高级持续性威胁（Advanced Persistent Threat，APT）。单纯依靠技术是很难抵御这种类型的攻击，风险评估如果只对技术层面的风险进行评估，那么，其结果则无法全面地反映系统所面临的安全威胁。

对于风险评估来说，后果的量化十分重要，它关系到风险评估结果的准确性和客观性。目前，风险评估的量化方式主要分为两种。一种是利用机密性、完整性和可用性三个指标对攻击后果进行量化。这三个指标的量化依赖于专家打分，评估人员的能力会影响评估结果，主观性强，而且工业控制系统特有的人员伤亡、环境污染等后果无法利用这三个指标进行量化。另一种是基于资产的后果量化方法，建立资产间的依赖关系，分析危害性的传播过程，然后估计系统的损失。基于资产的后果量化方法的核心问题是资产基础数据的获取以及资产之间关系精确建模。

此外，目前的工业控制系统信息安全风险评估方法大多是以静态风险评估为主，动态风险评估的相关研究较少。工业控制系统动态信息风险评估是最近发展起来的研究领域，还处于起步阶段，还有很多问题需要解决。

4　总结

风险评估作为工业控制系统信息安全防护的重要组成部分，已经不仅仅是关系到工业控制系统的问题，更是关系到国计民生的重大问题。相关组织要不断加强信息安全风险评估的研究，将工业控制系统信息安全风险评估置于战略层面，建立健全各类配套的安全标准和法规，以共同推进工业控制系统信息安全工程建设。

参 考 文 献

[1] 杨春艳.信息安全漏洞分析和风险评估工作不可或缺[J].中国信息安全,2011(11):28-29.

[2] 黄慧萍,肖世德,孟祥印. 基于攻击树的工业控制系统信息安全风险评估[J].计算机应用研究,2015(10):3022-3025.

[3] Sandip C. Patel, James H. Graham, and Patricia A.S. Ralston. Quantitatively assessing the vulnerability of critical information systems: A new method for evaluating security enhancements[J]. International Journal of Information Management,2008,28(6):483-491.

[4] M. A. McQueen, W. F. Boyer, M. A. Flynn, and G. A. Beitel. Quantitative cyber risk reduction estimation methodology for a small scada control system[C]. In Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS’06),2006,9(1):226-226.

[5] Y. Jiaxi, M. Anjia, and G. Zhizhong. Vulnerability assessment of cyber security in power industry[R]. In 2006 IEEE PES Power Systems Conference and Exposition,2006,10:2200-2205.

[6] Matthew H. Henry and Yacov Y. Haimes. A comprehensive network security risk model for process control networks[J]. Risk Analysis, 2009,29(2):223-248.

[7] Pil Sung Woo and Balho H Kim. A study on quantitative methodology to assess cyber security risk of scada systems[J]. Advanced Materials Research, 2014.

[8] JD Markovic-Petrovic and MD Stojanovic. An improved risk assessment method for SCADA information security[J]. Elektronika ir Elektrotechnika, 2014,20(7):69-72.

[9] Christopher J Alberts, Sandra G Behrens, Richard D Pethia, and William R Wilson. Operationally critical threat, asset, and vulnerability evaluation (octave) framework, version 1.0. Technical report[R] DTIC Document, 1999.

[10] 张闻,孙歆.信息安全风险评估在浙江省电力公司的应用[J].浙江电力,2011,(12):78-82, 2011.,33-1080/TM.

[11] 卢慧康,陈冬青,彭勇,王华忠.工业控制系统信息安全风险评估量化研究[J].自动化仪表,2014,(10):21-25, 2014. 31-1501/TH.

[12] J. O. Aagedal, F. den Braber, T. Dimitrakos, B. A. Gran, D. Raptis, and K. Stolen. Modelbased risk assessment to improve enterprise security. In Enterprise Distributed Object Computing Conference, 2002. EDOC ' 02. Proceedings[R]. Sixth International, 2002: 51-62.

[13] Grant Purdy. Iso 31000: 2009—setting a new standard for risk management[J]. Risk analysis, 2010,30(6):881-886

[14] Guillermo A Francia III, David Thornton, and Joshua Dawson. Security best practices and risk assessment of SCADA and industrial control systems[R]. In Proceedings of the International Conference on Security and Management (SAM), page 1. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2012.

[15] Keith Stouffer, Joe Falco, and Karen Scarfone. Guide to industrial control systems (ics) security[R]. NIST special publication, 2011,800(82):16-16.

[16] AUSTRALIAN STANDARD and NEW ZEALAND STANDARD. As/nzs 4360-2004-risk management, 2004.

[17] Jae-Gu Song, Jung-Woon Lee, Cheol-Kwon Lee, Kee-Choon Kwon, and Dong-Young Lee. A cyber security risk assessment for the design of i&c systems in nuclear power plants[J]. Nuclear Engineering and Technology, 2012,44(8):919-928.

[18] Christopher Beggs and Matthew Warren. Safeguarding australia from cyber-terrorism:a proposed cyber-terrorism scada risk framework for industry adoption[R]. In Australian information warfare and security conference, 2009:5.

[19] Eric J Byres, Matthew Franz, and Darrin Miller. The use of attack trees in assessing vulnerabilities in scada systems[R]. In Proceedings of the international infrastructure survivability workshop. Citeseer, 2004.

[20] Siru Ni, Yi Zhuang, Jingjing Gu, and Ying Huo. A formal model and risk assessment method for security-critical real-time embedded systems[J]. Computers & Security, 2016,58:199-215.

[21] Rattikorn Hewett, Sudeeptha Rudrapattana, and Phongphun Kijsanayothin. Cybersecurity analysis of smart grid scada systems with game models[R]. In Proceedings of the 9th Annual Cyber and Information Security Research Conference, CISR ' 14, 109-112, New York, NY, USA, 2014. ACM.

[22] M. H. Henry, R. M. Layer, K. Z. Snow, and D. R. Zaret. Evaluating the risk of cyber attacks on scada systems via petri net analysis with application to hazardous liquid loading operations[R]. In Technologies for Homeland Security, 2009. HST ' 09. IEEE Conference on, 2009,5:607-614.

[23] F. Baiardi, C. Telmon, and D. Sgandurra. Hierarchical, model-based risk management of critical infrastructures[C]. Reliability Engineering & System Safety, 2009,94(9):1403-1415. {ESREL} 2007, the 18th European Safety and Reliability Conference.

[24] Li Yang, Xiedong Cao, and Jie Li. A new cyber security risk evaluation method for oil and gas {SCADA} based on factor state space. Chaos, Solitons & Fractals, 89:203 - 209, 2016. Nonlinear Dynamics and Complexity.

[25] 陈连栋,吕春梅.基于模糊神经网络的电力系统信息安全风险评估[J].河北电力技术,2011,(01):11-13.

[26] 马国庆,李伟.电力企业信息安全风险评估模型研究[J].价值工程,2008(08):112-114.

[27] 林云威,陈冬青,彭勇,王华忠.基于d-s证据理论的电厂工业控制系统信息安全风险评估[J].华东理工大学学报(自然科学版),2014(04):500-505,31-1691/TQ.

[28] 王旭,张建业,苑嘉航,陈涛.基于风险矩阵的电力公司信息安全风险评估[J].信息技术,2014(01):139-142+145.

[29] 张伟.电力企业云计算信息安全风险评估探讨[J].广东科技,2013,(20):49-50+75.

[30] Arpan Roy, Dong Seong Kim, and Kishor S. Trivedi. Cyber security analysis using attack countermeasure trees[R]. In Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research, New York, NY, USA, 2010,8:1-28:4.

作者简介

周纯杰　华中科技大学自动化学院教授，博士生导师，在国内较早开展工业控制系统信息安全研究，主持了包括国家自然科学基金重点项目在内的多项国家级工业控制系统信息安全相关的研究课题。全国工业过程测量控制与自动化标准化技术委员会系统及功能安全分技术委员会委员、全国信息安全标准化技术委员会委员、中国自动化学会技术过程的故障诊断与安全性专业委员会委员、中国自动化学会过程控制专业委员会委员。目前主要从事工业控制系统的安全防护与控制技术（含功能安全和信息安全）、工业互联网和智能系统的研究。在国际权威刊物发表论文40余篇。

中国自动化学会通讯　第37卷　第4期　总第187期　2016年8月

王飞跃：阿尔法Go走向何方?

人机围棋大战之后，人们惊叹计算机程序“阿尔法Go”的战绩，但对其代表的真正人工智能水平及其现实意义却众说纷纭，观点不一。较为一致的认识是，围棋的计算复杂性和计算机围棋程序的胜利象征着人类现代技术的发展已进入了一个新的阶段：从“老IT”的工业技术（Industrial Technology），经“旧IT”的信息技术（Information Technology），到了“新IT”的智能技术（IntelligentTechnology）时代。相应地，IT的时代含义已进化成为：IT=老IT+旧IT+新IT，三者平行合一，其中新IT的时代特征就是大数据、大计算、大决策，三位一体。

从阿尔法Go到通用智能命题

生命是智能之源，而著名的人类学家和哲学家德日进曾称“生命就是复杂化的物质”。实际上，对技术而言，智能的实质就是有效地简化复杂性，将其约简到人类可以理解、操作和应用的水平。因此，智能化与复杂性本质相同，“所谓复杂，就是对立统一”。如何从技术上化对立为统一，正是人工智能研究的核心问题。

黑与白、方与圆、浅与深、简与繁，古老的围棋被视为对立统一的典型复杂性游戏和智力博弈。正由于这个原因，阿尔法Go的胜利才如此引人关注。其实，作为典型的集成智能技术，阿尔法Go本身在智能理论与方法上没有创新，但在应用和实践上的确是一次巨大的飞跃。其战果主要表明，通过特征提取并形成新的状态和决策特征空间，即所谓的“价值网络”和“策略网络”，深度神经元网络技术能够合适地约简围棋态势评估和决策问题的复杂性，进而使加强学习有效，使深度搜索可行，最终使阿尔法Go的深度学习方法成功。而且，尽管数据、算法、过程都十分明确，人们仍无法解释深度网络所提取的特征之含义。虽然这使一些人对这一方法的普适性产生怀疑，但这也正是这一技术的魅力所在及其“智能性”的体现。

七十多年前，关于可计算性的“邱奇—图灵命题（Church-Turing Thesis）”激发了冯·诺依曼的灵感，著名的诺依曼结构应运而生，催生了第一台现代意义下的计算机和后来蓬蓬勃勃的信息产业。今天，阿尔法Go的成功，可否使我们有一个关于复杂性和智能化的新命题，即任何机器可求解的复杂性问题和机器可实现的智能化问题，是否都可通过类似于阿尔法Go的方法和技术来解决？

毫无疑问，阿尔法Go不会是解决智能问题的唯一途径。按照德日进的观点，充分的可调参数、可变结构和可用资源，一定可以产生智能。据此，上述命题可进一步推广为关于特定问题的通用智能命题：任何有限资源条件下机器可处理的智能决策问题，其算法程序都可以通过具有充分可调参数和可变结构的网络方式实现。

从深度学习到平行智能

提出智能命题的动机在于强化新IT的时代意识，激发想象，推动整体社会在智能技术的研发和应用上进行多样、深入、全方位的创新与实践。正如人工智能之父明斯基所言：“是什么不可思议的诀窍让我们变得智能？诀窍就是没有诀窍。智能的力量来源于我们自身巨大的多样性，而非任一单个的，完美的原理。”

首先是数据驱动的深度学习的多样化与广泛普及。综合监督学习、加强学习、集成学习，形成数据与经验虚实互动的各种平行学习方法，产生各类特定问题的可描述深度网络，进而从深度学习到深度描述、深度过程、深度决策、深度控制、深度管理，等等。阿尔法Go的实践表明，真正的大数据产生于深度分析和深度评估，而非其他过程，而将这些数据约减，并用于解析和行动，是智能技术成败的关键。

为此，在物理形态的组织之外，我们需要软件定义的虚拟组织，如软件定义的车间、软件定义的企业，在此基础上形成“生产围棋”“管理围棋”，以“自我进行（SelfPlay）”的方式，产生大数据，提取特征与规则，进行深度学习、规划、决策等。最后，利用开源、实时的社会媒体与社会网络信息，及时搜索针对性的相关情报，通过物理形态组织与软件形态组织的平行互动、形式反馈式的平行智能，实现各类组织的可编程智能化运营与管理。

从技术角度上看，深度学习与决策的普及必然导致平行智能，其核心就是软件定义一切、基于开源信息的社会计算、搜索加智能的知识自动化。工业社会是工作自动化，知识社会也必然是知识自动化。平行智能的深化，更将导致可编程的智慧经济与社会，使各类组织在面对不定、多样、复杂的问题与任务时，具有灵捷神速、聚焦准确、收敛到位的能力，从而变自然调控的“无形之手”，为智能管控的“智慧之手”。

