

智能软件定义网络*

李可欣¹, 王兴伟¹, 易波¹, 黄敏², 刘小洁¹

¹(东北大学 计算机科学与工程学院, 辽宁 沈阳 110169)

²(东北大学 信息科学与工程学院, 辽宁 沈阳 110819)

通讯作者: 王兴伟, E-mail: wangxw@mail.neu.edu.cn



摘要: 近年来,人工智能(artificial intelligence,简称 AI)以强劲势头吸引着学术界和工业界的目光,并被广泛应用于各种领域.计算机网络为人工智能的实现提供了关键的计算基础设施,然而,传统网络固有的分布式结构往往无法快速、精准地提供人工智能所需要的计算能力,导致人工智能难以实际应用和部署.软件定义网络(software defined networking,简称 SDN)提出集中控制的理念,中央控制器能够按需快速地为人工智能适配计算能力,从而实现其全面部署.将人工智能与 SDN 网络相结合,实现智能化软件定义网络,既可以解决棘手的传统网络问题,也能够促进网络应用创新.因此,首先研究将人工智能应用于软件定义网络所存在的问题,深入分析基于人工智能的 SDN 的优势,说明软件定义网络与人工智能结合的必要性.其次,自底向上地从 SDN 的数据平面、控制平面和应用平面角度出发,思考了不同网络平面与人工智能的结合.通过描述智能化软件定义网络的相关研究历程,介绍了智能软件定义网络在路由优化、网络安全和流量安全这 3 个方面的关键技术和所面临的挑战.最后,结合其他新兴领域说明智能软件定义网络的优势和前景,并对未来研究工作进行了展望.

关键词: 软件定义网络;人工智能;流量预测;网络安全

中图法分类号: TP309

中文引用格式: 李可欣,王兴伟,易波,黄敏,刘小洁.智能软件定义网络.软件学报,2021,32(1):118-136. <http://www.jos.org.cn/1000-9825/6120.htm>

英文引用格式: Li KX, Wang XW, Yi B, Huang M, Liu XJ. Survey of intelligent software defined networking. Ruan Jian Xue Bao/Journal of Software, 2021, 32(1): 118-136 (in Chinese). <http://www.jos.org.cn/1000-9825/6120.htm>

Intelligent Software Defined Networking

LI Ke-Xin¹, WANG Xing-Wei², YI Bo¹, HUANG Min², LIU Xiao-Jie¹

¹(School of Computer Science and Engineering, Northeastern University, Shenyang 110169, China)

²(School of Information Science and Engineering, Northeastern University, Shenyang 110819, China)

Abstract: In the past few years, artificial intelligence (AI) has attracted the attention of both academia and industry with strong momentum and has been widely utilized in various fields. Computer networks provide critical computing infrastructure for the realization of AI. However, it is inefficient to provide AI with computing power in a fast and accurate manner, because of the inherently distributed structure of traditional networks, and it results in the difficulty in practical application and deployment. Software defined networking (SDN) proposes the concept of centralized control, which adapts computing capability for AI on demand and thereby can achieve comprehensive deployment. Combining AI and SDN to realize intelligent software defined networking can not only solve problems of traditional network but also promote network application innovation. Therefore, this paper introduces the problems which exist in the scenario where combining AI and SDN, explains the necessity of SDN based on AI, and analyzes the advantages of combining SDN with

* 基金项目: 国家重点研发计划(2019YFB1802800); 国家自然科学基金(61872073); 辽宁省“兴辽英才计划”资助项目(XLYC1902010)

Foundation item: National Key Research and Development Program of China (2019YFB1802800); National Natural Science Foundation of China (61872073); Liaoning Revitalization Talents Program of China (XLYC1902010)

收稿时间: 2019-07-27; 修改时间: 2019-10-29; 采用时间: 2020-01-19; jos 在线出版时间: 2020-07-27

AI. Secondly, from the bottom up, the different combination cases of AI and SDN are considered which include data plane, control plane, and application plane. Besides, the challenges and key technologies are introduced from three aspects: routing optimization, network security, and traffic engineering. Furthermore, the advantages and prospects of the intelligent software defined networking are analyzed via combining other emerging fields comparison, and some future research works are outlined.

Key words: software defined networking; artificial intelligence; traffic prediction; network security

近年来,随着智能设备和网络技术的快速发展,用户基数的指数级增加导致全球数据流量呈爆炸式增长.为了优化越来越复杂的大规模流量分配问题,网络变得更加异构和复杂.异构和复杂的网络基础设施增加了网络的复杂性,对有效组织、管理和优化网络资源提出了诸多挑战.为了解决上述问题,并且不破坏转发平面的开放性和透明性,提高管理网络方法的智能化,David 等人提出一种知识平面(knowledge plane,简称 KP)思想^[1],通过应用认知技术,将自动化、推荐和智能思想(如人工智能、机器学习)引入互联网,实现算法、策略、目标的分离以及创新的模型表示方式.然而,传统网络系统的分布式特点导致网络无法全局控制,因此考虑软件定义网络(software defined networking,简称 SDN)以降低其复杂性^[2].SDN 为弥补传统网络架构控制平面与数据平面紧密耦合、控制不足的特点,将控制平面单独解耦出来,实现与数据平面的分离^[3].数据平面仅负责路由转发,控制平面则实现转发决策.应用平面为用户提供网络可编程服务,管理人员可以按照自己的意愿控制转发,实现网络数据流的通用转发和高效操纵,从而增加网络的灵活性.

