

平行安全：基于 CPSS 的生成式对抗安全智能系统

李浥东¹, 张俊^{2,3}, 陶耀东¹, 王伟¹, 顾元祥⁴, 王飞跃^{2,5,6}

(1. 北京交通大学, 北京 100044; 2. 中国科学院自动化研究所, 北京 100190;

3. 武汉大学, 湖北 武汉 430000; 4. 爱迪德公司, 加拿大 渥太华 K2T1G5;

5. 中国科学院大学, 北京 100049; 6. 青岛智能产业技术研究院, 山东 青岛 266109)

摘要: 人工智能、大数据等新一代信息技术的兴起使网络空间安全面临的威胁与挑战进一步复杂化。传统防御技术多采用“打补丁”式的被动检测防护机制, 很难满足由新的攻击特征带来的安全防护需求。首次系统性地提出以平行智能 ACP 理论为基础思想的平行安全系统框架, 利用生成式对抗模型、平行情报、平行区块链等方法, 融入社会学、心理学和行为学等因素, 建立了集描述性安全、预测性安全和引导性安全于一体的防护体系, 旨在实现以“增强免疫力”为目标的预测引导防护。以工业互联网典型场景为实际案例, 设计并研发了首个以平行安全框架为基础的生成式对抗安全智能系统平台, 从而为平行安全在不同领域的实际应用提供指导和借鉴。

关键词: 网络空间安全; 平行安全; 生成式对抗系统; ACP; 人工智能; 平行系统

中图分类号: TP309.2

文献标识码: A

doi: 10.11959/j.issn.1000-436x.202022

Parallel security: generative adversarial systems for intelligent security in CPSS

LI Yidong¹, ZHANG Jun^{2,3}, TAO Yaodong¹, WANG Wei¹, GU Yuanxiang⁴, WANG Fei-Yue^{2,5,6}

1. Beijing Jiaotong University, Beijing 100044, China

2. Institute of Automation, Chinese Academy of Sciences, Beijing 100190, China

3. Wuhan University, Wuhan 430000, China

4. Irdeto Corp, Ottawa K2T1G5, Canada

5. University of Chinese Academy of Sciences, Beijing 100049, China

6. Qingdao Academy of Intelligent Industries, Qingdao 266109, China

Abstract: Developing technologies such as AI and big data are changing the landscape of cybercrime for both attackers and defenders. Traditional defense technology mainly use the passive detect-then-defend model, which is hard to meet the security protection requirements brought by new attack characteristics. A novel security framework, named parallel security was proposed, which aimed at providing a comprehensive solution with descriptive security, predictive security and prescriptive security. The main idea was based on the ACP theory of parallel intelligent, and integrated new methods such as generative adversarial learning model, parallel blockchain. Human elements, sociology and psychology were taken as an important component in the framework, in order to enhance the immunity of the system. In addition, a parallel security based platform was design and developed for several typical scenarios in the field of industrial internet as a proof of concept.

Key words: cyberspace security, parallel security, generative adversarial system, ACP, artificial intelligence, parallel system

收稿日期: 2020-04-02; 修回日期: 2020-04-29

通信作者: 李浥东, ydli@bjtu.edu.cn

基金项目: 国家重点研发计划基金资助项目 (No.2018YFB0803500); 国家自然科学基金资助项目 (No.U1934220)

Foundation Items: The National Key Research and Development Program of China (No.2018YFB0803500), The National Natural Science Foundation of China (No.U1934220)

1 引言

网络空间安全已成为国家安全和社会安全与稳定的基石。与此同时，网络空间安全的内涵不断发展和进化，由“万物互联”、智能系统、边缘计算和 5G 等新技术和新模式引发的新型安全（如工业互联网安全、车联网安全、泛在电力物联网安全等）问题日益凸显。因此，利用生成式对抗学习模型和区块链等新型防护方法，构建基于社会物理信息系统（cyber-physical-social systems, CPSS）的平行安全系统，使传统“打补丁”式的被动检测防护向以“增强免疫力”为目标的预测引导防护演进，促进大安全时代中防护理念、技术思想和产业思维的全面升级。随着信息安全与智能产业的关联愈发紧密，中国自动化学会在 2015 年针对智能产业的系统安全问题开展了 2 次前沿国际研讨会。在北京召开的第四届互联网安全领袖峰会上，王飞跃教授受邀做大会报告，首次提出了平行安全的主要思想、技术体系及其在国防和交通等领域的应用实践^[1-2]。随后，平行安全分别作为 2018 年世界人工智能大会和 2019 年第十届信息安全与软件保护国际学术论坛的热点主题^[3-4]，得到了国际信息安全领域专家的高度关注。2019 年 10 月，第六届行为、经济与社会文化计算国际会议设立了平行安全特别论坛，与会者深入探讨了社会因素给信息安全带来的挑战与机遇，平行安全思想的理论体系得到了进一步完善。

2 人工智能时代，网络空间安全面临的挑战

大数据、云计算、物联网和人工智能等新技术的兴起注定会使网络空间安全面临的威胁与挑战进一步复杂化，使其具有了新的“4V”特征，即攻击来源数量大（volume）、攻击方式多样化（variety）、攻击过程隐蔽性强（visibility）、攻击目标价值高（value）。

（1）攻击来源数量大

在震惊世界的 2016 年美国“断网事件”中，攻击者通过控制由十几万台智能物联网（Internet of things, IoT）设备组成的僵尸网络，利用技术原理非常简单的分布式拒绝服务（distributed denial of service, DDoS）攻击造成了半个美国的网络陷入瘫痪。2018 年年底，全球物联网接入设备量达到 220 亿，预计 2025 年将增长到 386 亿，而 2030 年将增长到