迈向智慧社会

著名的科学哲学家波普尔认为，世界由三部分组成，即第一物理世界、第二心理世界、第三人工世界。回顾人类社会的发展，农业社会和工业社会开发了第一和第二世界，而新IT时代，就是智慧社会的开始，其原料和驱动力就是大数据，核心任务就是构建各种各样软件定义的系统SDX，开发人工世界。未来的智能世界里，SDX就是一个社会的基础智能设施，如同当代的高速公路、机场、车站、码头、电网互联网。没有这些设施，一个社会就无法被称为现代化社会。同理，没有SDX，就没有智能化社会。其实，人工智能意味着人工SDX有多广，实际智能才能有多深。

计算机围棋程序的最开发者之一，著名物理学家格林教授曾认为：对于复杂决策，人很难做到公平优化，最好让人工智能去做。阿尔法Go的成功，不但使格林的希望向现实更进了一步，也让我们对从智能技术走向智慧社会更加充满信心。

（来源：科学网博客）

刘成林：模式识别急需借鉴脑和神经科学

随着计算机硬件、互联网、大数据的发展和深度学习的广泛应用，模式识别作为人工智能的一个重要分支，其方法不断更新发展，并已在许多领域中被推广应用，关注度与日俱增。

实际上，过去20多年中，互联网搜索、视频监控、文字识别、语音识别、人脸识别、人机交互等技术成功应用的背后都有模式识别方法作为支撑。

在人工智能发展早期，模式识别与人工智能密不可分，尤其人工神经网络是人工智能和模式识别共同关心的热点。20世纪70到80年代，人工智能更关心符号推理和知识工程，与模式识别分别形成不同的学科领域。上世纪80年代人工神经网络以及这些年深度学习的兴起，又使人工智能和模式识别之间的界限重新变得模糊起来。

“人工智能领域的范围比较广，主要研究感

知、认知推理、学习和动作。模式识别主要研究感知，而感知是人和机器从环境获取信息的最重要手段，学习也是模式识别中的重要研究内容，因此可以说模式识别是人工智能最重要的分支。”中科院自动化所副所长刘成林认为，从上世纪80年代模式识别和人工智能重新融合起，特别是近年来深度学习的发展，人工智能迎来突破性的快速发展时期，同时也面临着一些局限，急需新的理论来突破。

刘成林表示，目前由于深度学习结合大数据所提供的强大功能，使得人工智能领域在图像识别、语音识别等方面的精度得到了大幅提高。但是这种高精度过于依赖大数据训练，且学习过程很不灵活。他举例说，通常需要同时用大量有类别标记的训练样本来训练深度神经网络，而不能像人脑那样从少量样本开始学习，并在有标记或无标记混合数据的感知过程中渐进学习，达到高的识别精度。

另外，刘成林解释说，现在的模式识别和智能系统在识别的可解释性，如对模式结构和语义的解释，说明为什么是或者不是某一类别以及鲁棒性，即对模糊模式和噪声模式、信息缺失的稳定性等方面表现明显不足。而小样本泛化性、自适应性、可解释性、鲁棒性恰恰又是人脑的长处。因此，模式识别学者急需从脑科学和神经科学上寻找新的借鉴，发展新的类人感知和认知机理的模式识别学习理论与方法。

“借鉴脑与神经科学研究的成果，将脑神经结构和信息处理机制融入未来信息与智能系统，已经成为国际学术与产业界发展的趋势。欧盟与美国相继推出的脑计划中，都包含了脑模拟与类脑智能研究的探索。”在刘成林看来，如今的类脑智能研究包括四个研究方向：一是借鉴脑科学研究成果，建立人类脑神经结构的模拟计算系统，可以同时促进感知、认知、学习等智能计算模型和神经科学研究的发展；二是受脑信息处理机制启发，研究基于类脑信息处理机制，同时结合深度学习和大数据的多模态信息处理和语义理解；三是通过类脑智能研究，提升机器人的智能化程度，包括智能感知、决策、学习和感知协同的灵巧动作能力；四是人机协同和智能交互的研究，使机器在交互中快速学习知识和技能，并通过人机协同结合人与机器的长处共同完成复杂的任务。

（来源：中国科学报）

科　普　园　地

虚拟现实在现实中触碰虚拟世界
——视觉盛宴背后的技术革命

早在50年前，虚拟现实就已出现，如今它有变革人类视觉体验之势。在虚拟现实重构的世界里，我们不仅有视、听、触、嗅等感觉，而且它们将变得愈发真实，与现实世界无异。与虚拟现实相对应的，还有增强现实以及混合现实，它们在改变人类视觉体验的同时，也在真切地变革我们的生活。我们既可用它们来购物，也可进行模拟驾驶，甚至还可用它来治疗疾病。尽管目前虚拟现实技术仍有许多缺陷，但它注定会在不远的将来影响我们每一个人。本文来自上海交通大学

软件学院教授杨旭波日前在“新民科学咖啡馆”活动的分享。

早在50多年前，美国电影摄影师莫顿·海利希（Morton Heilig）就发明了一台叫Sensorama的机器，它就像现在的大型游戏机一样，当我们把头放进这台机器里后，不仅会有3D的视觉，还能闻到气味、听到声音。由于海利希以及机器具有自身的缺陷，如没有互动性、仅靠事先做好的画面播放，Sensorama机器当时并没有得到很好的反响。

最早的虚拟现实体验机Sensorama

虚拟现实的早期应用

头戴显示器的发展需回溯到上世纪60年代。1968年，拥有美国麻省理工学院博士学位的科学家伊凡·苏泽兰（Ivan Sutherland），在实验室里做了一个名为达摩克利斯剑的头戴显示器，这个显示器用的是CRT显示技术，可追踪头部的动作，往哪边看就会有感应，可以实时计算眼睛看到的画面。不过那时候计算机能力非常差，显示的像素也非常低。苏泽兰当时还写了一篇很有名的论文“终极显示”，他设想未来的显示器应该能够达到分不清真实与虚拟。当我们戴上这个以后，就会看到另一个世界，在这个虚拟的世界里，我们的感觉都是真的，有点像《黑客帝国》描述的那样。但实际上，即使是现在，我们离他的设想还很远。

至于头戴式显示器的思想，最早可追溯到1613年，伽利略时代就有一个头盔望远镜的设计，通过这种方式可以看到远处的东西就在眼前，也有很好的沉浸感。今天的虚拟现实技术头盔Oculus与这些早期头戴显示设备长得比较像，只是现在非常便宜了，以前这样的设备非常昂贵，一般人接触不到。2006年，东芝（Toshiba）公司出了这样的一个设备，但设计上很失败，戴上去像怪物一样。2014年，一个名为Oculus的创新公司，让虚拟现实重新火热起来，这并非仅仅因为技术上的革命性突破，还因为其低廉的价格，让普通民众仅以300至350美元即可购买到开发版的头戴显示器。Facebook花费20亿美元收购这家公司，也令人对其刮目相看。

三星公司也设计出廉价的头戴显示器Gear VR，当把三星手机放到这个盒子里面就可以用。谷歌的纸盒眼镜Cardboard则更便宜，我们甚至可以利用谷歌开放的设计图，买两个透镜，用纸板自己动手做。谷歌主要推安卓手机，当手机装上应用程序后，手机就会分成两个屏幕，左右两个眼睛可看到不一样的画面，产生立体的效果。当我们转动的信息被手机的传感器检测到时，就可以看到互动的效果，但这个比Oculus的舒适度差一些，因为距离难以调节，加上计算能力手机要比

PC机差很多，但它仍可获得较好的沉浸感。

虚拟现实技术：在现实中触碰虚拟世界

虚拟现实（Virtual Reality），简称VR，这两个词组合在一起看似矛盾，一个虚拟一个现实，但都在虚拟现实环境中体现，由计算机生成虚拟世界，人们通过虚拟现实系统进入到这个虚构的世界里。在这个世界里，我们可通过视觉、听觉以及触觉进行感知，也有人在研究嗅觉和味觉。

虚拟现实有如下几个特点：计算机生成、多通道感知、沉浸感以及想象力。当我们把虚拟现实头戴显示器放在眼前，即可进入到另一个世界。尽管一部电影也可能会带来沉浸感，但是它没有交互性。而在虚拟现实系统中，这种沉浸感有交互性，当我们头动一下，即可看到不同角度的场景。至于想象力方面，应该说这个虚拟的世界是我们构想出来的。它可以是现实世界的复制，如开会，戴上头盔之后，我们可能置身于旧金山一个会议室；也可以是想象出来的卡通世界，是你儿时从书本中看过的一个童话世界，现实中它根本不存在。

虚拟现实系统主要包括如下几个方面：首先是内容，它的核心是一个实时计算机图形和仿真器，然后是用户界面：一个输入，一个输出，这是非常简单的关系，输入主要是对应用户的头、眼睛、手以及整个身体动作的追踪，当把这些身体的信息代入到虚拟现实世界里，身体如何动，系统一旦感知到，就会给予一个相应的反馈。

事实上，虚拟现实是多学科结合的领域。从学科角度来说，其核心是计算机图形和仿真，此外还有计算机软硬件、图像与视觉、人工智能等技术，由于要用到视觉、触觉、听觉等多感知通道，还会涉及到光、声、电、机械等。虽然Oculus已经设计得还算不错，但戴十几分钟，眼睛仍可能会有点难受，还会头晕。目前，全球顶尖学者都在研究人机工程问题，如何设计得更加舒适，当我们戴上眼镜后，有人会有大脑被三维虚拟环境控制的感觉，这可能会带来心理上的冲击，因此虚拟现实的应用还会涉及到心理学、社会学等问题。

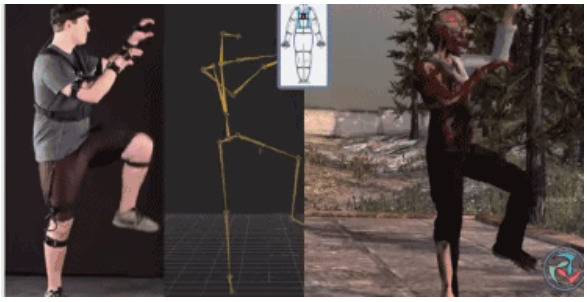
虚拟的内容最初一般由建模师通过三维电脑软件在屏幕上构建出来。例如，从一个简单的模型开始渐渐构造出复杂的角色模型，在电脑上设计出来之后，再赋予它们动作，最后贴上皮肤的纹理，这样就造出来一个虚拟的角色形象。还有一种虚拟内容，它不靠人工，而是靠一种特殊的相机——全景相机。这个相机有很多镜头，可以把360度的画面全部拍下来，数据也可以在虚拟现实中展现，这是将来一个重要的应用方向。两会期间也有一些记者用到了这样的摄像头，配上虚拟现实的头盔，我们可以从各个角度观看，也可以把数据存下来放给其他的人看。

当然，头盔并不是虚拟现实的唯一形式，还有很多其他形式，如CAVE是通过投影仪构建的，可模拟四面墙或六面墙，每个墙都用立体投影仪投出来，带上立体眼镜就很有沉浸感，但造价非常高。1999年，我在浙江大学参与安装过这样的一套系统，当时设备耗费约250万人民币。还有环幕投影，造价相对低一点，在博物馆、展览馆可看到，它应该算半沉浸式，因为整个视野没有完全被覆盖，当人转过去以后，感觉又回到现实世界。

虚拟现实技术可应用于游戏以及体育等方面

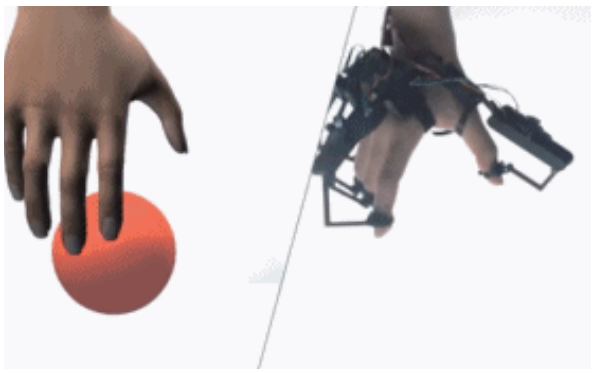
接下来是输入设备方面。输入设备需要捕捉人的信号，怎么把人的动作信号带到虚拟环境里去？最常用的设备是运动捕获设备，如演员做一

些动作，通过很多摄像头拍下来，再把这个动作放到虚拟的角色上去。输入设备又分两种：一种是光学运动捕获设备，相机加上红外线，人身上有很多发光的点，靠计算机计算能力实时算出动作，但它有一个缺点就是容易被遮挡；另一个是惯性传感设备，用户身上装了很多，手动一下就有一个惯性数据，可以算出角度。还有脸部动作捕获，电影里会经常使用，以前是在脸上加很多点，但现在技术发展了很多，不用在脸上铺点，而是直接用计算机视觉的算法来算，目前已经可做到实时。