SDN 为了有效地检测和管理网络提供了具有前景的技术支持.最近,人工智能技术广泛应用于 SDN 网络安全、流量工程等领域,随着研究的不断深入,研究者们发现:可以利用大数据的相关算法提高 SDN 运营效率,并降低运营成本^[4,5].同时,SDN 作为一种重要的网络范式,利用其解耦数据与控制平面、逻辑集中控制、网络全局视图、网络编程能力等特点,可以极大地促进大数据的采集、传输、存储和处理^[6,7].大数据在运用网络规划与优化方面的技术优势充分应用在 SDN 路由、流量、控制器等方面,可以极大地提高 SDN 的运行效率^[10,11].与传统网络的数据中心相比,基于 SDN 的数据中心可以通过将数据中心资源动态分配到不同的大数据应用程序,以满足这些大数据应用程序的服务水平协议(service level agreement,简称 SLA),从而获得更好的性能^[8,9].众所周知,人工智能技术的提出基于大数据背景,SDN 与大数据结合的成功,保证了基于人工智能的 SDN 的发展.

人工智能技术可以利用 SDN 控制器的全局控制能力以使得网络更易于控制与管理,并分别与 SDN 的数据平面、控制平面和应用平面相融合,使 SDN 流量分类预测、网络优化和网络安全等方面更加智能,进而使得 SDN 网络能够自动地智能处理分析数据.从宏观角度来看,云计算、边缘计算以及其他大数据技术的成型,确立了人工智能应用于软件定义网络在处理大规模、时间空间复杂度较高的路由及流量工程等问题的优势.相较于传统的 SDN 网络,基于人工智能的 SDN 不仅具备了快速处理大规模数据的能力,更重要的是继承人工智能特征而具备学习能力,使网络更具备灵活性.本文将从以下几个方面继续讨论基于人工智能的 SDN 网络要面临的挑战.

(1) 海量数据

SDN 被认为是可以通过适当的网络管理,彻底改变网络世界的最有前途的解决方案之一.SDN 架构下的流量工程可以利用 SDN 集中控制的优势,通过动态分析,预测和调节通过该网络传输的数据的行为,平衡网络负载和最大化网络利用率,以优化网络性能.但是,随着网络数据规模的不断扩大,数据的维度和复杂性也在增加,传统的 SDN 亟需攻克海量数据带来的技术瓶颈.

(2) 流量分类

传统的流量主要包括基于端口、深度包检测和人工智能等分类方法,随着应用程序的增多,且端口变为动态端口,导致传统的基于端口的流量分类方法失效.深度包检测方法大多采用对正则表达式的匹配实现数据包的识别,但两种实现方式——不确定性有限自动机(non-deterministic finite automata,简称 NFA)和确定性有限自动机(deterministic finite automata,简称 DFA)都存在一定的局限,其中,NFA 占用空间小,但匹配时间长;DFA 则反之,且存在状态爆炸隐患.因此,现在主要流量分类的方法基本集中在使用各类人工智能方法上.尽管人工智能方法能够有效地对流量进行分类,但是随着应用数据的增多和形式的改变,对算法训练的时间和空间复杂度也有了更高的要求.

(3) 路由优化

在 SDN 网络中,控制器可以通过修改交换机中的流表来控制流量的路由.控制器负责计算每个新流的路由策略,但目前,路由优化方法绝大多数以启发式算法为主,但启发式算法会给控制器带来计算负担,而人工智能算法由于其无需底层网络的精确数学模型,且经过训练能够快速给出接近最优的路由解决方案,因此,利用人工智能方法构建稳定、鲁棒的模型,满足 SDN 网络路由实时、准确的优化方法是未来的研究热点.

(4) 网络安全

在 SDN 网络中,通过应用大数据及人工智能的相关算法,可以有效地预防并解决 SDN 网络安全的部分问题.首先,利用大数据的各种有效方法获取网络中各项数据,通过分析各项数据检测网络数据异常,进行实时网络安全对抗,并进行有效的安全预防威胁;其次,构建多维到超高维数据模型,在线准确地分析数据流,实现实时检测以及预防攻击.利用有效的人工智能智能方法,例如回归分析、支持向量机等,可以分析网络历史数据,对历史数据中的攻击类型进行分类.但是,网络安全问题仍要面临时效性以及不可复用问题,网络攻击与防护是一个博弈过程,在对手之前找到棋局的下一步,是赢得网络攻防博弈的关键.

本文第 1 节分别从人工智能与 SDN 入手,详细讨论基于人工智能的 SDN 网络,从 SDN 的 3 层架构——数据平面、控制平面和应用平面角度详细描述人工智能的应用,并描述基于人工智能的 SDN 下的应用场景及标准化定义.第 2 节从路由优化、网络安全和流量工程这 3 个方面讨论基于人工智能的 SDN 当前面临的挑战和关键技术.最后一节讨论基于人工智能的 SDN 未来所面临的挑战及其与其他领域结合的发展趋势.

1 研究现状和动机

1.1 SDN 现状

随着网络规模的不断扩大,互联网流量的增长速度不断提高,用户对流量的需求发生改变,可编程网络产生了一种解决网络复杂问题的思想.研究人员依托这种可编程思想,相继提出转发抽象、分布状态抽象和配置抽象的概念^[12],将传统网络中交换机的控制功能解耦出来,由控制平面完成,在此基础上增加连接数据平面与控制平面的标准接口,仅保留交换机识别交换数据的功能.控制平面抽象全网分布设备的全局视图,综合全网信息,使应用平面的应用基于全网信息进行网络的统一配置.与此同时,用户仅通过控制平面提供的接口进行简单配置,就可以自动完成沿路径转发设备的统一部署.因此,网络中的数据转发路径不再依赖于数据平面,而产生了数据平面与控制平面解耦且接口标准统一的软件定义网络架构^[13].