500 亿^[5]。由于物联网设备计算和存储资源有限，其加密和验证机制较弱，据 Gartner 预测，超过半数的 IoT 设备制造商将无法保障产品安全。爆炸式增长的联网设备将为攻击者提供数量极其可观的攻击源，这对整个网络空间的安全构成了巨大威胁。

（2）攻击方式多样化

近年来，定向勒索病毒、数据投毒、社工攻击、生物识别欺骗等一系列基于人工智能技术的新型攻击不断涌现，网络攻击地下黑色产业链逐渐发展成熟，各种攻击案例层出不穷，MITRE ATT&CK 知识库总结的攻击者在攻击企业时利用的战术（tactics）和技术（techniques）分别达到 12 种和 244 种^[6]。攻击手段的演化速度也越来越快，如 2019 年年底勒索病毒的种类已经超过 234 种^[7]。有些攻击甚至通过定制化不同用户阅读到的网络内容来控制公众的认知和判断。这些“万变”的攻击手段，使得安全漏洞被利用的速度加快，大规模攻击案例难以复现，复合攻击难以预测，已有的安全防护措施难以及时应对。

（3）攻击过程隐蔽性强

在智能技术的支持下，以高级持续性威胁（advanced persistent threat, APT）为代表的长期持续性网络攻击（如伊朗布什尔核电站遭受的震网攻击、乌克兰和委内瑞拉电网遭受网络攻击造成大规模停电等）发展迅速。攻击者可以利用人工智能技术设计具有自我学习和隐蔽能力的智能化网络攻击软件，模仿系统中正常用户的行为，并通过不断改变隐藏方法尽可能长时间地停留在计算机系统中，使得传统安全检测系统无法有效检测，从而针对特定对象，长期、有计划和有组织地窃取数据。这些新型攻击手段的兴起，使得反制和追踪攻击行为变得越来越难，网络空间安全“易守难攻”的形势愈加严峻。

（4）攻击目标价值高

随着数字经济的快速发展，越来越多的企业和个人认识到数字资产的巨大价值和重要意义。随着工业互联网、车联网以及泛在电力物联网的发展，社会场景数字化、人工智能算法化、工业数据模型化、工业知识软件化等趋势越来越明显，数字资产的范围不断扩大，其价值已逐步接近物理世界资产，未来甚至会超越物理世界资产。近年来，针对智能数据资产的攻击事件频繁发生，造成的直接经

济损失越来越大。例如,工业领域的专业知识、软件、模型和数据等资产的价值将远超消费互联网领域的资产价值,而且“万物互联”的模式打通了物理世界和数字世界,使得网络攻击可能会给物理世界带来实际影响和损失。2018年1月,黑客攻击日本数字货币交易所 Coincheck,并成功窃取了价值5.3亿美元的虚拟货币。2018年3月,脸书公司遭遇了其史上最大的数据泄露事件,5 000万用户的数据被泄露,导致其一天内市值蒸发60亿美元。据统计,每年仅由勒索病毒造成的经济损失就高达750亿美元^[8]。2018年,台湾积体电路制造股份有限公司(以下简称“台积电”)感染勒索病毒,导致三大工厂停产,事后台积电对外公布称事件造成其季度营收降低3%,毛利率降低1%,外界估算此次网络安全事件造成的经济损失将高达2.5亿美元。2019年,挪威铝业巨头海德鲁公司因为感染勒索软件而停产,造成的直接经济损失高达4 100万美元。此外,社工攻击可专门针对价值高的目标实施周期较长的个性化攻击。这些攻击方式五花八门,不仅会造成巨大的经济损失,还可使国家安全受到严重威胁。

3 平行世界的安全观演化

网络安全安全与社会各个层面紧密相连,已从原来的通信安全、计算机安全或网络安全向网络安全空间安全延展,最终将进入无边界安全,逐步形成一个“大安全”概念。这就要求针对网络空间的安全防护从安全观、安全范畴、安全策略和安全机制等方面进一步演化升级。

(1) 安全观的演化

传统的安全观主要强调物理系统(如工业设备)或者网络空间(如互联网)的单一世界安全,而在安全边界延展过程中,基于波普尔的“三个世界”理论将成为新安全观演化的基础,即未来的安全应该是能够同时保障物理世界、心理世界和人工世界安全的“大安全”。整体的、动态的、开放的、相对的和共同的安全观已经成为网络信息安全领域的普遍共识。

(2) 安全范畴的演化

传统信息安全领域仅关注信息系统的保护,随着工业互联网、物联网和边缘计算等新模式打通信息世界和物理世界的边界,安全防护范畴也扩展到物理信息系统^[5-6],但其对“人”在安全系统中的影响考虑较少。因此,未来安全的防护范畴必须将

“人”纳入安全环路中,向兼具高度社会复杂性和工程复杂性的社会物理信息三元系统演化。作为信息安全行业的风向标,2020年2月在旧金山召开的RSAC2020将主题定为“人是安全要素(human element)”,凸显出安全范畴的扩展演化已经成为全球范围内的行业共识。

(3) 安全策略的演化

传统的安全策略还停留在以描述性安全为主、预测性安全为辅的“打补丁”式被动检测防护模式,这种被动的安全策略在面对由系统复杂性引发的安全威胁时显得力不从心。因此,需要将攻防双方的心理和社会因素纳入安全策略的建设体系中,将主要思想从“牛顿范式”向“默顿范式”演化,利用生成式对抗模型产生的安全大数据填补认知鸿沟,建立以引导安全为主、预测性安全和描述性安全为辅的主动式安全防护体系,不断增强系统的免疫力。