通过数据采集，电脑可快速合成虚拟图像，在虚拟的环境里，我们可以参与不同情境

除了脸部模拟以外，还有一种数据手套，当戴上这个特殊的手套后，手活动时每个关节角度，可被手套感知到，如模拟手握杯子，通过一个力反馈设备给手部一个反馈力量，虽然没有杯子，但通过设备施加的外力，我们可以感觉到拿了一个杯子样的东西。目前这一领域仍有很多技术难点没有突破。



当我们带上“数据手套“后，通过手套给予的刺激，我们即可感受到手里紧握的物体，它可能是一个杯子或者是球等。

总之，虚拟现实的本质是一种新的计算平台、通讯平台和交互界面。从计算机发展来看，最早是大型机，一个计算机占据整个房子。彼时人是渺小的，人需要适应计算机，后来个人电脑出现的时候，人类将电脑变得越来越小，等到手机出现的时候，我们可以随时进行计算。虚拟现实应该是下一个新的计算平台，不再是你感觉跟计算机的世界隔着个屏幕，而是以后你感觉计算机构造的世界跟现实世界相互融合，尽管目前还是通过屏幕的方式展现，以后就可能分不清在哪个世界里，这是一个发展趋势，计算机将逐渐适应人的习惯。

增强现实：一个同样令人惊艳的技术

有关虚拟现实和增强现实（Augmented Reality，AR）之间的关系，很多人可能并不能准确地区分它们，另外还有一个叫混合现实。混合现实是一个从真实世界到虚拟世界的过渡， 包含了虚拟现实和增强现实。增强现实已有很多代表性的产业发展，如谷歌眼镜，但它不太成功。微软也刚推出了增强现实眼镜产品Hololens，卖得比较贵，大概3000美金。它们有一个共同的特点，就是半透明的，因为我们仍需要看到真实的现实情景，而以Oculus为代表的虚拟现实眼镜前面则是不透光的，别人看不到你的眼睛，你也看不到周围的东西，这是它们之间主要区别所在，但未来增强现实应用面更广。

一个有趣的增强现实情境，通过听、视觉让人身临其境。

例如，当我们对着镜子穿衣服时，可通过增强现实让自己换上一件别的衣服或裙子，或合适的款式，这就是所谓的虚拟试衣。它还可应用于远程会议，当戴上增强现实的眼镜之后，我

们可看到虚构的桌子以及从远处传过来的参会者影像，尽管它们置身于不同的空间，但此刻如同在同一个环境下讨论问题。最近，微软推出一个视频，通过增强现实眼镜，即使你的孩子不在身边，在增强现实的情景里，他（她）可被置身于同一个房间，让你感觉到小孩就在跟前。不过这方面现在做不到这么好，有一些概念性的成分，还有很多缺陷。增强现实还可用于汽车导航，如果我们看导航信息，需低头看汽车面板，这样可能会分心。利用增强现实技术，导航的信息直接显示在挡风玻璃上，这样就可以看到路面信息。

虚拟现实的应用：未来前景无限

虚拟现实除了可用于影视游戏等娱乐应用之外，在其他非娱乐的应用领域也前景广阔。虚拟现实同样也可用于虚拟试衣，这是阿里巴巴的“Buy+”计划，今年3月刚推出概念，戴上虚拟现实的眼镜之后，人们可通过虚拟模特身上的衣服来进行选择和购买。很多汽车公司也开始利用虚拟现实眼镜进行模拟驾驶，让用户体验开车时的感受，但不能真的开到路上。此外，还可做虚拟旅游，戴上眼镜后，可体验以前从未去过的地方，身临其境。此外，还可以虚拟看房或设计房子，我们可事先让设计师设计一个虚拟图景，通过体验，我们还可以纠正需要改造的地方。

日常生活体验可对我们的大脑有影响，同样虚拟的体验也能影响大脑，因此虚拟现实还可用于心理治疗，很多有抑郁症的人，通过虚拟现实技术辅助治疗可以得到一些改善。对于社交恐惧症患者来说，他们平时不敢对很多人说话，在虚拟的世界，你知道这是假的，心理会放松防线，更容易跟其他人交流，从而逐渐提高社交能力。再如，有很多人害怕蜘蛛，通过虚拟现实模拟，蜘蛛“近”在眼前，尽管你很难抗拒潜意识中的害怕，但是可以通过这种方式逐渐“脱敏”。恐高症同样可通过虚拟现实得到缓解。

心理学家还用虚拟现实来进行其他治疗，如烧伤患者非常痛苦，尤其是给他换药的时候，如果有医生把虚拟现实技术用到他们身上，让他戴上一个头盔，看到一个冰凉的世界，大脑相应作出反应，疼痛感会减弱。在美国911恐怖袭击之后，很多人心理创伤很大，通过虚拟现实技术，把患者带回到当时的环境，这也是一个类似于“脱敏”的治疗，从而使患者心理上得到疏解，目前证明可以起到比较明显的效果。此外还有对自闭症患者的治疗，他们不愿跟人交流，难以亲近，通过虚拟现实技术，让他们在虚拟的世界里玩游戏，并逐渐接受自己在其中的角色，然后锻炼跟人交往的技巧。研究发现治疗前后患者大脑的活跃度有明显改善，这说明虚拟现实起到了良好的作用。

在医疗方面，虚拟现实还可用来训练医生。当前医生培训代价比较高，既缺少设备，同时人又非常多，我们可以通过虚拟现实设备，帮助医生练习手术。例如，在虚拟的世界里，连接力反馈的设备可模仿一个手术刀，当手术刀碰到虚拟器官之后，会有一个力反馈，也会模拟器官的形变，通过这种方式医生可以得到手术技能的锻炼。

对于学习和教育来说，虚拟现实也是非常有帮助的。通常来说，小孩对形象直观的东西容易接受，通过虚拟现实技术，把一些比较抽象的东西，以直观方式表现出来，这样可提高他们的记忆能力和学习动机，通过这种方式他们既愿意学习，又觉得很好玩，此外也可以增强小孩子间的合作。

总的来说，虚拟现实已经诞生50多年，由于以前成本太高，它最近才刚刚走近大众。虚拟现实、增强现实它们之间相关，又各有特点，但核心都是以实时计算机图形为主，应用也在不断拓广。通过与互联网、机器人、人工智能以及大数据进一步结合，虚拟现实的未来应用会更广泛。

（来源：知识分子）

加快发展智能机器人技术和产业 培育新的科技发展动能

近日，我国智能机器人研发又取得了一项国际水平的成果，北京大学口腔医学院吕培军教授科研团队成功研制出国际首套“牙体预备小型机器人系统”，该系统采用自动控制飞秒激光束，严格按照临床医学标准和规范要求，在患者口腔内精确定位并自动完成各种牙齿治疗需要的切割与磨除，当与其他数字化义齿制作设备同步联用时，可快速完成患者的义齿修复治疗，大大地提高治疗精准程度和工作效率，缩短治疗时间，改善患者就医的舒适度。该成果已获得国际发明专利1项，国内发明专利8项，申报软件著作权2项，发表SCI/EI论文22篇，在英国《自然》（Nature）、杂志子刊《科学报告》（Scientific Reports）上发表论文6篇。

“十二五”期间，我国医疗领域智能机器人研发进展较大，取得了一系列具有自主知识产权的研发成果。骨科机器人研发方面，北京积水潭医院田伟教授科研团队联合北京航空航天大学、北京天智航医疗科技股份有限公司等单位制定了国内首个“骨科机器人产品标准”，研发了“GD2000骨科机器人导航定位系统”和“GD-S骨科机器人导航定位系统”，并用于日常手术，填补了国内空白。脑科机器人研发方面，海军总医院田增民教授科研团队联合北京航空航天大学先后研制成功了机器人辅助脑外科立体定向手术系统CRAS-BH1、CRAS-BH2、CRAS-BH3和黎元BH-600，目前已对多种脑外科疾病进行了5000余例定向手术治疗。

随着人工智能、数字化制造与移动互联网创新融合步伐的不断加快，具有感知、识别、认知等功能的智能机器人技术和产业成为当今衡量一个国家科技创新和制造业水平的重要标志。目前，我国工业机器人研发在关键部件、产品与产业化方面与发达国家依然存在较大差距，但智能机器人领域所取得的研发成果可以成为我国机器人发展的突破口，大力发展智能机器人技术和产业对推动供给侧结构改革、培育新的科技发展动能和新产业具有重大现实意义，需要从国家战略层面予以重视。

1. 加大支持力度，推进智能机器人核心技术的研发。在“十一五”和“十二五”科技发展规划和布局的基础上，“十三五”期间瞄准智能机器人前沿和热点，进一步凝练和聚焦，加大资金支持力度，加快核心技术研发，突破产业技术瓶颈，推动面向医疗康复、家庭服务、公共安全等领域智能机器人的研发。

2. 梳理整合智能机器人研发成果，支持智能机器人成果转化。“牙体预备小型机器人系统”“GD2000骨科机器人导航定位系统”和“GD-S骨科机器人导航定位系统”以及“机器人辅助脑外科立体定向手术系统”如能转化装备县级医院，国内将有至少3万台套的市场前景，产生约100亿元人民币产值，具有广阔的市场前景，同时可帮助解决目前我国高水平医生短缺、看病难、看病贵的问题。因此，应及时梳理“十一五”和“十二五”期间智能机器人研发成

果，加大成果转化支持力度，培育新产业，同时积极参与国际竞争，走向国际市场。

3. 加快制定智能机器人标准体系和人机交互安全规则。开展智能机器人国内标准体系的顶层设计，制定完善智能机器人产业标准体系，加快智能机器人在国内的推广应用。同时，积极参与智能机器人国际标准的制定，促进我国智能机器人参与国际市场竞争。此外，智能机器人与人的互动过程中会产生涉及操作行为和个人隐私的安全性问题，应制定完善人机交互安全规则。

（作者简介：郑彦宁，中国科技信息研究所科技报告服务与产业情报研究中心主任；梁琴琴，中国科技信息研究所科技报告服务与产业情报研究中心博士后）

（来源：中国科技网）

2016年人工智能最重要的发展：面向所有人的深度学习

过去一年，深度学习领域发生了很多事情。有很多令人拍案叫绝的案例，如微软用多达152层的神经网络（通常只有六七层），漂亮地赢得ImageNet比赛冠军。但过去6个月里，对深度学习影响最为深远的，还是商业模式的大转变。

突然之间——真的可以说是突然之间，亚马逊、IBM、谷歌、Facebook、Twitter、百度和微软这些巨头都将代码开源。其中，谷歌还像商业顾客免费使用这家公司的旗舰AI产品——TensorFlow。

从2015年底到今年8月，下面列出的这些项目都开源了。

Company	Cloud Machine Learning Platform	Deep Learning Now Open Source
Amazon	Amazon Machine Learning	DSSTNE (sounds like Destiny) Deep Scalable Sparse Tensor Network Engine
Baidu	None	Deep Speech 2
Facebook	None	TorchNet (built on the previously open source Torch library)
Google	Google NEXT Cloud Platform	TensorFlow
IBM	IBM Watson Analytics	IBM System ML
Microsoft	Azure Machine Learning	CNTK-Computational Network Toolkit
Twitter	None	Twitter Cortex
Yahoo	None	CaffeOnSpark

如果你是谷歌的商业客户，或者是愿意花时间做开源代码的开发员，所有这些优质IP都任你挑选。那么，是什么促成了这股开源浪潮？为什么会发生如此大的转变？人类最先进、最神奇的技术，就像超市里的促销品。

情况确实如此，但只说对了一半。推动开源的原因有以下几点。

主导深度学习及应用

上图所提到的8家公司中，有一些是云服务平台，他们想要扩大用户基础，而另一些，包括提供云服务的在内，是以深度学习为发展引擎的数字技术公司。

深度学习处在图像识别、自动标记、文本语音转换、自动翻译以及语义分析的核心。此外，以亚马逊为代表，深度学习也开始应用于推荐系统和异常检测（如欺诈交易）。因此，不难理解为什么巨头都要将深度学习视为攸关生死存亡的技术和能力。

对这些公司而言，文字和图像识别与分类的应用，还有购物推荐对亚马逊的意义显而易见。不过，这个道理就没那么明显了：开发出用户数

量最多、普及程度最广的AI平台的人，将成为新兴市场的主宰，包括那些你现在还想不到的市场。

学界已经为分析算法打好了基础。现在至少有50套不同的深度学习工具，大部分都是开源的。过去五六年，很多创业公司都想利用这些开源资源打造完美的AI平台。然而，市场的主导权仍然掌握在少数巨头手里面。这个事实很可能表明，开发独立大平台的机会已经过去了，顶多也就是能开发小平台，之后也会被收购。

例如，位于加州的初创公司Ersatz Labs，投入了很多资源开发商用深度学习AI平台。去年，公司融资未果，CEO Dave Sullivan讲述了如今销售让人使用深度学习的产品或服务的难处。这些产品或服务的目标用户，很多都在大公司工作，而他们更愿意使用自己的工具，或者在内部招人。