软件定义网络的优势在于转发与控制的分离、支持软件可编程以及网络状态集中控制,目前已在网络虚拟化^[14]、数据中心网络^[15]、无线局域网^[16]和云计算^[17,18]等领域得到广泛应用.SDN 将传统网络联系十分紧密的各个平面解耦为数据平面、控制平面和应用平面,使控制与管理集中得到逻辑上的支持,并且结构灵活且易于管理.图 1 所示为 SDN 的架构.

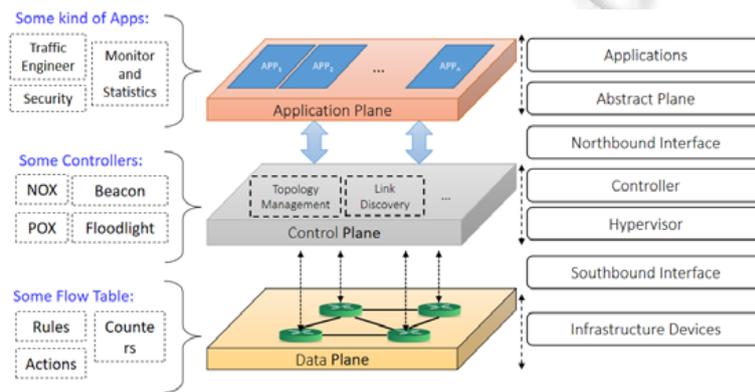


Fig.1 SDN architecture

图 1 SDN 架构

如图 1 所示,SDN 架构从上至下分别包括应用平面、控制平面和数据平面.应用平面体现用户意图,用户可以根据本身意图以及实际需求开发应用程序.在应用平面,开发人员通过收集例如拓扑状态、网络统计等网络数据,开发网络可视化应用以及网络自动化相关应用,这些应用程序可以根据实际需求提供端到端的解决方案.应用平面与控制平面通过北向接口连接,北向接口允许用户按实际需求定制开发.目前,大部分传统的北向接口开发基于为现有设备提供编程接口,以便于业务应用调用.控制平面负责管理底层物理网络,可以根据需求灵活地控制控制器,通过获取和维护不同类型的网络信息、拓扑结构信息等保证网络的稳定,是网络系统的控制中心.市场上基于 SDN 控制器的解决方案可分为商业方案和开源方案:商业方案由大型网络设备厂商提供,例如思科公司提供的 Cisco Open SDN controller、NEC 公司开发的 PFC SDN controller 以及 Brocade SDN controller 等;开源方案一般由社区组织提供,由于系统开源受到个人用户的广泛使用,目前较为优秀的开源方案包括 Ryu、OpenDaylight、Floodlight 等等,典型的控制器对比见表 1.控制平面负责物理层的交换机的实现,交换机最初为硬件形式,随着虚拟化技术的不断发展,软件交换机(open vswitch,简称 OVS)克服硬件交换机的发展瓶颈,同时具备虚拟化集成与交换机的功能,支持多个物理机的分布环境,基于开源技术实现虚拟化组网.目前,OVS 支持 NetFlow、sFlow 等传统的标准管理接口.南向接口连接控制平面和数据平面,许多组织着手南向标准接口的标准化制定,例如,开放网络基金会(Open Networking Foundation,简称 ONF)提出采用 OpenFlow 协议^[19],除此之外,还包括国际互联网工程任务组(the Internet Engineering Task Force,简称 IETF)定义的可扩展消息处理现场协议(extensible messaging and presence protocol,简称 XMPP)等其他协议.OpenFlow 的产生打破了 SDN 硬件市场的壁垒,使应用可以通过软件的形式与 SDN 控制器通信传输数据.数据平面包括各种基于软/硬件实现的基础设备,通过南向接口接收来自上层的各项指令,根据上层的指令处理网络数据,并将处理数据结果指令以及运行时间等信息通过南向接口反馈至上层.

Table 1 Comparison of controllers

表 1 控制器对比表

| 控制器 | 语言 | 创建者 | OpenFlow 版本 |
|--------------------|------------|---------------------|-------------|
| NOX/POX | Python,C++ | Nicira | 1.0,1.3 |
| ONIX | - | Google,Nicira | - |
| Beacon | Java | Stanford university | 1.0.1 |
| Maestro | Java | Rich university | 1.0 |
| Floodlight | Java | Big switch networks | 1.0 |
| Floodlight-plus | Java | Big switch networks | 1.3 |
| Ryu | Python | NTT labs | 1.0~1.4 |
| (ODL)Open daylight | Java | Linux foundation | 1.0,1.3 |

模拟器可以模拟创建一个支持 SDN 的网络,经过以太网端口的数据包,被交换机、路由器接收并处理,实现网络模拟过程.目前,很多网络的模拟实验都基于此来进行.模拟网络能够为网络添加新的功能并进行相关测试,然后根据实验结果,将相应的功能部署到真实的硬件环境中.表 2 给出目前存在应用较广泛的模拟器的介绍.

Table 2 Comparison of SDN simulators and emulators

表 2 模拟器对比表

| 模拟器 | 是否开源 | 语言 | 平台 | OpenFlow 版本 |
|------------------------------|------|-----------|-----------------|--|
| Mininet (simulator) | Yes | Python | BSD open source | OF 1.3 of the reference user switch and NOX from CPqD and Ericsson |
| NS-3 (simulator) | Yes | PythonC++ | GNUGPLv2 | Pre OF 1.0 and version of OF-SID that support MPLS |
| EstiNet (emulator/simulator) | Yes | - | - | OF 1.3 and 1.0 |

1.2 人工智能现状

人工智能自 1956 年在 Dartmouth 学院的一次小组会议上被提出之后,经过几十年的发展,其思想深刻地影响了人类科学,并广泛应用于图像识别^[20]、自动驾驶^[21]、模式识别^[22]、计算机视觉^[23]等领域.