(4) 安全机制的演化

传统的安全机制主要对特定系统、特定应用或特定攻击进行分析,并设计相应的防护方案,局限于待保护系统的内部。而未来的安全机制应该将安全系统的输入机制(威胁情报的获取与共享)和输出机制(防护手段的认证与存储)作为一体化安全机制构建的重要组成部分。前者可以利用情报学等技术实现威胁情报共享、恶意软件归因和数据隐私评估等,后者可以利用区块链技术进行机制认证与固化。

4 平行世界的安全新范式:平行安全

中国科学院自动化研究所研究员王飞跃提出了平行系统的思想,其核心为通过构建虚实互动的真实系统和人工系统来研究复杂系统的控制优化^[9]。近年来,平行智能理论已被广泛应用于国防安全、智能交通、智能控制和智能感知等领域,并取得了显著的实践效益^[10-12]。平行智能通过研究数据驱动的描述智能、实验驱动的预测智能以及互动反馈的引导智能,为不定、多样和复杂问题提供敏捷、聚焦和收敛的解决方案。而平行安全是有效解决与网络安全空间建模、实验与决策相关的问题的理论方法,是平行智能与网络安全空间的深度结合。平行世界的安全新范式体系如图1所示,即以面向平行智能的ACP理论为基础理论,采用生成式对抗模型(平行安全的核心基础方法)、平行情报、平行区块链等关键方法,有机地融入社会学、心理

学和行为学等因素，建立集描述性安全、预测性安全和引导性安全于一体的防护体系。

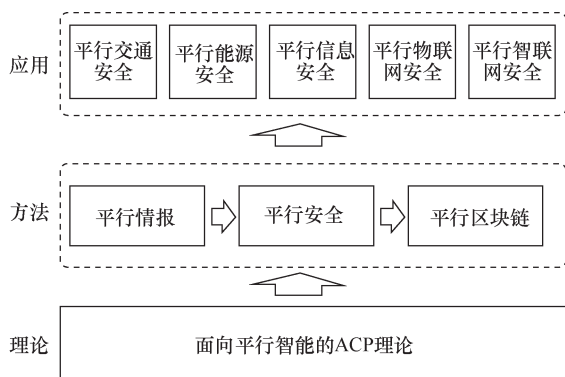


图1 平行世界的安全新范式体系

4.1 ACP 理论

平行系统的核心理论与技术是 ACP 方法，其主要思想是在构建与真实系统相似的人工系统（artificial systems）基础上，通过利用高效、鲁棒性强的人工智能和机器学习等方法对构建的不同数学问题进行计算实验（computational experiments），最终实现人工系统和真实系统的平行执行（parallel execution），即用人工系统来指导真实系统，同时真实系统也可优化人工系统。

具体来说，在人工系统的构建过程中，需要保证人工系统与真实系统的一致性，只有在足够准确的模型基础上获得虚拟控制和决策，才能对真实系统起到指导作用。在具体实施过程中，主要通过描述学习的方法对系统进行描绘和构建。同时，模型的精度可以在平行执行的过程中实时提升。计算实验在人工系统和真实系统 2 个维度中同时进行。在真实系统中，主要对历史数据和实时数据进行处理和分析，以获得能够指导真实系统运行的知识；在人工系统中，通过预测学习和引导学习获取未来的或者未经历过的知识，从而提高平行系统的完备性。平行执行则无时无刻不在平行系统中体现，包括人工系统和真实系统之间的数据流、控制流、模型流等。反馈是人工系统流向真实系统的描述，利用大量人工智能、机器学习算法获得知识，从而引导真实系统；提升是真实系统流向人工系统的描绘，真实系统的知识能够更好地反馈当前整个系统的走向和趋势，从而对人工系统的模型进行引导和修改。

4.2 基于 ACP 的平行安全系统框架

平行安全是面向复杂系统建模与调控的 ACP

理论在网络空间安全领域中的推广应用^[13]。其核心是利用人工系统模拟和表示复杂的实际系统，通过计算实验进行各种安全模型的训练与评估，借助虚实互动的平行执行来在线优化安全模型，实现对复杂系统的智能安全防护与免疫能力的提升。相较于已有的基于 ACP 理论的平行智能系统，“人”对平行安全系统的影响更为重要。网络空间安全的攻防是一个交互性极强的过程，攻防双方的技术能力、心理素质以及对即时攻防态势的阅读和评估都可能对最终结果起到决定性作用。因此，在平行安全系统的设计过程中，必须将心理学、社会学、行为学等因素纳入考量，并将这些因素作为对系统进行有效性评估的重要度量标准。

基于 ACP 方法的平行安全系统基本框架如图 2 所示。综合考虑 CPSS 中的各种复杂因素，结合理论建模、经验建模和数据建模方法，建立与真实系统“伴生”的一个或多个安全系统（以下简称“人工系统”）。在人工系统中，利用生成式对抗学习与人工参与结合的方式对安全系统攻防双方特征与行为进行精确建模，以自底向上的涌现方式实施海量计算实验，并在实验过程中模拟、记录系统实时状态及演化特性，进而辅助推理和预测实际安全系统的各核心要素在不同情况下的耦合关系与演化规律。真实系统与人工系统通过特定的平行交互机制与协议连接，实时同步数据、模型、场景和决策等要素，并通过人工系统中“What-if”形式的场景推演，实现对系统未来状态的预测，并相应地调节各自的管理与控制方式。具体步骤如下。