“现在人人都在等着下一个杀手级深度学习应用，还没有人知道是什么，”Sullivan说，“但不会是平台。”

成为云服务市场的主宰

对亚马逊、微软和谷歌而言，这事关云服务用户的竞争。这三家公司都想在云市场赢得巨大的份额，但谷歌却远远落后一大截。

Forrester Research前不久发表数据称，今年，亚马逊的云利润大约108亿美元，微软101亿美元左右，而谷歌只有39亿美元。这促成了史上最大的深度学习大放送。

根据《华尔街日报》今年7月20日的报道，谷歌宣布将TensorFlow的语义分析和语音转换文本的两大库开源。语音转文字、翻译和解释（语义分析）都是技术老大难，大型B2C公司都会遇得到。谷歌举例说，假设一家公司分析了超过20亿分钟的客服通话录音，一种情况是系统理解了顾客的需求，为顾客提供了满意的服务，另一种是系统没有理解，当然也就提供不了服务，这两种情形对比，所花费的成本和得到的收益，差距是巨大的。

因此，谷歌云服务的竞争力是人工智能，强调人工智能也将是谷歌推广云服务时市场营销的重点。

免费可能是头一遭，但在云服务里竞争人工智能却是由来已久。亚马逊、IBM和微软都提供类似的AI服务。谷歌的机器学习产品“很不错，也终于以一种开发商真正想要的方式被包装起来，”Forrester Research的首席分析师John Rymer说：“但他们并不是独一家……而且亚马逊和微软遥遥领先。”

谷歌（还有他的竞争对手）云服务的收费标准是按次数计算，顾客每请求使用一次就会征收多少钱。几个月前发布的谷歌图像识别功能（不是免费的），哪怕只有一两个客户，但这些客户都是大客户，使用量都是上万亿次的，最终收入也是相当可观的。

吸引人才、提高声望、加速创新

数据科学家的数量算少，而深度学习的专家更是少得可怜。对于大公司而言，开源能够帮助他们招聘更多的顶级AI人才。就跟收购IP一样，人才资源稀缺也是深度学习领域融资并购的一大推力，收购初创公司，就意味着增加了有经验的员工。（有意思的是苹果，在几乎巨头都纷纷开源的浪潮中，仍然坚守代码的所有权。目前还不清楚苹果能撑多久。）

开源不仅能吸引学界和产业界的优秀研究人员和开发人员，也能吸引产生创新的个体。许多世界顶级的人工智能专家都来自学术界，研究人员也是开源软件的活跃用户。Brandon Ballinger以前是谷歌的工程师，现在他与加州大学旧金山分校合作研究心脏病学。Brandon Ballinger说：“如果你守着不开，像苹果那样，你根本不会吸引最优秀的人才。”

除此之外，还有实际的问题，不管你规模有

多大，你的研发预算也是有限度的。IBM 研发副总裁Rob Thomas 说：“关键是速度和创新。现在，我的‘研发’受研发预算的控制，除非我们是在开源做的项目。”

如果你的平台被Apache Institute作为新的开源项目收归旗下，你就能获得很高的信誉和很多的用户，由此创新的速度也更快。

能建立最强大硬件的公司，跑在最前面

不是有意贬低要在分布式系统上面运行100多层神经网络的能力，但深度学习剩下的问题还是在硬件方面。而说到硬件，又有谁比亚马逊、微软、谷歌和IBM在他们的云服务数据中心上面投资更多的呢？

有多大？IBM的Watson使用了90台IBM Power 750服务器，每台服务器含有一个3.5GHz的POWER7八核处理器，每个核有4个线程。加一来，系统一共拥有2880个POWER7处理器线程，内存为16TB。

IBM的研究员John Rennie介绍，Watson每秒可以处理数据500GB，相当于一万本图书。如果你认为这很厉害，那么Watson的性能实际上，还不到Top 500超级计算机的一半。

为当今的云服务数据中心优化AI，需要注重在处理器中不常见的芯片类型，特别是GPU和FPGA。当前的数据中心没有那么多GPU或FPGA，但需要处理的数据量又这么大。怎么办呢？英特尔就发现了机会。去年夏天，英特尔用167亿美元收购了FPGA制造商Altera，很明显是标识出市场的新方向。

深度学习初创公司Skymind首席研究员Adam Gibson说，深度学习已经成了“硬件问题”。是的，我们仍然需要顶尖的研究人员来指导神经网络的建立，但越来越多的时候，寻求更强大的硬件成了一种粗暴简单的解决方式。Gibson说，深度神经网络工作非常出色，但我们并不理解原理，因此，诀窍在于找到最好的算法组合。而更多更好的硬件能缩短寻找的时间。

最终的结果是，能够建立最强大的硬件网络的公司跑在最前面。几乎可以肯定，领跑的将是谷歌、亚马逊、微软和其他极少数公司。

没有OpenAI，就没有Open AI

这一点挺有意思。如果没有特斯拉的创始人Elon Musk和其他一大串鼎鼎有名的科技明星，这股开源运动或许还真流行不起来。

2015年底，上面那批人宣布成立初创公司OpenAI，而且是一家非营利性人工智能公司。

OpenAI 迅速从巨头、初创企业和学术界笼络了一批顶尖AI开发人员和研究人才，在很短时间内树立起了地位。Greg Brockman 以前是初创公司Stripe 的首席技术官，现在是 OpenAI 的一位负责人。他在最近的博客文章里写道，“我们的目标是推动数字智能，造福整个人类，不受财务回报约束”。

除了Musk 和Thiel，OpenAI的其他支持者包括“PC之父”Alan Kay、深度学习先驱Yoshua Bengio。OpenAI表示这些支持者已经承诺，要投资10亿美元到项目中。

就个人而言，我打赌这些非常聪明的技术人员肯定知道好好利用这些投资。如果没有OpenAI，巨头还会急不可耐地开源吗？

接下来……

除了上面提出的问题，还有一些值得思考。其中，最主要的一个或许是为什么深度学习平台能够脱颖而出？是技术好、容易使用，还是跟硬件有关呢？这得留到下次再说了。

总之，2016年感觉越来越像2007年，那时候Hadoop第一次开源，商业应用如何火箭升空，一发而不可收拾。

（来源：新智元）

中共中央办公厅、国务院办公厅印发《关于进一步完善中央财政科研项目资金管理等政策的若干意见》

近日，中共中央办公厅、国务院办公厅印发了《关于进一步完善中央财政科研项目资金管理等政策的若干意见》，并发出通知，要求各地区各部门结合实际认真贯彻落实。

《关于进一步完善中央财政科研项目资金管理等政策的若干意见》全文如下：

《中共中央、国务院关于深化体制机制改革加快实施创新驱动发展战略的若干意见》和《国务院关于改进加强中央财政科研项目和资金管理的若干意见》印发以来，有力激发了创新创造活力，促进了科技事业发展，但也存在一些改革措施落实不到位、科研项目资金管理不够完善等问题。为贯彻落实中央关于深化改革创新、形成充满活力的科技管理和运行机制的要求，进一步完善中央财政科研项目资金管理等政策，现提出以下意见。

一、总体要求

全面贯彻落实党的十八大和十八届三中、四中、五中全会及全国科技创新大会精神，以邓小平理论、“三个代表”重要思想、科学发展观为指导，深入学习贯彻习近平总书记系列重要讲话精神，按照党中央、国务院决策部署，牢固树立和贯彻落实创新、协调、绿色、开放、共享的发展理念，深入实施创新驱动发展战略，促进大众创业、万众创新，进一步推进简政放权、放管结合、优化服务，改革和创新科研经费使用和管理方式，促进形成充满活力的科技管理和运行机制，以深化改革更好激发广大科研人员积极性。

——坚持以人为本。以调动科研人员积极性和创造性为出发点和落脚点，强化激励机制，加大激励力度，激发创新创造活力。

——坚持遵循规律。按照科研活动规律和财政预算管理要求，完善管理政策，优化管理流程，改进管理方式，适应科研活动实际需要。

——坚持“放管服”结合。进一步简政放权、放管结合、优化服务，扩大高校、科研院所在科研项目资金、差旅会议、基本建设、科研仪器设备采购等方面的管理权限，为科研人员潜心研究营造良好环境。同时，加强事中事后监管，严肃查处违法违纪问题。

——坚持政策落实落地。细化实化政策规定，加强督查，狠抓落实，打通政策执行中的“堵点”，增强科研人员改革的成就感和获得感。

二、改进中央财政科研项目资金管理

（一）简化预算编制，下放预算调剂权限。根据科研活动规律和特点，改进预算编制方法，实行部门预算批复前项目资金预拨制度，保证科研人员及时使用项目资金。下放预算调剂权限，在项目总预算不变的情况下，将直接费用中的材

料费、测试化验加工费、燃料动力费、出版/文献/信息传播/知识产权事务费及其他支出预算调剂权下放给项目承担单位。简化预算编制科目，合并会议费、差旅费、国际合作与交流费科目，由科研人员结合科研活动实际需要编制预算并按规定统筹安排使用，其中不超过直接费用10%的，不需要提供预算测算依据。

（二）提高间接费用比重，加大绩效激励力度。中央财政科技计划(专项、基金等)中实行公开竞争方式的研发类项目，均要设立间接费用，核定比例可以提高到不超过直接费用扣除设备购置费的一定比例：500万元以下的部分为20%，500万元至1000万元的部分为15%，1000万元以上的部分为13%。加大对科研人员的激励力度，取消绩效支出比例限制。项目承担单位在统筹安排间接费用时，要处理好合理分摊间接成本和对科研人员激励的关系，绩效支出安排与科研人员在项目工作中的实际贡献挂钩。

（三）明确劳务费开支范围，不设比例限制。参与项目研究的研究生、博士后、访问学者以及项目聘用的研究人员、科研辅助人员等，均可开支劳务费。项目聘用人员的劳务费开支标准，参照当地科学研究和技术服务业从业人员平均工资水平，根据其在项目研究中承担的工作任务确定，其社会保险补助纳入劳务费科目列支。劳务费预算不设比例限制，由项目承担单位和科研人员据实编制。

（四）改进结转结余资金留用处理方式。项目实施期间，年度剩余资金可结转下一年度继续使用。项目完成任务目标并通过验收后，结余资金按规定留归项目承担单位使用，在2年内由项目承担单位统筹安排用于科研活动的直接支出；2年后未使用完的，按规定收回。

（五）自主规范管理横向经费。项目承担单位以市场委托方式取得的横向经费，纳入单位财务统一管理，由项目承担单位按照委托方要求或合同约定管理使用。

三、完善中央高校、科研院所差旅会议管理

（一）改进中央高校、科研院所教学科研人员差旅费管理。中央高校、科研院所可根据教学、科研、管理工作实际需要，按照精简高效、厉行节约的原则，研究制定差旅费管理办法，合理确定教学科研人员乘坐交通工具等级和住宿费标准。对于难以取得住宿费发票的，中央高校、科研院所在确保真实性的前提下，据实报销城市间交通费，并按规定标准发放伙食补助费和市内交通费。

（二）完善中央高校、科研院所会议管理。中央高校、科研院所因教学、科研需要举办的业务性会议(如学术会议、研讨会、评审会、座谈会、答辩会等)，会议次数、天数、人数以及会议费开支范围、标准等，由中央高校、科研院所按照实事求是、精简高效、厉行节约的原则确定。会议代表参加会议所发生的城市间交通费，原则上按差旅费管理规定由所在单位报销;因工作需要，邀请国内外专家、学者和有关人员参加会议，对确需负担的城市间交通费、国际旅费，可由主办单位在会议费等费用中报销。

四、完善中央高校、科研院所科研仪器设备采购管理

（一）改进中央高校、科研院所政府采购管理。中央高校、科研院所可自行采购科研仪器设备，自行选择科研仪器设备评审专家。财政部要简化政府采购项目预算调剂和变更政府采购方式审批流程。中央高校、科研院所要切实做好设备采购的监督管理，做到全程公开、透明、可追溯。

（二）优化进口仪器设备采购服务。对中央高校、科研院所采购进口仪器设备实行备案制管理。继续落实进口科研教学用品免税政策。

五、完善中央高校、科研院所基本建设项目管理

（一）扩大中央高校、科研院所基本建设项目管理权限。对中央高校、科研院所利用自有资金、不申请政府投资建设的项目，由中央高校、科研院所自主决策，报主管部门备案，不再进行审批。国家发展改革委和中央高校、科研院所主管部门要加强对中央高校、科研院所基本建设项目的指导和监督检查。

（二）简化中央高校、科研院所基本建设项目审批程序。中央高校、科研院所主管部门要指导中央高校、科研院所编制五年建设规划，对列入规划的基本建设项目不再审批项目建议书。简化中央高校、科研院所基本建设项目城乡规划、用地以及环评、能评等审批手续，缩短审批周期。