1940s~1970s 期间是人工智能的第一次浪潮,当时的人工智能仅处理一些特定问题,例如游戏规则、知识表

达及推理、专家问题等等,这些问题的开发框架都基于特定任务,仅适应于特定场景.典型的例子是由 IBM 公司开发的象棋电脑深蓝计算机,它采用混合决策的方法,计算出可能的棋步和结果.超级计算机根据这些结果决定最终的棋步.尽管深蓝计算机当时已经能够推测 4~6 步棋局,但由于其启发式算法的高度复杂性以及不能应用于国际象棋以外的任何场景,很难处理大规模数据.随着数据规模的扩大,传统的人工智能方法已经不能满足人类对于特定场景之外的应用要求,因此,研究人员侧重于从观测数据中提取规则,相应地产生了自然语言处理(natural language processing,简称 NLP)^[24]、计算机视觉(computer vision,简称 CV)^[25]、统计机器学习(statistical machine learning,简称 SML)^[26]等技术.从那时起,机器学习下的监督学习^[27]、非监督学习^[28]以及半监督学习^[29]成为人工智能领域的研究重点,这些技术至今仍然是人工智能领域应用范围最广泛、结合最紧密的算法.例如,2009 年,卡耐基梅隆大学的 Carlos Guestrin 启动的开源项目 GraphLab 提供了包括多核和分布式应用程序编程接口(application programming interface,简称 API)在内的强大特性^[30],其优势在于,GraphLab 包含主题模型、图分析算法、图形模型、聚类算法、协同过滤算法等.GraphLab 等框架使得统计机器学习模型更容易应用于特定的人工智能问题,但它需要大量的数据来驱动统计机器学习算法.

深度学习算法的提出,不仅引发了深度学习在研究和应用领域的热潮,同时标志着人工智能进入第三次浪潮^[31].至今为止,深度学习被广泛应用到语音识别^[32]、图像识别与处理^[33]、自然语言处理^[34]等领域.例如,微软公司推出的基于深度神经网络的语音识别系统,突破了已有的语音识别框架,将原来的语音识别错误率降低了 20%~30%.

1.3 基于人工智能的SDN各平面动机研究

人工智能初步应用于 SDN 时期,仅能处理路由、安全、架构等方面的小规模、时间复杂度低的场景.传统的 SDN 将控制平面与转发平面分离,交换机通过标准接口接收控制器下发的统一标准规则,执行相应的动作即可.但是传统的 SDN 工作模式已经无法满足当今大数据时代下大规模、结构复杂的流量,更不可能根据流量数据的自身情况制定相应的规则,实现智能网络调配.因此,许多研究人员致力于增加 SDN 路由、安全以及架构等方面更大规模、更加智能化的工作^[35].本节总结目前人工智能应用于数据、控制以及应用这 3 个平面的相关研究,并分析其优劣,证明人工智能可以应用于 SDN 各个平面并产生具有优势的效果.

1.3.1 数据平面

数据平面相关技术研究包括两个方面:交换机设计研究和转发规则研究.交换机设计研究包括设计可扩展的快速转发设备,实现设备在灵活匹配规则的基础上能够快速转发数据流;其次是转发规则的相关研究,包括考虑解决突发情况的转发规则,例如规则失效后的一致性更新问题等.

交换机分为硬件交换机和软件交换机,惠普、思科、华为、H3C 和瞻博这五大公司占据了全球硬件交换机市场的绝大份额.监管硬件交换机能够存储增加数据转发的速率,但是,如果过分依赖硬件交换机,会使网络升级速率过慢、成本较高;并且这些技术被大公司所垄断,将产生一个相对封闭的市场,新生力量难以生存,市场缺少创新性和竞争力,阻碍了网络设备产业的发展.因此,着重发展软件交换机,将一些在软件上实现的服务从硬件交换机转移到软件上,不仅可以降低成本,而且使网络配置更加灵活,从而打开了硬件厂商垄断市场的壁垒.国际软件交换机论坛给出如下定义:软件交换机是基于分组网利用程控软件提供呼叫控制功能的设备和系统,能够提供更多的数据包处理方式.但在增加新功能时,却存在代码量巨大、需要修改内核以及极其依赖修改人员的专业知识等缺陷,因此,研究者们又提出许多新的分组方案以提升交换机性能.Rahimi 等人^[36]开发了一个名为 Netmap 的新的数据包 I/O 框架,并通过在 Netmap 上运行 OVS,比较了 OVS、IP 转发、Linux 桥接器和 DPDK vSwitch 的性能.