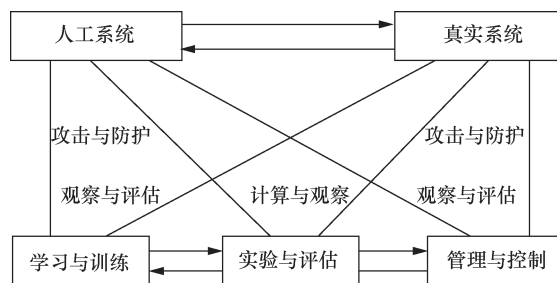


图2 基于 ACP 方法的平行安全系统基本框架

(1) 学习与训练

首先，构建能够反映真实系统状态与演化规律的人工系统。然后，以多媒体、可视化技术为主要手段，收集系统已有的攻击方法形成攻击集合，将这些攻击集合进行自动化组合，形成真实系统中可

能出现的各种攻击方法,自动生成攻击模型,并产生大规模、多样性的攻击案例。利用这些攻击案例进行场景式攻防训练,使相关人员熟悉尽可能多的攻击方法和相应的防护方法。同时,人工系统为每个参与者建立相应的“人工模型”,从而提高安全任务平行执行过程的效率和准确性。最后,以“以万变应不变”的培养方式,为安全人员提供必备的安全知识和技术支撑,使其能够灵活应对各种不确定情况。

(2) 实验与评估

在人工系统对真实系统进行大量计算实验,验证并评估真实系统在各种可能攻击场景下的检测和防护效果。以实际系统的运行数据为输入,结合人工系统攻击案例和真实系统攻击案例,用计算的方式分析了解复杂真实系统面对不同攻击时的行为和反应,设计和优化安全检测和防护算法,评价安全算法在不同攻击场景下复杂系统中的检测和防护效果。对不同的解决方案、管理策略、法律法规的效果进行评估,并将评估结果作为辅助管理与控制决策的依据。

(3) 管理与控制

通过建立人工系统和真实系统的平行执行与协同演化机制,实现对真实系统的管理和控制。将安全防护模型在真实系统与人工系统中平行执行,通过人工系统中构建的攻击集和攻击组合,对模型进行密集的强化学习和快速评估,使安全模型的训练和评估在线化、长期化。通过真实系统与人工系统之间的虚实互动和人机混合,持续优化安全计算系统。在复杂系统中,安全防护与免疫是极其困难的,不存在“绝对安全”的解决方案,只能在系统运行过程中不断调节和改善,以平行执行的方式持续优化,达到“以不变应万变”,从而完成对复杂多变情况下执行安全防护任务过程的有效控制、管理和指挥。

4.3 平行情报与平行区块链

平行安全的最终目标是形成一体化机制,实现对系统有效、持续、及时地防护与免疫。因此,在与安全相关的数据和知识的感知、融合、分析、共享等方面需要依靠平行情报^[14]和平行区块链^[15]等新的理论和方法进行支撑。由于篇幅所限,感兴趣的读者可以阅读相关文献,本文仅对其主要思想做简要描述。

平行情报将智能技术、数据工程、情报解析集

成于一体,形成基于模型和数据驱动的情报分析,为实现智能化平行情报系统提供了完备的框架和算法。其主要思想是首先在建立人工情报机构的基础上,通过引入游戏动漫等方式帮助工作人员快速熟悉情报业务。同时,人工情报系统建立了每个工作人员的“人工模型”,并针对性地用于情报任务的平行执行过程,从而提醒、监督、奖惩相关工作人员。然后在人工情报系统中解析评估周期、流程、生产、控制、传播等情报工作与方式的设置以及情报质量等一系列问题,并对各种各样的情报计划和解决方案进行不同程度的测试,提出最佳的情报工作方式。最终将人工情报系统与实际情报系统相连,形成虚实互动、反馈闭环、实时自适应调节的平行情报系统。在平行安全系统框架中,平行情报作为系统的重要输入信息起着举足轻重的作用,其收集和提供的信息质量会极大地影响平行安全系统防护的有效性和及时性,这方面的工作值得进一步深入研究。

在平行安全系统框架中,平行区块链是一种非常有效的数据共享和攻击行为溯源方法。其基本思想是通过形式化地描述区块链系统核心要素的静态特征与动态行为构建人工区块链系统,利用计算实验对特定区块链应用场景进行试错实验与优化,并通过人工区块链系统与实际区块链系统的虚实交互与闭环反馈,实现决策寻优与平行调谐。以平行区块链在车联网中的应用为例,首先基于多智能体方法对智能传感器及其构成的区块链 P2P 网络进行人工建模,并建立与之“等价”的虚拟传感器及虚拟区块链。然后,针对虚拟区块链进行基于智能合约的计算实验,以可编程的智能合约实现复杂场景与复杂传感器的行为,计算虚拟区块链系统在不同场景、不同参数配置下的运行效果,并对效果进行评估,以此作为合约选择和支持最优决策的依据。最后,通过虚拟区块链和实际区块链的互动反馈形成对实际区块链的管理与控制。通过构建多传感器的区块链 P2P 网络,建立区块链驱动的多传感器共识与去中心化信任机制。同时,将传感器作为区块链节点,参与数据校验与记账。当某个传感器感知到数据时,在 P2P 网络中对该数据进行广播,相邻节点收到数据后对其进行有效性校验,只有通过半数节点验证的数据才能被保留。