六、规范管理，改进服务

（一）强化法人责任，规范资金管理。项目承担单位要认真落实国家有关政策规定，按照权责一致的要求，强化自我约束和自我规范，确保接得住、管得好。制定内部管理办法，落实项目预算调剂、间接费用统筹使用、劳务费分配管理、结余资金使用等管理权限;加强预算审核把关，规范财务支出行为，完善内部风险防控机制，强化资金使用绩效评价，保障资金使用安全规范有效;实行内部公开制度，主动公开项目预算、预算调剂、资金使用(重点是间接费用、外拨资金、结余资金使用)、研究成果等情况。

（二）加强统筹协调，精简检查评审。科技部、项目主管部门、财政部要加强对科研项目资金监督的制度规范、年度计划、结果运用等的统筹协调，建立职责明确、分工负责的协同工作机制。科技部、项目主管部门要加快清理规范委托中介机构对科研项目开展的各种检查评审，加强对前期已经开展相关检查结果的使用，推进检查结果共享，减少检查数量，改进检查方式，避免重复检查、多头检查、过度检查。

（三）创新服务方式，让科研人员潜心从事科学研究。项目承担单位要建立健全科研财务助理制度，为科研人员在项目预算编制和调剂、经费支出、财务决算和验收等方面提供专业化服务，科研财务助理所需费用可由项目承担单位根据情况通过科研项目资金等渠道解决。充分利用信息化手段，建立健全单位内部科研、财务部门和项目负责人共享的信息平台，提高科研管理效率和便利化程度。制定符合科研实际需要的内部报销规定，切实解决野外考察、心理测试等科研活动中无法取得发票或财政性票据，以及邀请外国专家来华参加学术交流发生费用等的报销问题。

七、加强制度建设和工作督查，确保政策措施落地见效

（一）尽快出台操作性强的实施细则。项目主管部门要完善预算编制指南，指导项目承担单位和科研人员科学合理编制项目预算;制定预算评估评审工作细则，优化评估程序和方法，规范评估行为，建立健全与项目申请者及时沟通反馈机制;制定财务验收工作细则，规范委托中介机构开展的财务检查。2016年9月1日前，中央高校、科研院所要制定出台差旅费、会议费内部管理办法，其主管部门要加强工作指导和统筹;2016年年底前，项目主管部门要制定出台相关实施细则，项目承担单位要制定或修订科研项目资金内部管理办法和报销规定。以后年度承担科研项目的单位要于当年制定出台相关管理办法和规定。

（二）加强对政策措施落实情况的督查指导。财政部、科技部要适时组织开展对项目承担单位科研项目资金等管理权限落实、内部管理办

法制定、创新服务方式、内控机制建设、相关事项内部公开等情况的督查，对督查情况以适当方式进行通报，并将督查结果纳入信用管理，与间接费用核定、结余资金留用等挂钩。审计机关要依法开展对政策措施落实情况和财政资金的审计监督。项目主管部门要督促指导所属单位完善内部管理，确保国家政策规定落到实处。

财政部、中央级社科类科研项目主管部门要结合社会科学研究的规律和特点，参照本意见尽快修订中央级社科类科研项目资金管理办法。

各地区要参照本意见精神，结合实际，加快推进科研项目资金管理改革等各项工作。

（来源：中国科协）

万钢：加快创新驱动发展 建设世界科技强国

7月22日上午，全国政协副主席、中国科协主席、科技部部长万钢在中国科协与中央党校联合举办的“高层次科技领军人才专题研修班”上作题为《加快创新驱动发展 建设世界科技强国》的专题辅导报告。报告围绕学习贯彻习近平总书记系列重要讲话，特别是在“科技三会”上的重要讲话精神，结合“十三五”科技创新规划的制订和实施，系统介绍我国创新驱动的新形势、科技改革的新进展和科技创新的新部署。中国科协党组书记、常务副主席、书记处第一书记尚勇主持报告会。

万钢指出，党的十八大以来，习近平总书记高度重视科技创新，对科技创新做出一系列重要论述，提出一系列新思想、新论断和新要求，站在新的历史起点上吹响了建设世界科技强国的号角，迎来了我国科技创新的又一个春天。

万钢回顾了“十二五”期间我国科技改革和发展取得的新成就，指出当前新一轮的科技革命和产业变革正在孕育兴起，我国正处于跨越“中等收入陷阱”的紧要关头，创新驱动是大势所趋、国运所系，必须紧紧依靠科技创新打造发展新引擎。科技创新要和体制机制创新一起，实现双轮驱动。

万钢指出，“十三五”科技创新规划紧紧围绕经济竞争力提升的核心关键、社会发展的紧迫需求、国家安全的重大挑战，采取差异化策略和非对称路径，强化重点领域和关键环节的任务部署，重点从六个方面加强系统部署和谋划。一是构筑国家先发优势，重点实施重大专项，启动“科技创新2030—重大项目”。二是提升原始创新能力，加大基础研究，加快设施建设，大力培养和引进创新型人才。三是拓展创新发展空间，打造区域创新高地、“一带一路”协同创新共同体，全方位融入和布局全球创新网络。四是推动“双创”有效服务实体经济，大力发展科技服务业，打造“新创天地”，引导社会资金投入创新创业。五是构建激励创新的体制机制，建立完成

科技成果转化的收益分配机制，加快政府职能从研发管理向创新服务转变。六是加强科学普及和创新文化建设，全面提升公民的科学素质，营造激励创新的社会文化氛围。

万钢强调，中国科协要深入贯彻落实习总书记关于科协工作的指示要求，切实履行好为科技工作者服务，为创新驱动发展服务，为提高全民科学素质服务，为党和政府科学决策服务的职责定位，全面推进开放性、枢纽型、平台型组织建设，团结带领广大科技工作者为决胜全面建成小康社会攻坚克难、创新争先，为建设世界科技强国、实现中华民族伟大复兴的中国梦作出更大的贡献！

尚勇在主持中表示，万钢主席的报告，紧密结合我国科技创新实践，深入诠释了习近平总书记科技创新思想，深入浅出地论述了当今国内外科技创新的新趋势、新特点、新规律，对系统把握“十三五”科技发展的战略重点、明确努力方向具有重要的指导意义。希望大家认真学习、深刻领会报告内容，坚定创新赶超跨越的决心，立足岗位、创新争先，努力为国家创新发展和中华民族伟大复兴作出更大贡献。

研修班期间，中央党校原副校长李君如作了题为《不忘初心，继续前进》专题辅导报告，详细解读了习近平总书记的“七一”讲话。他重点回顾了党的历史上几次重要的“七一”讲话，深入解读了中国共产党走过的95年光辉历程，系统地回答了“不忘初心、继续前进”，必须紧紧依靠人民群众这个基本问题，全面阐述了“不忘初心、继续前进”的八个基本要求。他认为，习近平总书记的“七一”讲话思想深刻、内在逻辑紧密、针对性强，是当前和今后一个时期我们坚持和发展中国特色社会主义、全面建成小康社会、实现“两个一百年”奋斗目标和中华民族伟大复兴中国梦的纲领性文献。

国家发改委副主任林念修作了题为《深入学习领会习近平总书记重要讲话精神 全力推动我国经济实现创新驱动发展》的辅导报告。他从对推进创新驱动发展的认识、我国创新驱动发展取得明显进展、清醒认识制约创新驱动发展短板、以新思维推进落实创新驱动发展战略、当前发改委推进创新驱动发展的重点工作等五个方面，深刻分析经济新常态的新特点、新挑战，全面阐述了创新驱动发展的重要意义，以及推动我国经济实现创新驱动发展的关键要素。

来自高校、科研院所和企业的高层次科技人才，以及全国学会理事长、千人计划专家等230多名领军人才参加本次研修班。

（来源：中国科协）

首届中国创新创业大赛机器人创客大赛通知

根据科技部国科发火〔2016〕106 号文，中国创新创业大赛机器人创客大赛在安徽合肥举办。为聚集和整合全国机器人领域创新创业资源，布局机器人产业 2.0 时代，推动《中国制造 2025》实施促进机器人与制造产业升级，深化供给侧结构性改革，将举办“中国创新创业大赛机器人创客大赛”。

（详情请登录学会官网：www.caa.org.cn）

中国自动化学会通讯 第37卷 第4期 总第187期 2016年8月

IEEE服务运筹、物流与信息化、汽车电子与安全、综合可持续交通系统三大国际会议在京成功举办

2016年7月10日—12日，由中国科学院自动化研究所复杂系统管理与控制国家重点实验室和中国自动化学会联合承办的IEEE/INFORMS服务运筹、物流与信息化国际会议(SOLI 2016)、IEEE汽车电子与安全国际会议(ICVES 2016)、IEEE综合可持续交通系统论坛(FISTS 2016)三大国际会议同期在北京友谊宾馆隆重召开。

本次会议吸引了来自中国、美国、英国、德国、芬兰、奥地利、荷兰、日本、新加坡等多个国家和地区的专家、学者百余人参加。在为期三天的会议里，会议方共安排了7场大会主题报告、3个专题分会场、41场论文报告以及37个海报展示。会议议题集中反映了服务运筹、物流与信息化、汽车电子与安全以及交通综合可持续发展领域内的主要学术成就，当前关注的核心问题，以及未来新的发展方向。来自世界各地的专家、学者和科技人员汇聚一堂，针对各自领域的相关问题畅所欲言，积极讨论，气氛热烈。

7月11日上午，复杂系统管理与控制国家重点实验室主任王飞跃研究员主持了大会开幕式并致欢迎辞。奥地利替代推进系统协会高级技术顾问Reinhard Pfliegl教授作了题为“Introduction of Automated Vehicle on Roads - Impact to Society and Technology”的大会报告，美国密歇根大学Henry Liu教授作了题为“Next Generation Traffic Control with Connected and Automated Vehicles”的大会报告，清华大学李力副教授作了题为“Intelligence Testing for Autonomous Vehicles: A New Approach”的大会报告，中国科学院自动化研究所袁勇副

王飞跃教授主持开幕式

Reinhard Pfliegl教授作报告

Henry Liu教授作报告

李力副教授作报告


袁勇副研究员作报告

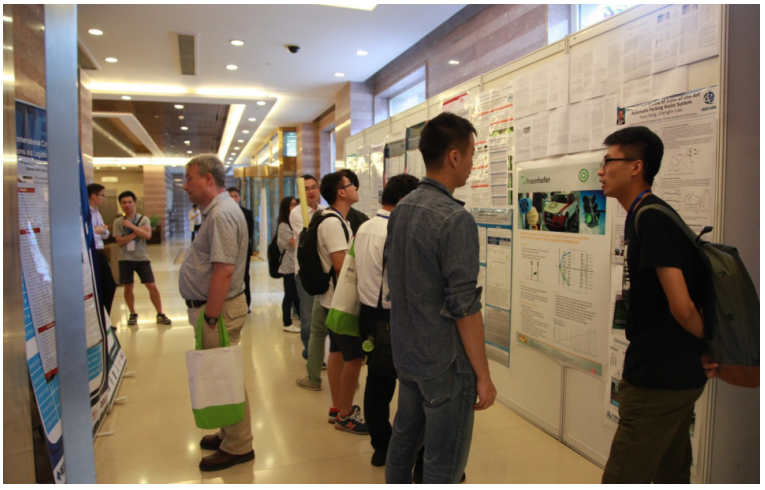

曹东璞副教授作报告


杨柳青教授作报告


张晓东教授作报告

研究员作了题为“Transportation 5.0: Five Transportations in One and Blockchain-based ITS”的大会报告。

7月12日上午，英国克兰菲尔德大学曹东璞副教授作了题为“Collaborative Decision Making in Automated Vehicles towards Parallel Driving”的大会报告，美国科罗拉多州立大学杨柳青教授作了题为“ACP-Based Self-Driving Vehicles”的大会报告，北京交通大学张晓东教授作了题为“Parallel Logistics Systems: ACP based Analysis and Management for China's Integrated Logistics Operations”的大会报告。



IEEE/INFORMS服务运筹、物流与信息化国际会议是服务科学领域的重要学术年会，旨在汇集研究人员和从业者探讨相关问题，明确所面临的挑战和未来的发展方向，交流彼此在服务设计、创新、市场营销、运筹等领域的科研成果和经验。SOLI 2016收到了来自国内外涉及服务运作、服务创新、物流和供应链、服务营销、服务管理等众多方面的论文投稿，研究内容覆盖了日益发展的服务科学与技术的整个领域，反映了国内外在该领域所取得的最新研究成果。

IEEE汽车电子与安全国际会议和IEEE综合可持续交通系统论坛由IEEE智能交通系统协会（ITSS）发起主办，旨在汇集智能车辆和综合交通系统等领域的专家和学者，交流和探讨汽车电子和安全、综合交通系统方面的研究成果和新发现。ICVES 2016和FISTS 2016收到了来自国内外涉及车辆检测技术、信号处理、微机电系统、汽车/发动机控制、车辆总线、驾驶员辅助驾驶系统、传感网络、自适应巡航控制系统、水上运输、能源管理等众多方面的论文投稿，研究内容覆盖了日益发展的信息技术与智能技术在车辆和交通运输的应用研究，反映了国内外在该领域所取得的最新研究成果。