基于数据平面转发规则的研究方向主要包括两方面:开发新的南向接口协议^[37]或提出智能协议.SDN 控制平面与数据平面分离,给网络管理提供统一的编程接口,并使网络更加灵活.但是上述控制平面与数据平面分离的方式需要借助 OpenFlow 交换机和控制器之间频繁交互各种控制器南向接口消息,过于频繁的信息交互,给控制器的处理能力、数据通路处理时延、南向接口的信道带宽等性能提出很高的要求.Zheng 等人^[38]提出一种基于流量特征的正南向接口技术,针对网络流量分布不均衡的特征,重点关注仅占据少量网络带宽但却种类繁多的

小流,消除了冗余路径,降低了传输时延,优化了控制器南向接口交互开销。Ba 等人^[39]研究发现,具有树状拓扑的数据中心网络存在类似的问题,他们提出一个网络范围的电源管理器和若干相关启发式算法,动态打开/关闭网络元素,以满足不同的流量负载。但是上述对于协议的研究仅限于启发式算法,启发式算法虽然在一定程度上可以对路由或流量起到智能控制的作用,但却增加了数据平面的计算负担,因此,基于数据平面的各种算法仍须考虑日益增长的数据规模,通过降低计算复杂度来节约能耗。

1.3.2 控制平面

控制平面是整个网络的大脑,其核心组件是控制器,控制器逻辑上集中控制交换机,快速转发网络数据,利用全局视图安全管理网络,提升网络的整体性能。目前,对于控制器的研究大致分为如下几个方面。

- a) 分布控制器研究。单一集中控制存在单点失效问题,限制网络的伸缩性;另一方面,在大规模网络中,单一集中控制在其他域与交换机之间存在的延迟处理问题略显乏力,因此,大多采用分布式控制器解决上述问题;
- b) 控制器安全研究。控制器是 SDN 网络的核心,从安全角度来看,SDN 网络架构的集中性和开放性在提高整个网络灵活性的同时,也为 SDN 网络安全带来巨大的隐患。传统 SDN 控制器安全防护的方法大多采用基于 OpenFlow 流进行流量监控和入侵检测,利用 SDN 的优势实现算法的改善和性能的优化。但是,以上方法都忽略了历史数据蕴含的安全信息,也无法预防未来安全攻击。通过引入人工智能算法,可以构建 SDN 网络安全模型,实现控制平面的智能优化。

由于网络状态与人类的行为规律密切相关,因此可以通过人工智能技术对网络覆盖、用户分布、业务等人类行为特点进行综合分析,预测流量负载,提高带宽利用率,降低网络损耗,实现全网负载均衡。例如,Tang 等人^[40]提出一种新的基于深度学习的流量负载预测算法,用于预测未来网络中的流量负载和堵塞,并在此基础上,结合深度学习的信道分配算法(deep learning based partially channel assignment algorithm,简称 DLPOCA)解决信道智能分配到 SDN-IoT 网络中的各个链路问题,智能地避免潜在的拥塞,快速地在 SDN-IoT 中分配合适的信道。Leguay 等人^[41]通过探究 SDN 与机器学习的一些算法,发掘 SDN 运行计算密集型机器学习工具,并以集中方式解决复杂优化问题的潜力。另一方面,通过在控制平面引入人工智能技术,可以根据历史数据对攻击者和合法用户进行分类,并根据其特点有效识别攻击者,有效保障 SDN 控制平面安全。Nanda 等人^[42]提出在 SDN 控制器定义安全规则,使用机器学习算法根据历史网络攻击范例,预测将要被攻击的主机,通过阻塞整个子网来限制潜在攻击者的访问。但是目前,应用于控制平面基于人工智能网络安全方法中仍缺少实时反馈对攻击评估的考虑,仅针对历史数据不能准确识别新的攻击进行了分析。

1.3.3 应用平面

SDN 的应用平面包含若干个应用,这些应用可以通过可编程方式,通过北向接口把需要请求的网络行为提交给控制器。基于应用平面的研究大体分为开发北向接口和开发 SDN 应用。传统网络开始思考动态灵活的流量问题最早可追溯到对 Google B4 架构的描述^[43],该架构提供数据中心间的网络连接,具体负责同步数据复制、交互服务系统的推送索引以及计算用户数据的可用性副本等工作,但是该架构仍然无法有效地处理动态流量问题。人工智能的相关技术结合 SDN,可以很好地解决上述问题。例如,Shi 等人提出一种基于深度学习的流量鲁棒最优的新特性优化方法和特征选择算法^[44],该方法利用删除网络流量数据集中无关的特性来保证对称性,然后,基于深度学习生成应用于该特征的相应模型。但是互联网流量具有复杂非线性特征,现有的特征选择(feature selection,简称 FS)技术对流量分类不具有很强的鲁棒性,不能可靠地为机器学习(machine learning,简称 ML)算法提供最优、最稳定的特征保证。为了解决上述问题,Shi 等人在现有算法的基础上提出一种新的特征提取和选择方法^[45]:首先,利用小波前导多重分形形式化,从流量流中提取多重分形特征来描述流量流;然后,将基于主成分分析的 FS 方法应用于这些多重分形特征,去除不相关和冗余特征后,得到需要的特征。其他研究包括通过比较贝叶斯网络、决策树和多层感知器等方法不同类型的互联网流量和内容交付流量进行基于流的分类,调查不同的流量分类性能所依赖的训练数据量,得出贝叶斯网络和决策树等适合互联网高速流量分类的结果^[46,47]。

1.4 基于人工智能的SDN标准化历程

目前,开放网络基金会 ONF、欧洲电信标准化协会(European Telecommu-Nications Standards Institute,简称 ETSI)、国际互联网工程任务组(the Internet Engineering Task Force,简称 IETF)等标准化组织以及思科(CISCO)公司都在致力于基于人工智能的 SDN 相关技术的标准化制定,这些标准化组织的侧重点不尽相同,从不同的角度出发对 SDN 标准化加以定义。

1.4.1 开放网络基金会

ONF 组织由 Google、德国电信、Yahoo 等组成,该组织联合发起致力于推动 SDN 和 OpenFlow 技术标准化与商业化的研究.ONF 是一个用户驱动的组织,致力于通过开放标准开发来推广和采用 SDN.ONF 强调从最终用户角度出发的开放式协作开发流程,并介绍 OpenFlow 标准,该标准可实现转发平面的远程编程。

ONF 工作组分析 SDN 要求,发展 OpenFlow 标准以满足商业部署的需求,并研究新标准以扩展 SDN 的优势.技术社区分为区域、理事会和小组.区域处理与 SDN 相关的特定问题,并与 SDN 和 OpenFlow 标准方面的世界领先专家就 SDN 概念、框架、架构、软件、标准和认证进行合作;理事会在组织的战略、运营执行和技术方向等方面提供全面的领导;小组为有助于实现组织目标的活动提供指导和建议.截止 2019 年末,ONF 组织的工作进展可见表 3.