5 工业互联网中的平行安全应用

平行安全作为一种新的安全框架体系,其完备

性和成熟性需要经过大量严格的实践检验。本节以工业互联网安全领域为例,介绍平行安全框架在实际系统中的实现方法。

5.1 工业互联网面临的安全挑战

近年来,工业信息在国民经济中占据的重要地位使得工业互联网安全备受关注。产业界和学术界围绕工业信息安全方面,尤其是工业控制系统的信息安全问题开展了广泛的研究,从系统的整体到局部给出了多种安全防护的理论观点^[16-17]。然而,在实际应用中,工业互联网安全依旧面临极大的挑战。

(1) 安全认知不深入

现有研究主要集中在工业信息安全的规范制定、导则制定和控制系统的软件漏洞发现方面,很少从具体控制系统的自身技术特性入手来研究工业信息安全的具体问题和处理措施。工业信息系统在设计之初更多考虑的是系统的可靠性和实时性,一般都假设系统内的装置与设备是安全可靠的,而不太关注信息安全的问题,致使缺乏足够的安全机制(如采用的授权、鉴别和加密等信息安全技术不足),因此很容易被攻击者利用。

(2) 工业系统差异化程度较高

与信息系统安全相比,工业系统信息安全较难管理,原因在于旧有系统很少升级,大量分散的资产需要频繁地远程访问服务,而安装杀毒软件、防火墙等传统防护措施并不完全适用于工业系统。同时,在工业系统安全防护中普遍存在不同领域的理论与技术混合使用的情形,而不同工业领域的产品并不完全兼容,所用到的防护技术与方法存在极大差异。

(3) 生产系统进行攻防演练困难

在工业互联网安全领域,构建与真实系统同时运行的人工系统的需求尤为突出^[18-20]。由于实际的工业系统资产价值高,其控制系统时刻监控生产过程的运行,不允许在真实系统中实时地开展与安全相关的测试评估,因此工业互联网安全研究一般采用构建仿真测试验证环境的方法^[21-23]。部分研究者还利用仿真测试系统生成了安全数据集供其他研究者使用^[24]。然而,这类仿真测试系统大部分仅实现了对真实系统的功能模拟,建模依赖真实系统的静态参数,很难根据真实系统面临的动态攻防变化进行迭代学习,因此难以从根本上提升系统的免疫能力。同时,大多数仿真模型并未系统性地考虑人为因素对系统状态的影响,从而

导致防护模型和方法的有效性、持续性和及时性无法得到保障。

5.2 面向典型工业互联网场景的平行安全系统

本文以平行安全框架为理论基础,提出了一套面向典型工业互联网应用场景的平行安全智能系统,并开发了相应的测试与验证平台(如图3所示)。该系统目前已经实现了火力发电厂、轨道交通、智能电网、智能制造4个典型平行城市^[25]应用场景的人工系统建模,不同于传统的安全仿真平台,本文提出的系统对工业互联网中分属不同层级的节点均进行了建模,如生产系统、监控系统、办公系统、灾备系统等,可以最大限度地模拟攻击对系统的整体影响及演化趋势。同时,由于控制系统在工业互联网中具有极为重要的作用,人工系统将对应用场景中的控制系统进行单独建模,并利用实际设备建立了用于平行执行实验室验证的最小系统,从而实现对工业互联网核心系统与装备的分级防护。

以轨道交通平行安全子系统为例。对列车运行控制系统、调度系统、牵引供电系统、屏蔽门控制系统、监控系统等实际系统及其互连网络进行建模,从而建立可反映轨道交通实际运营场景的人工系统。利用目前已知的较为流行的针对控制系统、监控系统、应用软件等的攻击案例,对人工系统进行手动和自动的组合攻击,并进行有针对性的安全防护(手动和自动)。系统记录攻击防护的全过程信息以及相应的系统状态,形成可供机器学习的攻防样本案例库。通过对攻防样本进行特征提取和深度分析,给人工系统提出有效的安全防护模型和策略建议,最终构建具有一定免疫能力的人工系统。

在实验与评估阶段,将在轨道交通系统真实攻击案例中采集的数据注入人工系统,通过对系统的状态演化进行追踪,验证系统的有效性。在此基础上,设计组合攻击案例,并对人工系统进行有组织的攻击,通过生成式对抗学习不断优化迭代人工系统的免疫模型。同时,构建轨道交通各子系统的状态演化模型,并对各演化状态对实际运营的影响进行多角度评估。