本次IEEE系列国际会议的成功举办，不仅增进了国内外学术界相关领域专家、学者的彼此了解，还为物流服务、汽车电子与安全以及综合交通运输的研究提供了新的方向。同时也开阔了广大青年学者的学术视野，进一步加强中国与其他国家和地区的合作与研究，对扩大我国在这些领域内的国际影响起到了重要的推动作用。

中国工程院、科技部人机混合智能发展战略研讨会在京举行

8月20日，由中国工程院、科技部部署主办的第三次人机混合智能发展战略研讨会、首次人机混合平行智能研讨会暨中国自动化学会人机混合平行智能专业委员会筹备会在北京中国科学院自动化研究所举行，会议由郑南宁院士与王飞跃研究员共同主持。“人机混合智能”是“中国人工智能2.0发展战略研究”重大咨询项目的六个方向之一，郑院士主持该方向的咨询与论证工作。此次会议重点研讨未来人机混合智能所面临的挑战性问题、预期理论突破与重大创新应用。来自西安、杭州、上海、深圳、长沙、福州、成都、青岛、兰州、澳门等十余所高校、企业及科研单位的50多名专家及科研人员参加了会议并进行了热烈讨论。

郑南宁院士作题为“《人工智能2.0》方向四：人机协同的混合智能”主题报告

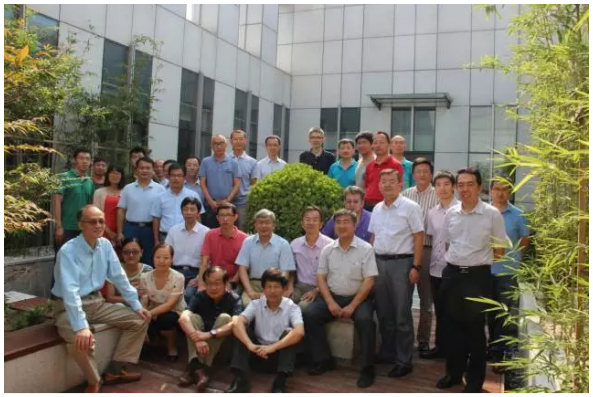
会议首先由郑南宁院士介绍“中国人工智能2.0发展战略研究”及其主要研究目标、任务以及任务基本特征。郑院士指出，当前国家对于人工智能领域的投入已高达160亿，如何超越传统人工智能理论框架，实现自主学习与更加健壮的人工智能（即人工智能2.0）是此次会议要探讨的主要问题。围绕“人机混合智能的目标与任务”“人机混合智能的重大应用”和“人机混合智能的科学问题与研究内容”，郑院士指出，人工智能2.0，不仅要实现AI对于知识的学习，而且要实现AI对于学习过程的学习、分析与反馈。

王飞跃研究员与郑南宁院士共同主持会议

随后，各位与会专家分别围绕“脑机交互智能”“人的智能、机器的智能以及人机混合的智能”“智能驾驶中的人机混合智能”“人机混合交互过程中的编码”“人机混合智能中人与机器的分工界限”“智能信息的粒度”，以及核电、医学、智能设备中的人机混合智能应用等多个主题进行了深入探讨。与会专家一致表示，要突破传统人工智能问题、框架以及应用的限制，积极探索并扩展人工智能的应用场景，更好地发挥技术对社会生产力的推动作用。

会上，中科院自动化所王飞跃研究员介绍了“人机混合平行智能研讨会”和中国自动化学会“人机混合平行智能专业委员会”的筹备工作，得到了与会专家的积极响应及热情参与。

经过多次激烈讨论与协商，参会的各位专



与会专家合影

与会专家紧围绕“人机混合智能所面临的挑战性问题、预期理论突破与重大创新应用”展开讨论

家最终达成一致，围绕“城市智能”“智慧农业”“智慧医健”“智慧经济与社会”“智慧物流”“智慧教育”“人机路的协同”等七个CPSS人机一体化混合智能主要场景，借助人工智能2.0，考虑人在系统之内的不确定性因素，对之前阶段无法还原、无法理清、无序、无法度量的复杂系统问题进行更深层次的探索。

会议的最后，郑南宁院士对此次的讨论进行了总结与展望。郑院士指出，在各位专家的共同努力下，这次的会议是非常成功、富有成效的。但距离重大咨询项目的最终目标，还有一些差距，需要各位专家在本次会议的基础上，进一步凝练“人机混合智能”的重要问题及应用场景与目标，形成有效的行动指南与发展规划。郑院士同时指出，“人机混合智能战略研讨会”是开放的、交互的、不断深入探讨并发展壮大的，希望各位专家协同努力，共同建设并引导“人机混合智能”新场景。

京津冀智能电气设计人才培养师资培训

2016年7月29日—30日，由中国自动化学会分布式能源专业委员会、诺信产教集团、法国Trace Software集团联合、河北科技大学理工学院共同举办的“京津冀智能电气设计人才培养暑期师资培训班”圆满结束。学员分别来自河北科技大学、石家庄铁道大学、天津科技大学、太原工业学院、太原理工大学等高校，以及中国兵工集团河北太行机械等企业代表共计50多名。工业和信息化部人才交流中心推广部执行主任王济胜、法国逸莱轲软件贸易中国公司总经理、中国自动化学会智能分布式能源专业委员会委员王瑞、诺信产教集团董事长穆海新、河北科技大学理工学院常务副院长刘朝英等一同出席开班仪式。

此次培训班的开办，是为了积极响应中央“中国制造2025”“京津冀一体化”的号召，随着近几年智能制造业信息化的飞速发展，智能制造业将逐步成为国家重要战略，政策的提出为京津冀智能制造人才的培养指出了方向，同时也为智能制造人才带来了机遇和挑战。为此，辅助院校深入开展智能电气设计的人才培养工作，支撑院校教学改革和专业建设，提升专业教师授课水平，已成为迫在眉睫的任务。

通过结合企业实际案例的培训，具体问题具体分析，学员很快掌握了使用elecworks软件智能

电气工程设计方法，并深入了解与传统电气设计的区别。另外，通过学习一些实际项目先进的设计流程和经验，暑期培训结束后学员将会具备有标准化和高效化的设计能力。

随着政策的导向和智能制造业的深入、全面的发展，制造业专业人才也将迎来多重机遇和压力，因此国内高校对电气设计课程与实践结合愈加重视，更加关注校企合作，注重对企业一线需求人才的培养。通过校企合作的形式，联合优质企业资源，在高校开展以项目为基础的设计培训班，对教师的教学深度有了进一步帮助，为培养应用型专业技术人才提供理论支持和技术保障。也为分布式能源的未来迅速、全面发展的打下了坚实的人才基础。

Trace Software International成立于1987年，具有28年电气CAD/CAE解决方案的开发和服务经验（1987年—2016年）。公司合作伙伴遍布全球（包括Autodesk, Dassault Systèmes，RS Component），所提供的解决方案涵盖了工业自动化电气设计，低压/高压电气系统计算，太阳能光伏计算等领域，中国子公司逸莱轲软件贸易（上海）有限公司总经理王瑞是中国自动化学会智能分布式能源专业委员会委员。

（智能分布式能源专委会 供稿）

关于举办2016国家智能制造论坛的通知

在新常态的经济环境下，工业领域的结构演变和调整正成为新的经济增长动力，特别是在《中国制造2025》正式发布以后，智能制造成为了我国制造业未来发展的主攻方向。推进《中国制造2025》是深化结构性改革，尤其是供给侧结构性改革、发展新经济、加快中国制造提质增效的重要举措。智能制造是实现中国制造业由大变强的基础，也是落实《中国制造2025》的关键，尽管，目前中国企业在实现智能制造的道路上,还存在着技术、人才、工业基础等诸多的难题，但是，智能制造趋势不可阻挡,自动化、数字化、网络化、绿色环保的制造模式将是未来的发展方向。为推动中国工业产业转型升级,提升制造业水平,服务地方经济发展，中国自动化学会、宁波市委人才办、宁波市科学技术协会及宁波市江北区人民政府主办的2016国家智能制造论坛定于9月26日-9月28日在宁波举行。

（详情请登录学会官方网站：www.caa.org.cn）

2016全国第二十一届自动化应用技术学术交流会在东北大学圆满召开

2016年8月19—20日，由中国自动化学会应用专业委员会、中国金属学会冶金自动化分会、东北大学轧制技术及连轧自动化国家重点实验室和钢铁共性技术协同创新中心联合主办，冶金自动化研究设计院、东北大学信息科学与工程学院、鞍钢集团信息产业有限公司、上海宝信软件股份有限公司、山信软件股份有限公司、中国瑞林工程技术有限公司、北京首钢自动化信息技术有限公司、北华大学、北京信息科技大学和混合流程工业自动化系统及装备技术国家重点实验室联合协办的2016年全国第二十一届自动化应用技术学术交流会在东北大学国际学术交流中心召开。

冶金自动化研究设计院副院长、中国自动化学会副秘书长，中国自动化学会应用专业委员会秘书长、中国金属学会常务理事、中国金属学会冶金自动化分会秘书长孙彦广主持了大会开幕式，东北大学校长赵继致欢迎辞，中国自动化学会常务理事王成红、中国金属学会副秘书长高怀、东北大学轧制技术及连轧自动化国家重点实验室主任王昭东出席了大会并致辞。

此次大会以“面向中国制造2025的智能工厂共性技术与应用”为主题，在中国制造2025战略出台的大背景下，从智能设计、智能生产、智能管理、智能制造等关键环节为切入点，深入探寻智能制造技术的发展趋势及实施路径。大会由主会场、两个分会场、技术交流论坛和参观环节组成，

特邀专家报告二十余篇，其中中国工程院院士报告三篇，汇集了来自各个高校、企业、科研院所从事自动化、信息化技术研发和应用工作的专家、学者、科技人员、管理人员、高校师生等两百余人。

主会场会上，中国工程院院士、东北大学教授王国栋作了题为《钢铁工业的绿色智能制造》的报告；中国工程院院士、中科院沈阳自动化研究所研究员王天然作了题为《机器人助力中国制造》的报告；中国工程院院士、华东理工大学副校长钱锋作了题为《“互联网+”时代原材料工业智能优化制造》的报告；中国机械工业联合会专家委员会名誉主任朱森第作了题为《智能制造——〈中国制造2025〉的主攻方向》的报告；冶金自动化研究设计院副院长孙彦广作了题为《欧盟RFCS项目与钢铁集成智能制造》的报告；上海宝信软件股份有限公司资深技术总监吴毅平作了题为《工业4.0背景下,钢铁企业智能制造和技术方案》的报告；鞍钢集团矿业有限公司信息中心经理王欢作了题为《冶金矿山智能生产新模式》的报告。

钢铁工业和非钢铁工业智能工厂共性技术与应用两个分会场上，东北大学教授张殿华、宝钢集团中央研究院首席研究员郭朝晖、北京科技大学工程技术研究院院长何安瑞等16位专家学者作了相关的精彩报告。

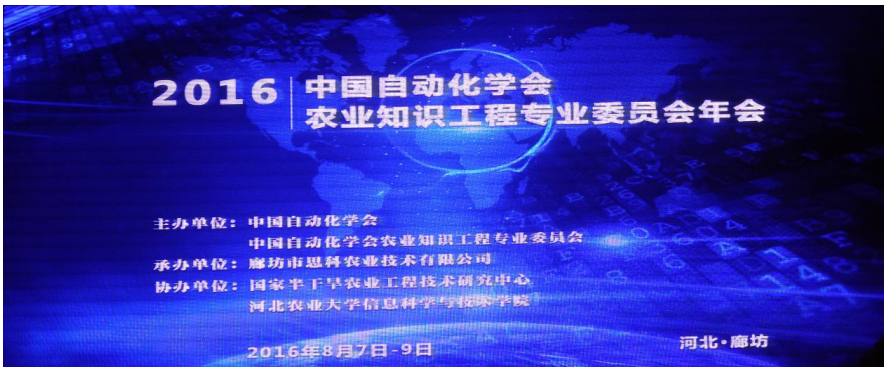
为了便于与会代表进行更加充分和深入的技术交流，大会还特别设立了技术交流论坛。中国工程院院士王国栋、中国工程院院士钱锋、冶金自动化研究设计院副院长孙彦广、宝钢研究院自动化所首席研究员杜斌等多位专家为与会代表就大会报告及自选问题进行了答疑互动，行业专家们的精彩解答令与会代表受到极大启发。最后，大会安排与会代表们参观了东北大学校史馆和东北大学轧制技术及连轧自动化国家重点实验室。