Table 3 Progress of SDN by ONF

表 3 ONF 组织关于 SDN 工作进度

| 分类标准 | 主要职责 | 进展情况 |
|----------------------|---|--|
| 技术规范 | OpenFlow 相关标准作为技术规范发布,可能包括协议定义、信息模型、组件功能和相关框架文档 | 2017 年 6 月发布 SPTN OpenFlow 协议扩展; 2017 年 4 月发布光传输协议扩展协议; 2015 年 4 月发布 OpenFlow 交换机规范 1.5.1 版本 |
| 技术建议 | 包括定义 API、数据模型、协议、信息模型等所有标准.技术建议是 ONF 的规范性文件 | 2018 年 11 月发布核心信息模型; 2018 年 10 月发布设备管理接口配置文件和要求; 2013 年 3 月发布 OpenFlow 配置和管理协议 1.1.1 |
| 书面文件(白皮书、用例、解决方案简报等) | 有助于进一步开展 ONF 使命和开放网络解决方案开发和/或部署的出版物 | 2016 年 9 月发布可协商的数据路径模型和 TTP 签名; 2016 年 9 月发布 ONF SDN Evolution |

由于 OpenFlow 通过显式地声明协议头部来表明可以处理的操作,OpenFlow 由于协议结合头部增加会导致系统复杂性提高、灵活性降低等情况.为解决上述问题,ONF 提出了 P4 概念.P4 是一种高级语言,用于编写与协议无关的包处理器,具有以下优势:协议独立,P4 程序指定交换机如何处理数据包;目标独立,P4 适用于描述从高性能转发 ASIC 到软件交换机的所有内容;字段可重新配置,P4 允许网络工程师在部署后更改交换机处理数据包的方式.因此,有人称 SDN 是网络的未来,P4 是 SDN 的未来.2018 年 12 月,ONF 召开的“Next-Gen SDN Track”中提出 P4 与机器学习相结合^[48],可以丰富网络获取数据.例如,传统网络仅可获取出入节点信息以及路间延迟,引入 P4INT(in-band telemetry)技术可以获取 Collector ID、Sequence number、Time stamp、Switch ID、Ingress port、Egress port、Hop latency 等信息.通过获取上述信息,可以理解数据是否能够通过机器学习技术预测网络性能,比较 P4INT 的预测结果与传统预测结果,并利用上述预测结果修正循环决策.

1.4.2 欧洲电信标准化协会

ETSI 是独立的非赢利性的欧洲地区性信息和通信技术标准化组织,由 55 个国家的 688 名成员组成,其宗旨是为贯彻欧洲邮电管理委员会和欧共体委员会确定的电信政策,满足市场各方面及管制部门的标准化需求。

ETSI 的行业规范组(industry specification group,简称 ISG)提出将人工智能技术应用于网络管理系统中,以解决未来基于经典的 OODA(observe-orient-decide-act)模型的网络部署和运行中存在的一些问题,使系统能够根据用户需求、环境条件和业务目标的变化等参数,适应调整网络配置以及管理开放智能功能的服务,以推动行业整体管理下的智能决策能力.以上过程被称为体验网络智能(experiential networked intelligence,简称 ENI)^[49].ENI 的目的是定义一种结合人工智能技术和上下文感知元数据技术的架构,基于 OODA 控制回路模型^[50],根据用户需求等变化,为推动决策调整所提供的服务.该模型的主要挑战包括:适应复杂的人控自动化决

策过程;确定提供能够满足服务水平协议(service-level agreement,简称 SLA)的服务,并将其作为环境变化的函数;定义如何最好地可视化提供和管理网络服务,以改进网络维护和操作;提供体验式架构(即结合人工智能架构)和其他机制来提高其对环境与经验的理解.该模型可以帮助决策系统,如网络控制和管理系统,根据用户需求、环境条件和业务目标的变化调整所提供的服务和资源.

自 2017 年 2 月开始以来,ISG 一直在指定一组用例,通用技术无关的系统架构的派生要求,对 ENI 在情境感知和基于决策的标准方面的工作进行差别分析.ISG 同年指定使用 AI 机制来学习和制定决策的高级架构,并且建立了用于创建一个或多个概念证明(proofs of concept,简称 PoC)的工作项.

1.4.3 国际互联网工程任务组

国际互联网工程任务组 IETF 是一个公开性质的大型民间国际团体,主要任务是负责互联网相关技术标准的研发和制定,是国际互联网业界具有一定权威性的网络相关技术研究团体.