在平行执行阶段,人工系统与实验室最小功能系统(如图4所示)进行交互,从而验证人工系统的免疫模型在实际物理系统中的有效性和及时性。

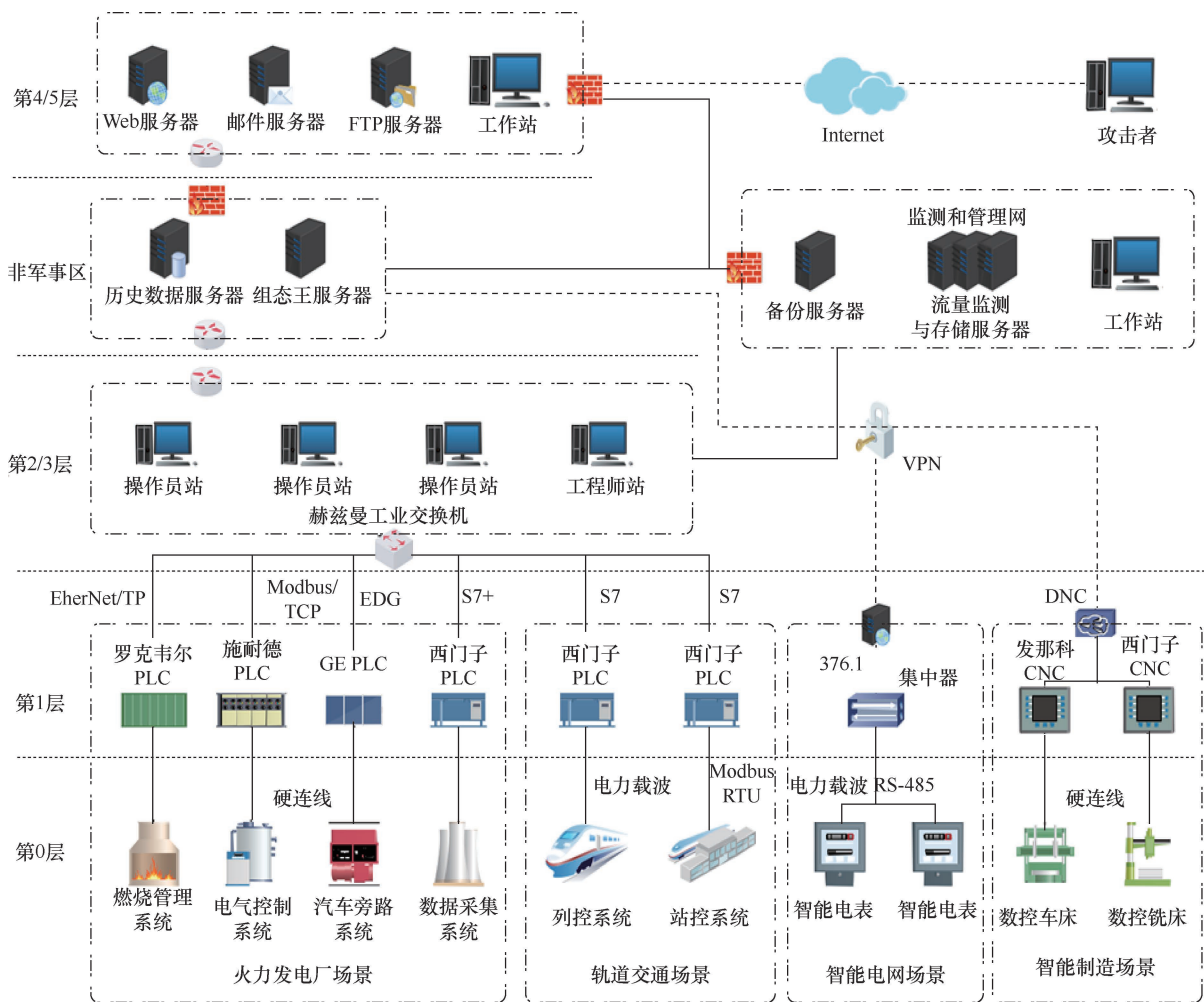


图 3 面向典型工业互联网应用场景区的平行安全系统逻辑架构

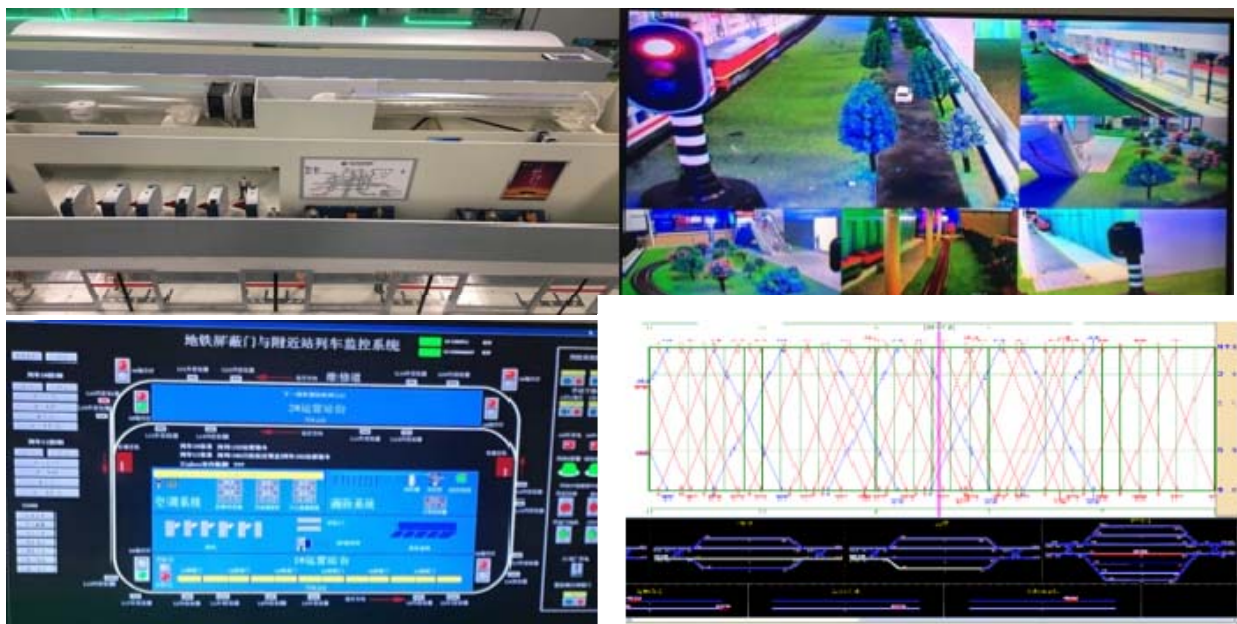


图 4 轨道交通平行安全实验室功能验证最小系统示意

6 结束语

人工智能时代的网络空间安全愈发成为一种高技术对抗,而且攻守双方严重不对称,易守难攻。安全人员使用人工智能技术阻挡黑客攻击,反过来黑客也会使用人工智能技术发起更复杂的攻击。为了应对新时代赋予网络空间安全的新特征,需要从安全观、安全范畴、安全策略、安全技术和安全机制等方面不断演化。这就需要基于平行智能的 ACP 理论,建立集描述性安全、预测性安全和引导性安全于一体的安全防护体系,以生成式对抗模型、平行情报等为主要技术手段,有机地融入社会学、心理学、行为学等社会因素,实现在知识世界“吃一堑”,在物理世界“长一智”。可以说,在人工智能时代,平行安全将成为保护平行世界中各类 CPSS 最有效的解决方案,不仅在平行智能与网络空间安全理论研究方面具有创新意义,而且在智能数字资产保护、工业互联网安全和个人隐私保护等方面具有重要的应用价值。

参考文献:

- [1] WANG F Y, LIU K L. An acp-based parallel systems approach for integrated security management, evaluation, education, and training (ISMEET)[R]. 2014.
- [2] 王飞跃. 平行世界的平行安全: 基于 CPSS 的生成式对抗安全智慧系统[C]//第四届互联网安全领袖峰会. 出版地不详: 出版者不详, 2018. WANG F Y. Parallel security: an intelligent security system based on generative adversarial inCPSS[C]//The 4th Cyber Security Summit. [S.l.:s.n.], 2018.
- [3] WANG F Y. Parallel security: asolution for digital asset protection[C]//The International Workshop on Information Security and Protection. Beijing: [s.n.], 2019.
- [4] WANG F Y. Parallel security in parallel world: CPSS-GAN-based smart security systems[C]//The 2019 World Artificial Intelligence Conference. Beijing: [s.n.], 2018.
- [5] STRATEGY ANALYTICS. Internet of things now numbers 22 billion devices but where is the revenue?[R]. 2019.
- [6] STROM B E, APPLEBAUM A, MILLER D P, et al. Mitre att&ck: design and philosophy[R]. MITRE, 2018.
- [7] NJCCIC. Ransomware[R]. 2020.
- [8] DATTO: American small businesses lose an estimated \$75 billion a year to ransomware, new datto survey finds[R]. 2016.
- [9] 王飞跃. 人工社会、计算实验、平行系统——关于复杂社会经济系统计算研究的讨论[J]. 复杂系统与复杂性科学, 2004(4): 28-38. WANG F Y. Artificial societies computational experiments and parallel system:a discussion on computationaltheory of complex social-economic systems[J]. Complex Systems and Complexity Science, 2004(4): 28-38.
- [10] WANG F Y, ZHANG J, WEI Q, et al. PDP: parallel dynamic programming[J]. IEEE/CAA Journal of Automatica Sinica, 2017, 4(1): 1-5.
- [11] WANG F Y, WANG X, LI L, et al. Steps toward parallel intelligence[J]. IEEE/CAA Journal of Automatica Sinica, 2016, 3(4): 345-348.
- [12] WANG F Y. Parallel control and management for intelligent transportation systems: concepts, architectures, and applications[J]. IEEE Transactions on Intelligent Transportation Systems, 2010, 11(3): 630-638.