一篇篇精彩纷呈、智者见“智”的报告，一次次答疑交流中思想的对接与碰撞，使与会者对智能制造的科学范畴有了较深的理解，并对在目前中国制造业的现状下如何统筹地逐步实现智能制造有了相关认识。会议主题突出、契合实际，报告水平先进、内容丰富，会议形式多样、设主分会场，参观实验室、学术气氛浓厚，交流答疑深入，因此会议取得了圆满成功，相信必将对企业自动化、信息化新技术的推广应用起到积极的促进作用。

大会同期还召开了中国金属学会自动化分会、中国自动化学会应用专业委员会工作会议。工作会由秘书长孙彦广主持，副秘书长李亚丽向各位委员汇报了2015年学会工作总结，通报了中国金属学会自动化分会第七届委员会换届工作情况。武汉科技大学信息科学与工程学院院长王斌汇报了下届学术大会的承办方案。委员们对学会工作表示了充分的肯定，并就今后的发展愿景提出了希望和建议。

（应用专业委员会 供稿）

2016年全国智能工程与农业信息化学术会议在廊坊成功召开



2016年8月7日—9日，由中国自动化学会与其农业知识工程专业委员会主办，廊坊市思科农业技术有限公司承办，国家半干旱农业工程技术研究中心和河北农业大学信息科学与技术学院协办的“2016年全国智能工程与农业信息化学术会议”，在河北省廊坊市顺利召开。

中国自动化学会农业知识工程专业委员会主任、国际自动控制联合会IFAC Fellow、中国自动化学会会士熊范纶研究员，担任会议主席。晏国生、张友华分别担任组织、程序委员会主席。

中国工程院汪懋华院士，国家农业部信息中心杜维成副主任，原廊坊市政协主席薛伯昌，市委副秘书长崔万友，廊坊市科技局副局长董立峰，以及来自全国21个省（市、自治区）的57个农业院校、科研机构、政府部门和企业等单位的128位人工智能与农业信息化等领域的知名专家与学者出席了会议。

本次会议旨在探讨将智能技术、控制技术、信息技术等运用于农业、环境生态、生物处理等领域，形成相互交叉的新兴学科方向，并得到实际应用。会议收到论文60多篇，经组委会和相关专家认真讨论筛选，选择35篇论文汇聚成册，作为学术资料并在会议上交流。

熊范纶主任首先致开幕词。他阐述了本次会议的主题，并希望与会代表积极交流，增进友谊，加强协作，取得收获。原廊坊市政协主席薛

伯昌与半干旱农业工程技术中心高振峰主任分别致辞，对专家学者的到来表示欢迎。

在8月8日上午的主题报告会上，5位专家分别从国家战略、主管部门、学术研究、应用示范、智能与道德等层面作了精彩报告。中国农业大学汪懋华院士作了以《围绕国家十三五规划纲要，加快推动农业农村信息化创新发展》为题的报告，他指出，“十三五”是全面建成小康社会的决胜阶段，实现“四化”同步发展，农业是短腿、农村是短板，中央一号文件连续3年将农业现代化作为关键词写入文件标题，明确要求要加大改革创新力度，推动农业供给侧结构性改革，加快转变农业发展方式，走“产出高效、产品安全、资源节约、环境友好”的农业现代化道路。因此加快补齐农业现代化短板刻不容缓。国家农业部信息中心杜维成副主任作了题为《云服务及大数据的建设》的报告，他阐述了国家农业部信息中心的云服务及大数据建设的实施方案。中科院智能所熊范纶研究员作了题为《智能化：现代农业的重要发展方向》主题报告。他指出了当前农业信息化所面临问题，提出相应的意见和建议，并介绍了本专委会的宗旨和发展历程。河北省农林科学院李志宏研究员作了题为《智能农业应用发展的途径探讨》的报告，他从成本效益角度分享了他们所开展的工作。暨南大学孙东川教授作了题为《试论计算机的智能与道德——基于系统哲学的思考》的报告，从伦理道德角度提出，在智能技术研究过程中，需考虑防范意识。

在8月8日下午及9日上午举行的专题报告会上，有18位专家从云计算、大数据、物联网、图像处理、虚拟现实、地理信息系统、智能装备、传感器和电池研发等角度，分别介绍了他们的研究成果及应用情况，既有理论创新，又有实践检验，充分展现智能信息技术与农业的高度融合，使参会人员全面了解当前我国农业信息技术研究和应用现状，以便更好把握未来发展方向。

8月7日晚，还召开了本届专业委员会工作会议，会上分别就年会议程和增补委员等事宜进行了通报和协商。8日晚又召开了有新增补委员参加的工作会议，就专委会的发展及明年学术年会等问题进行了热烈讨论。

闭幕式上，农业知识工程专业委员会刘世洪副主任对本次会议作了全面总结，简要概括了本次会议的基本情况及特点，并向给予本次会议支持的相关单位及个人表示感谢。会议结束后，与会人员参观了廊坊大数据中心，了解廊坊各领域的信息化应用现状。

综上，在承办单位晏国生院长、刘君老师及专委会董俊常务副秘书长的辛勤努力下，2016年中国自动化学会农业知识工程专业委员会举办的学术年会，顺利完成各项会议议程，圆满完成各项任务，达到了预期目标。

（农业知识工程专委会 供稿）

2016中国自动化学会智能建筑与楼宇自动化专业委员会年会暨工作总结大会成功举行

党的十八届五中全会确立了创新、协调、绿色、开放、共享五大发展理念，其中绿色发展着重解决经济发展与环境保护协调问题，绿色建筑是这一发展的重要组成部分，中国自动化学会智能建筑与楼宇自动化专业委员会一直致力于推动中国智能建筑的创新发展，通过为企业搭建技术交流平台、为科研院所提供企业技术需求推广、为民众提供智能建筑科学普及，推动中国智能建筑与楼宇自动化行业的发展。

2016年7月30日下午1点30分，中国自动化学会智能建筑与楼宇自动化专业委员会在北京工业大学工大建国饭店三层大会议厅举办了专委会年会暨工作总结表彰大会。

本次年会参会嘉宾83人，参会企业41家，共得到四家企业的赞助支持：广东西奥物联网科技股份有限公司、锐捷网络股份有限公司、北京三永华通科技有限公司和深圳实达信息技术有限公司。

本次年会由专委会秘书长孙中华主持，专委会工作委员会主任郭维钧教授介绍了到会领导与新增专家情况；专委会主任贾克斌教授对2015年度专委会工作进行了总结，并介绍了下一年度即将展开的工作规划。中国自动化学会党支部书记吕爱英老师代表总会对大会的召开表示祝贺，并介绍了中国自动化学会对智能建筑与楼宇自动化专业委员会的工作肯定与新的期望。

本次大会设置了1个主题报告——“新型智慧城市顶层设计思考”，报告人为北京工业大学智慧城市研究院常务副院长林绍福教授；以及4个技术交流报告。本次大会同时举行了“智慧家居科普基地”授牌仪式，由中国自动化学会领导吕爱英书记向北京工业大学城市建设与规划学院院长戴俭教授颁发基地铭牌，该科普基地作为智能建筑的应用示范基地，为智能建筑和智慧家居专业知识推广提供了一个优质平台。

本次大会评选出2015年度专委会创新企业9家，评选出优秀会议论文10篇，发表在《电气&智能建筑》杂志2016年第7—8月刊上。

本次大会在领导和各参会嘉宾的大力支持下取得圆满成功，并于7月30日下午五点顺利闭幕。

（智能建筑与楼宇自动化专委会 供稿）

部分优秀论文作者合影

中国自动化学会党支部书记吕爱英为北京工业大学智慧家居科普教育基地授牌

第八届全国平行控制会议暨中国自动化学会平行控制与管理专业委员会2016年全体会议在北京举行

第八届全国平行控制会议暨中国自动化学会平行控制与管理专业委员会2016年全体会议于7月29日在北京举行。来自我国平行控制领域企业、院校和科研院所等40多个单位的70余名代表参加会议并进行了交流。美国工程院院士何志明教授，湖南大学电气与信息工程学院院长、湖南大学机器人学院院长王耀南教授参加会议，并作大会主题报告。

中国自动化学会副理事长王飞跃教授代表学会向代表致欢迎辞，简要介绍了平行控制研究的缘起和发展历史中的重要事件，回顾了平行控制理论、支撑方法和主要应用情况，并对平行控制的未来作了预测和展望。会议邀请嘉宾作主场报告6篇、钱学森国际杰出科学家演讲1篇。代表们围绕“自动化——复杂系统控制与管理”的主题，分别就平行控制学科领域发展现状及趋势、智能制造机器人自动化生产线关键技术及应用、面向社会性突发事件的人工社会计算实验平台研究、空间遥操作技术研究进展及展望、宇宙黑暗时代超长波探测系统、卫星重力反演的理论，方法和关键技术研究、复杂系统的控制等专题开展多元化研究领域交叉融合的讨论。

会上还完成了中国自动化学会平行控制与管理专业委员会的换届工作，新选举产生的第二届委员会的委员数量较上届有较大提升，由原来的40余人扩大为60余人，委员也由原来全部来自高校扩展为企业、院校和科研院所都有参与。同时，还在中国自动化学会秘书处吕爱英书记的指导下，以无记名投票的形式选举出第二届委员会

王飞跃教授

全体合影

骨干。清华大学航天航空学院王兆魁副教授当选为新一任委员会主任委员，湖南大学王耀南教授、西北工业大学黄攀峰教授、哈尔滨工业大学张锦绣教授、中国航天科技集团钱学森空间技术实验室郑伟研究员、海军航空工程学院沈如松副研究员当选副主任委员，清华大学工业工程系李乐飞副教授当选秘书长。在新任主任委员王兆魁副教授的主持下，全体委员对专委会后续工作开展讨论，并就学术交流、学术会议、信息平台建设、配合学会工作等方面形成一致意见。

随着信息技术的发展、网络化的普及和社会系统数字化进程的加快，复杂系统进行管理控制的方式暴露出的问题也越来越多。特别是在军事领域，联合作战呈现出了前所未有的复杂性，对军事系统研究提出严峻的挑战。为了更好地解决复杂系统面临的“不可分性”“不确定性”，我国科学家提出了“平行控制与管理”这个学术概念，进行了以平行控制和ACP方法为基础的一系列研究，并已取得了初步的理论和工程实践创新成果。

本次会议以“自动化——复杂系统控制与管理”为主题，旨在为来自多元化研究领域的专家、学者和研究人员提供一个针对平行控制及相关问题开展学术交流的平台，形成国内专门支持平行控制相关领域交流与合作的学术组织，促进我国平行控制研究的进步。

（平行控制与管理专委会 供稿）

大数据专业委员会成立大会在沈阳召开

2016年7月17日，中国自动化学会大数据专业委员会成立大会在辽宁沈阳举行。专委会成立大会由中国自动化学会理事、东北大学教授丁进良主持。东北大学副校长汪晋宽教授致欢迎词，对与会专家表示欢迎与感谢；中国自动化学会副理事长王成红研究员代表中国自动化学会宣读了同意成立大数据专业委员会的批复文件并致辞，并特别建议专委会成立后可以综合各方力量，团结一致，促进大数据与控制领域的结合，在做好学术研究的同时做好应用研究。

会议选举出了第一届专委会负责人。东北大学柴天佑院士当选为专委会主任，清华大学戴琼海教授、哈尔滨工业大学李建中教授、中国科学院数学与系统科学研究院吕金虎研究员、中国科学院大学石勇教授、西北工业大学周兴社教授当选为专委会副主任，东北大学丁进良教授当选为专委会秘书长。

柴天佑院士代表第一届专委会当选的负责人发言。他表示专委会成立后，将从学术角度，通过大数据来解决现在常规的，包括动态系统的建模、复杂系统的控制、多目标动态优化决策在内的一些问题，为国家控制科学与工程未来的发展助力。

与会人员还认真听取了哈尔滨工业大学李建中教授、香港中文大学秦泗钊教授以及德国汉堡大学张建伟教授的报告并进行了学术交流与讨论，会后参观了东北大学流程工业综合自动化国家重点实验室。大数据专业委员会为相关领域的研究学者提供了一个良好的学习和交流平台。本次成立大会的成功召开，将为推动国内相关学术研究和产业发展起到积极作用。

（大数据专业委员会 供稿）

中国自动化学会网络信息服务专业委员会工作会议暨2016年网络信息服务学术研讨会在上海召开

2016年8月25日下午2点，“中国自动化学会网络信息服务专业委员会工作会议暨2016年网络信息服务学术研讨会”在上海嘉定唐朝酒店牡丹厅隆重举行。

郑南宁院士首先作了以“人工智能下一步会是什么”为主题的学术报告。针对创造抽象思维、虚构想象、敏捷灵巧的运动能力等方面郑院士剖析了相关国内外的最前沿技术，并从直观概念学习与认知推理、人机合作、意图理解以及想象力—创作等方面，详细介绍了课题组最新研究进展。利用行为、行动以及对基本动作的解析，可以模拟音乐指挥家的动作；从健壮性设计、视觉系统设计方面，介绍最新机器人情景识别、无人车驾驶等方面的最新研究成果。最后郑院士指出了人工智能在健壮性的学习与认知推理、智能计算前移、新的计算架构等方面面临的新挑战。同时郑院士还指出，目前虽然深度学习很热门，但其不是人工智能的全部，仍然要关注并解决人工智能的基础性理论问题。