2017 年,IETF 提出了关于人工智能驱动网络(intelligence driven network,简称 IDN)草案^[51],明确 IDN 的工作范围,挖掘潜在的标准化工作.草案中首先分析了现有方法存在的问题,例如数据结构问题.目前,人工智能算法的输入和输出可以是数值矩阵或向量,但是网络数据不是完全格式化和规则的,它们需要在算法前后进行翻译或转换.因此,将网络数据完全与人工智能算法相结合需要解决数据格式、数据编制等方面的不足.另一个问题是基于人工智能的预测和自主决策应该是一个快速的反应过程,整个过程应尽可能地避免拥塞的发生,若时间较长,则人工智能算法应用于网络毫无意义.因此,草案围绕如何实现这样的快速反应问题提出一系列解决方案.草案随后提出一种基准框架设计方法,该方法在机器学习和推理过程中具有重要意义.最后提出了 IDN 的 3 层参考模型,该体系结构可以覆盖、解释和支持大多数当前用例和场景,并在此基础上分析了潜在的标准化工作.

1.4.4 思科

思科(CISCO)公司凭借对网络经济模式的深刻理解和先进的技术,成为全球顶尖的网络解决方案供应商,其宗旨是为全球市场提供具有战略性的、富于创新的、高品质的技术和产品.

2019 年 10 月,思科公司举行全球在线活动“Networking.Next 联网未来”,基于第三方机构 IDC 的调研结果发布思科《2020 年全球网络趋势》.该报告中描述思科公司数字网络就绪模型建立的趋势为最开始信息时代的人工运营孤岛至端到端管理、人工运营,直至现在基于软件定义网络实现在每个域基于控制器的策略自动化,在此基础上,结合人工智能等其他技术,实现在每个域满足业务需求,甚至最后跨所有域持续满足动态的业务需求.报告中着重指出:在过去的业务处理上,SDN 在自动化方面为业务提供持续性的服务性能和保护起到至关重要的作用.但在业务后续工作中,网络公司仍需要对网络进行持续的网络监控和优化,SDN 网络自身无法提供支持日益动态并以数字驱动的业务模式.因此,必须了解不断变化的业务意图,并对动态的网络状况进行监控,这样才能不断顺应需求.基于意图的网络可捕获业务的意图,并使用分析、机器学习、机器推理和自动化使网络持续、动态地适应不断变化的业务需求,同时适应不断变化的网络负载和其他环境影响.这可能意味着,要在整个网络中不断应用并保障服务性能要求及用户、安全、合规性和网络技术运营策略^[52].

2 关键技术及研究方法

SDN 日益受到国内外研究组织的关注,人工智能能够在 SDN 集中控制管理的基础上,执行数据分析、网络优化,使管理更加智能.本节将回顾人工智能技术解决 SDN 网络中的具体问题,如智能路由优化、网络安全智能方法以及基于人工智能的流量工程等.下面简要介绍人工智能应用于 SDN 网络具体问题所采用的关键技术及研究方法.

2.1 智能路由优化方法

路由是网络的一项基本功能,在 SDN 网络中,控制器通过修改交换机的流表来控制流量的路由,引导交换机丢弃一个流量或将其路由到指定路径.低效率的路由策略会导致数据丢失、负载不均衡以及资源浪费等情况,因此,优秀的路由策略对于网络数据传输具有重要意义.目前,路由策略大部分基于最短路径优先策略或启

发式算法做出优化或改进.对于智能软件定义网络下的路由研究包括路由策略优化和软件定义路由研究两个方面,本节将从以上两个方面对智能路由优化方法进行简要描述.

2.1.1 策略优化

SDN 是为了解决由于集中管理困难、供应商依赖以及进程改变导致网络复杂增加等问题而提出的.在目前的 SDN 网络中,路由算法多为基于 Dijkstra 算法,选择最短的流路径来传递数据包.但仅考虑路径的长短而不考虑带宽开销等其他参数,会在大量的流量进入网络时导致网络拥塞.为了解决上述问题,研究人员考虑结合人工智能方法规划路由算法.Mhdawi 等人^[53]在中型混合软件定义的网络数据中心环境中开发智能功率降低决策路由协议(intelligent power reduction decision routing protocol,简称 IPRDR),该算法根据计算的公制值,以最优功率路径将大流量路由到高索引设备,并对其聚合和隔离.但该算法并不适用于更大功率情况的优化,无法管理和控制多个传统数据中心站点位置.Kim 等人提出一种基于 Q-learning 的 SDN 高效路由以防止网络拥塞的机制^[54],该方法通过使用预定义的阈值和 Q-learning 路由算法重新选择路径和改变流表,可以极大地改善网络拥塞.但是上述方法仅适用于固定流量生成模式和带宽大小的情况,为了满足更复杂的网络状况,需要考虑更多的复杂、可扩展的因素.Pasca 等人从流量优先级的角度优化路由策略^[55],认为流量应有优先级,率先完成优先级高的流量调度可以有效地避免多个流争抢有限资源的状况.在此基础上,提出一种应用程序感知的多路径转发框架,该框架集成了机器学习和 SDN,使用机器学习算法对每个流进行优先级排序,并使用 SDN 根据流优先级和网络状态将其路由.但是上述算法在执行多路径分配时,未将用户的使用经验和一些 QoS 需求考虑在应用的分类步骤中.随着无线网络的发展,无线骨干网中路由方法等高效的网络流量控制成为一个关键性的挑战^[56],这是因为传统的路由协议没有从历史经验中学习网络异常,如拥塞等,因此智能网络流量控制方法是解决此类问题的关键.针对这一问题,Mao 等人提出一种新的基于实时深度学习的智能网络流量控制方法,利用具有独特输入和输出特性的深度卷积神经网络(deep convolutional neural networks,简称 DCNNs)来表示所考虑的无线网状网络(wireless mesh network,简称 WMN)主干网,以降低平均延迟和丢包率^[57].