- [13] 王飞跃. 智能产业与平行安全及可持续发展[C]//第二次智能产业系统安全问题前沿国际研讨会. 青岛: 出版者不详, 2015. WANG F Y. Intelligence industry and parallel security[C]//The 2nd International Workshop on System Security in Intelligence Industry. Qingdao: [s.n.], 2015.
- [14] 王飞跃. 情报 5.0: 平行时代的平行情报体系[J]. 情报学报, 2015, 34(6): 563-574. WANG F Y. Intelligence 5.0: parallel intelligent architecture in parallel world[J]. Journal of the China Society for Scientific and Technical Information, 2015, 34(6): 563-574.
- [15] 袁勇, 王飞跃. 平行区块链: 概念、方法与内涵解析[J]. 自动化学报, 2017, 43(10): 1703-1712. YUAN Y, WANG F Y. Parallel blockchain concepts methods and analysis[J]. Acta Automatica Sinica, 2017, 43(10): 1703-1712.
- [16] 工业互联网产业联盟. 工业互联网安全框架[R]. 2018. AII. Industrial internet security framework[R]. 2018.
- [17] 边缘计算产业联盟, 工业互联网产业联盟. 边缘计算参考架构 3.0[R]. 2018. ECC, AII. Edge computing reference architecture 3.0[R]. 2018.
- [18] ANDREEVA O, GORDYCHIK S, GRITSAI G, et al. Industrial control systems and their online availability[R]. 2016.
- [19] XU W, TAO Y D, GUAN X. The landscape of industrial control systems (ICS) devices on the Internet[C]//International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA). Piscataway: IEEE Press, 2018: 1-8.
- [20] MCLAUGHLIN S, KONSTANTINOU, WANG X Y, et al. The cybersecurity landscape in industrial control systems[J]. Proceedings of the IEEE, 2016, 104(5): 1039-1057.
- [21] XU W, TAO Y D, YANG C, et al. MSICST: multiple-scenario industrial control system testbed for security research[J]. CMC-Computers, Materials & Continua, 2019, 60(2): 691-705.
- [22] CANDELL R, ZIMMERMAN T A, STOUFFER K A. An industrial control system cybersecurity performance testbed[R]. 2015.
- [23] CANDELL R, STOUFFER K, ANAND D. A cybersecurity testbed for industrial control systems[C]//Proceedings of the 2014 Process Control and Safety Symposium. Houston: [s.n.], 2014.
- [24] TAO Y D, XU W, LI H B, et al. Experience and lessons in building an ICS security testbed[C]//International Conference on Industrial Artificial Intelligence. Shenyang: [s.n.], 2019.
- [25] 吕宜生, 王飞跃, 张宇, 等. 虚实互动的平行城市: 基本框架、方法与应用[J]. 智能科学与技术学报, 2019, 1(3): 311-317. LYU Y S, WANG F Y, ZHANG Y, et al. Parallel cities: framework, methodology, and application[J]. Chinese Journal of Intelligent Science and Technology, 2019, 1(3): 311-317.