之后，举行了中国自动化学会网络信息服务专业委员会的专委主任、副主任、秘书长的选举工作。45位与会委员共同投票决定，由蒋昌俊教授担任专委会主任，段振华教授、宋爱波教授、单志广教授、庞善臣教授、谭民教授、刘民教授、程立高级工程师（支付宝公司首席技术官）为专委副主任，丁志军教授担任秘书长。蒋昌俊主任随后发表讲话，他表示对于继承自Petri网的网络信息服务专委会，未来要结合自动化、计算机、通信等方面，面向网络应用服务的方方面面，发挥委员的专长和优势，扩大学术影响力，同时蒋主任也表示之后会进一步打造具有国际影响力的国际专委组织。各位副主任以及丁志军秘书长，委员代表吴智铭教授、罗军舟教授，均发表了对新成立委员会支持的讲话，大家对专委的发展提出了自己的意见和建议，同时表示愿意尽自己的力量，促使专委会得到更好的发展。会议在各位与会委员热烈讨论的气氛中结束，网络信息服务专业委员会的工作会议圆满完成。

8月26日上午，在上海嘉定唐朝酒店牡丹厅举行了2016年网络信息服务学术研讨会。

首先，何友院士作了题为《信息感知与融合研究展望》的报告。何院士以“数字城市+物联网+云计算”为背景，分析了时空信息，并详细介绍了传感器信息融合研究的新进展，包括信息融合定义、信息融合系统功能模型、信息融合系统结构模型和信息融合数学模型的研究等，尤其在多传感器信息融合的权值分配与降维算法组合方面

的研究令与会者耳目一新。何院士指出，当前可以用人为传感器来感知环境信息，并举出了信息融合在智能交通和协同作战系统中的典型应用。同时具有海军军事背景的何院士也十分关注美国在通信与网络结构、计算与信息结构、频谱控制等方面最新展开的项目。何院士对国际军事技术的准确把握，让与会者对信息领域在国家战略层面的重要性有了更深刻的认识和体会。


之后，由中国自动化学会副理事长兼秘书长王飞跃教授作了题为《平行情报：迈向智能信息服务与决策支持》的报告。王飞跃教授从介绍英文LASER被命名为“激光”的过程，引出钱学森先生提出情报的“激活”理念。王教授指出，从普通的信息或知识，到钱学森“激活”的“活”的情报，充分认识到必须从牛顿的机械系统升华到默顿的智能系统是非常重要的一步。王教授进一步针对如何从牛顿、爱因斯坦的物质“激光器”转化成默顿或钱学森的情报“激活器”这一问题，提出情报5.0（Intelligence 5.0）或平行情报1.0（Parallel Intelligence 1.0, PI 1.0），即基于ACP平行理念的智能系统是构建情报“激活器”的一条可行途径。王教授宽广的知识面和深入浅出的讲解令与会者印象深刻。

专委会主任蒋昌俊教授作了题为《互联网+战略与实践》的报告。蒋昌俊教授指出随着互联网的深入应用，特别是以移动技术为代表的普适计算、泛在网络的发展，使互联网逐渐成为人们生产生活、经济社会发展各行各业所必需的生产要素。当前“互联网+”正全面应用到第三产业，形成了诸如互联网金融、互联网交通、互联网医疗、互联网教育等新业态，同时不断向第一产业和第二产业渗透。他结合各国的互联网发展战略，分析了国际互联网行业发展现状，深入探讨了与“互联网+”密切相关的大数据、物联网和云计算等新一代信息技术，并对“互联网+”战略进行了分析和综述，最后介绍了所领导的课题组在互联网交易支付风险防控与智能城市路网所取得的技术突破和应用成果。

蚂蚁金服CEO首席执行官程立高级工程师作了题为《人工智能驱动的金融生活》的报告。在报告中程立指出目前金融应该融入生活而不独立于商业，针对金融领域，当前数据风控、可信计算、生物信息识别应融合深度学习，加强学习，迁移学习等技术，形成AI+金融的安全体系。从蚂蚁智能客服、蚂蚁安全大脑、芝麻信用、大数据微贷、保险等方面给大家解析了人工智能的融入及未来发展前景。作为工业界代表，程立先生丰富的实际工业经验为与会者带来了非常直观的工业技术需求。


此次大会为从西面八方来到的同行提供了很好的认识和交流机会，为大家今后的合作及发展提供了良好的平台，各位参会人员都收获颇丰，感受到了从学术界到工业界一致的对网络信息服务技术的需求及研究热情。

（网络信息服务专委会 供稿）

中国自动化学会通讯 第37卷 第4期 总第187期 2016年8月

“党建强会”科普下基层活动——中国自动化学会走进西北农林科技大学

2016年7月5日，中国自动化学会党支部（以下简称“学会党支部”）一行来到西北农林科技大学，通过送资料、作报告、座谈交流等方式开展了此次学会党支部“党建强会”活动。

7月5日上午，学会党支部走进西北农林科技大学机电学院举办了精彩纷呈、内容丰富的学术报告会。学会副秘书长兼党支部副书记张楠以《蓬勃发展的中国自动化学会——“中国自动化学会科普下基层”走进西北农林科技大学》为题，介绍了中国自动化学会的发展历程。智能机器人专家、中国科学院自动化所高技术创新中心主任原魁研究员，陕西省自动化学会副理事长兼秘书长、西安交通大学曹建福教授，分别从不同的角度，以图片、视频和故事等形式，对机器人技术的“前世今生”及未来发展作了介绍。原魁研究员在以《离我们越来越近的机器人》为题的报告中表示，机器人在做我们不愿意做的工作、做我们做不了的工作、提高生产效率、做危险工作、家用服务等方面发挥重要作用。曹建福教授以《机器人改变世界——无所不在的机器人》为题，强调了机器人就在我们身边，世界农业的未来将大量采用机器人技术，以提高作业效率，实现精准农业和绿色农业。此次学术报告会得到了老师及学生的热烈欢迎，近两百名师生到场聆听学术报告。

7月6日上午，学会党支部在机电学院举办了“以自动化思维服务三农”的主题讲座。人民日报高级记者蒋建科、北京市昌平区科协秘书长甄

中国自动化学会副秘书长兼党支部副书记张楠作报告

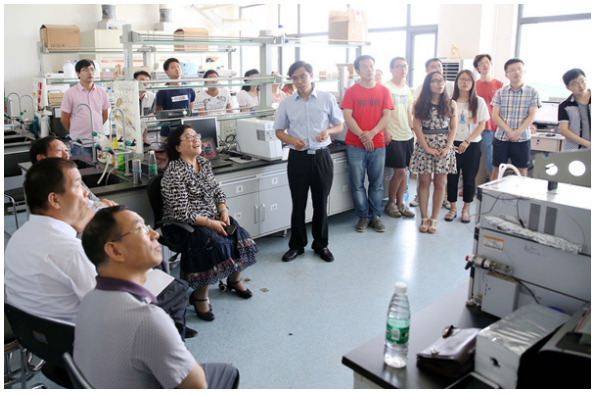
智能机器人专家、中国科学院自动化所高技术创新中心主任原魁研究员作报告

陕西省自动化学会副理事长兼秘书长、西安交通大学曹建福教授作报告

北京市昌平区科协秘书长甄燕昌（左）和人民日报高级记者蒋建科（右）与师生们进行亲切交流

学会党支部“党建强会”活动报告会现场

学会党员支部成员与机电学院部分师生合影留念



学会党支部听取理学院糖生物学团队党支部的工作汇报

“以自动化思维服务三农”讲座现场

燕昌、学会党支部书记吕爱英与师生们进行了亲切交流。甄燕昌和蒋建科两位专家采用“一问一答”新颖的座谈形式，通过列举多个典型案例，向师生们介绍了如何打破常规思维，从事物的另一面开辟蹊径，做好三农工作中的科技服务与新闻报道。讲座期间，同学们积极提问，专家们热情解答，会场气氛十分热烈。当日下午，学会党支部在校党委宣传部部长闫祖书陪同下，来到理学院糖生物学团队党支部，与支部师生党员进行了交流。

在此次活动中，学会党支部为西北农林科技大学师生赠送《习近平关于科技创新论述摘编》《中国自动化学会通讯》《中国共产党章程》等资料。期间，学会党支部一行还与校党委宣传部党支部部分成员共赴扶眉战役烈士陵园，向革命先烈们敬献花篮，并在烈士纪念碑前重温入党誓词。

西北农林科技大学地处中华农耕文明发祥地、国家级农业高新技术产业示范区——陕西杨凌，现为教育部直属、国家“985工程”和“211工程”重点建设高校。具有82年办学历史，先后涌现出国家最高科技奖获得者李振声院士、小麦育种家赵洪璋院士等一大批著名农业科学家，为社会累计培养输送本科以上专业人才13万余名，为我国干旱半干旱农业作出了突出贡献，学校党建工作特色鲜明。该校机电学院及其自动化专业不仅在农业自动化领域取得一大批科技成果，也培养了大批专业人才。今后我会将加强与西北农林科技大学机电学院等相关院系的互动交流，促进自动化事业在农业领域的发展，为推动“一带一路”战略实施作出应有的贡献。我会通过此次“党建强会”活动，进一步推动了学会党建工作的深入开展，也有力地促进了学会业务活动的拓展。

（学会秘书处 供稿）

中国自动化学会

中国自动化学会（Chinese Association of Automation，缩写CAA）于1961年在北京成立，是我国最早成立的国家一级学术团体之一，是中国科学技术协会的组成部分，是发展我国自动化科技事业的重要社会力量。学会现有个人会员近4万人，团体会员近200个，专业委员会33个，工作委员会8个，29个省、自治区、直辖市设有地方学会组织，基本覆盖了我国自动化科学技术领域的各个层面。

中国自动化学会在改革中求发展，不断加强学术影响力、社会公信力、会员凝聚力和自主发展能力的建设。近年来，中国自动化学会重点从学术交流与应用推广、组织建设与会员服务、科技评估与人才评价、课题研究与决策支撑、科学普及与继续教育等几方面开拓创新，推动中国自动化科学和事业的发展和壮大，成为连接政府、产业、学术、科研、会员的重要纽带，致力于成为国内外有影响力的现代社会团组织。

学会品牌学术活动

中国自动化大会
智能车发展论坛
钱学森国际杰出科学家系列讲座
中国过程控制会议
国家机器人发展论坛
世界机器人大会
中国控制会议
青年学术年会.....

学会奖励奖项

CAA科学技术奖励
CAA优秀博士学位论文奖
杨嘉墀科技奖

会员服务

了解自动化领域前沿科研成果，领略自动化领域专家风采免费或优惠参加中国自动化大会等顶级学术活动、学术刊物赠阅、技术咨询、成果鉴定、技术培训、人才推荐等增值服务。

官方微信　　官方微博

地址：北京市海淀区中关村东路95号　　电话：010-62521822，010-82544542
邮编：100190　　邮箱：caa@ia.ac.cn　　网站：http://www.caa.org.cn/

中国自动化学会

电话：010-82544542
传真：010-62522248
邮箱：CAA@IA.AC.CN

您想了解自动化领域前沿科研成果吗？

您想免费参加中国自动化大会等顶级学术活动吗？

您想领略自动化领域专家风采吗？

让我们走进中国自动化学会，

一同感触自动化学界的魅力！

在这里，
作为个人会员，您可以：

- **免费获得自动化领域学术刊物和《控制科学与工程学科发展报告》**
- **优惠或免费参加学会和分支机构主办的学术活动（中国自动化大会、钱学森国际杰出科学家系列讲座、中国控制会议、中国过程控制会议、青年学术年会，等）**

作为团体会员，您可以：

- **在学会会刊及相关宣传媒介发布专利、项目成果信息**
- **优先获得学会提供的技术咨询服务**
- **优先获得学会提供的产品展示、技术培训服务**
- **优先获得学会提供的成果鉴定、项目验收、奖项申报服务**
- **优先获得学会提供的人才推荐、宣传和推广服务**

只需一分钟，一切都将实现！

姓　　名		性　　别		出生年月	
专　　业		工作单位		职称职务	
电子邮件				联系电话	
通信地址				邮　　编	

欢迎通过中国自动化学会官方网站WWW.CAA.ORG.CN，中国自动化学会新浪微博（@中国自动化学会微博）以及“中国自动化学会”微信平台与我们互动交流！感谢您对中国自动化学会的关注与支持！

微信二维码　　微博二维码