[作者简介]



李滢东（1982- ），男，博士，北京交通大学教授，主要研究方向为大数据分析与安全、机器学习、智能交通系统等。



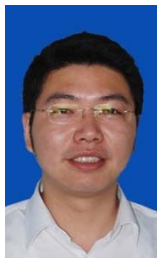
王伟（1976- ），男，博士，北京交通大学教授，主要研究方向为网络与系统安全、工业互联网安全及区块链安全等。



张俊（1981- ），男，博士，武汉大学教授，主要研究方向为智能系统、人工智能、知识自动化及其在智能电力和能源系统中的应用。



顾元祥（1951- ），男，爱迪德公司高级技术顾问，中国西北大学客座教授，主要研究方向为软件安全和保护及人工智能的安全。



陶耀东（1981- ），男，博士，北京交通大学特聘教授、工业互联网安全研究中心主任，主要研究方向为工业互联网安全、数控技术、嵌入式系统等。



王飞跃（1961- ），男，博士，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主任，中国科学院大学中国经济与社会安全研究中心主任，青岛智能产业技术研究院院长，主要研究方向为平行系统的方法与应用、社会计算、平行智能以及知识自动化。

Chinese Journal of Intelligent Science and Technology

Vol.2 No.2 June 2020

Contents

Review Intelligence

- Reinforcement learning: toward action-knowledge merged intelligent mechanisms and algorithms
..... *WANG Fei-Yue, CAO Dongpu, WEI Qinglai* (101)

Surveys and Prospectives

- The application of deep learning in data-driven modeling of process industries
..... *YUAN Xiaofeng, WANG Yalin, YANG Chunhua, GUI Weihua* (107)
- Brain abnormalities in depression based on multimodal imaging
..... *LI Shan, LI Yongchao, ZOU Ying, YANG Lin, WANG Yin, YAO Zhijun, HU bin* (116)

Papers and Reports

- An intelligent optimization scheduling method for community patrolling and investigation in epidemic situations
..... *CHEN Xin, WU Jiayu, WU Xue, ZHANG Minxia, ZHENG Yujun* (126)
- A novel blockchain-based surveillance and early-warning technology for infectious diseases
..... *OUYANG Liwei, YUAN Yong, ZHENG Xinhua, ZHANG Jun, WANG Fei-Yue* (135)
- Fusion of discourse structural position encoding for neural machine translation
..... *KANG Xiaomian, ZONG Chengqing* (144)
- Research on certificate information authentication method of expressway toll based on blockchain technology
..... *LIU Xiaoming, SHANG Chunlin, ZHANG Jie, CHEN Jie, WEI Xiangda, ZHU Guiqing* (153)
- Research on path curvature smoothing method based on energy function for intelligent vehicles
..... *SHI Qiang, YANG Ming* (161)
- Research on data-driven modeling for photovoltaic characteristics based on hybrid neural network
..... *ZHANG Guobin, WANG Xinying* (169)
- A fuzzy system optimization modeling method based on improved genetic algorithm and support degree
..... *DU Hongqing, CHEN Dewang, HUANG Yunhu, ZHU Fenghua, LI Lingxi* (179)
- Dynamic optimization algorithm of cement firing system based on differential evolution
..... *HAO Xiaochen, JI Yakun, ZHENG Lizhao, SHI Xin, ZHAO Yantao* (186)
- Parallel security: generative adversarial systems for intelligent security in CPSS
..... *LI Yidong, ZHANG Jun, TAO Yaodong, WANG Wei, GU Yuanxiang, WANG Fei-Yue* (194)

收录声明

本刊对发表的文章, 拥有出版电子版、网络版版权, 并拥有和其他网站交换信息的权利。本刊支付的稿酬中已经包含上述费用。

Chinese Journal of Intelligent Science and Technology has the copyright to publish electronic edition, online edition of the published articles, and has the right to exchange information with other sites. The expenses have been included in the fee paid by editorial department.

道德声明

本刊发表的论文是作者独立取得的原创性研究成果, 无一稿多投; 论文内容不涉及国家机密; 未曾以任何形式用任何文种在国内外公开发表过; 论文内容不侵犯他人著作权和其他权利。若发生一稿多投、侵权、泄密等问题, 论文作者将承担全部责任。

The authors of *Chinese Journal of Intelligent Science and Technology* guarantee that their submitted articles are original and contain nothing confidential. The said article is only submitted to *Chinese Journal of Intelligent Science and Technology*. The said article has not been published before and has not been submitted elsewhere for print or electronic publication consideration. The said article is no way whatever a violation or an infringement of any existing copyright or license from the third party. Otherwise, the authors of the said article shall take the blame for the violation or infringement of the related copyright and the leakage of secrets.