2.1.2 软件定义路由

互联网核心和有线/无线异构骨干网络的构建方式多年来基本上保持不变,因此本质上,路由器背后的主要算法原理上非常相似.为了适应不断扩大的网络规模,互联网核心数据通过添加更多、更大的路由器和更多的链路而继续扩展.软件驱动的路由策略的进步,似乎总是落后于流行的路由策略,但软件定义路由器(software defined routing,简称 SDR)也称为可编程路由器,它提供了一个具有易扩展性和可编程性的具有成本效益的包处理平台.学术界和行业研究人员对利用 CPU 或 GPU 提供的多核或线程并行操作路由任务以提高处理器的处理吞吐量表现出极大的兴趣,多核平台显著提升了 SDR 并行计算能力,使其能够采用人工智能技术,即深度学习,管理路由路径^[58,59].目前有许多学者致力于 SDR 的研究,例如,Mao 等人采用监督的 DBA 计算后续节点与边缘路由器的流量模式作为输入、基于深度学习的路由表构造方法^[60].仿真实验结果显示,基于深度学习方法的路由方法的确能够极大地改善主干路由的控制.但是,该方法并未考虑网络层的安全问题.Geyer 等人^[61]提出了基于图的深度学习生成分布路由协议方法,与 Mao 等人的方法相比,该方法独立于拓扑的底层结构,因此应用于更广泛的网络拓扑.SDR 为网络设备编程实现不同目标提供了灵活性,并消除了对第三方供应商特定硬件的需求.

2.2 网络安全智能方法

SDN 以中央控制器来管理整个网络,以简化网络管理工作.这种管理机制在为用户提供良好的网络可编程性的同时,也使整个网络的核心暴露在攻击者面前,攻击者仅通过编码的形式就可以访问网络的中心,使 SDN 网络时刻面临攻击的危险,降低了整个网络的安全性.Wang 等人对 SDN 网络安全机制进行了综述^[62],分析归纳了 SDN 中存在的典型的安全威胁问题.他们分别从 SDN 安全控制器的开发、控制器可组合安全模块库的开发和部署、控制器 DoS/DDoS 攻击防御方法、流规则的合法性和一致性检测、北向接口和应用安全性等多个方面详尽地探讨了 SDN 安全.SDN 控制器的全局网络视图简化了网络流量的收集和分析,此外,SDN 的可编程性使网络在检测到攻击时拥有立即做出反应的能力.在 SDN 网络中,基于人工智能的入侵检测已有很多研究,如

入侵检测和 DDoS 攻击检测.以下将对网络安全智能方法研究进行综述.

入侵检测的目的是识别访问是否正常,通过将流量分类为正常流和攻击流,拦截异常访问,保证网络安全.人工智能方法用一组属性和关联标签来说明每个流,基于属性的类型,确定用于异常检测的相关技术.例如, Sanda 等人^[63]利用机器学习算法的预测输出,定义 SDN 控制器的安全规则,以防止恶意用户访问网络.他们分别使用 C4.5、决策表、贝叶斯网络和朴素贝叶斯算法这 4 种机器学习方法,根据历史数据预测攻击的主机.然而,在利用人工智能方法分类访问流的方法中,仅可以解决特定的攻击或提出具体的防御方法,并没有解决检测和控制恶意或可疑流量等基本需求.此外,SDN 控制器中仍存在许多尚未发现的漏洞,攻击者可以利用这些漏洞继续威胁 SDN.因此,创建一个全面的安全设计,可以抵御 SDN 中的各种漏洞,以防御各种潜在的攻击.为了解决上述问题,Song 等人^[64]提出一种基于 SDN 和机器学习技术的感知实时威胁的网络入侵检测系统,引入入侵响应系统,该系统使用反应式路由进行 SDN 中的影响分析,在 SDN 中的一个开源项目中实现原型,并使用网络公开归档数据和实时数据评估所提出的系统.Anderson 等人^[65]提出了基于 SDN 网络的异常检测、分类和缓解框架 ATLANTIC,该框架包括一个负责监控流量的轻量级阶段和一个负责异常分类和缓解的重量级阶段:轻量级阶段利用信息论计算流表熵的偏差,重量级阶段利用 SVM 算法对异常流量进行分类.根据不同量级,使用不同方法对流量异常进行分类,通过使用所收集的信息,以特定方式处理每个流量配置文件,阻止恶意流量.

DDoS 攻击是 SDN 网络安全的一大威胁.DDoS 攻击的目标是:通过使用许多傀儡机同时发送大量假请求来耗尽系统资源,从而无力满足合法用户的请求.在 SDN 网络中,DDoS 攻击会耗尽数据平面和控制平面的网络、存储和计算资源,使 SDN 网络不可用.因此,DDoS 攻击检测对于 SDN 网络的正常运行至关重要.应用人工智能技术,根据与流量特征相关的某些功能区分网络流量,并将其分类为恶意或良性,以减轻对 SDN 控制器或交换机的入侵和 DDoS 攻击^[66,67].Niyaz 等人^[68]将系统构建为 SDN 控制器上的网络应用程序,使用深度学习算法减少从网络数据包头部导出的大量特征的情况,在 SDN 环境中,提出了一种基于深度学习的多向量 DDoS 检测系统.但是上述算法均不具备从原始字节中直接提取特征的能力,而是从派生的特征中降低特征维度.Chen 等人^[69]从 SDN 控制器角度入手,结合分类器 XGBoost 改进决策树方法,利用收集的流数据包数据集进行 DDoS 检测.但截止到目前,基于 SDN 的 DDoS 流量检测仍然无法满足 DDoS 攻击检测的应用特定要求.其中,DDoS 攻击检测的流量阈值可能因应用而异,然而现有的解决方案没有实现任何机制来满足这一重要需求并设定相应的约束条件.此外,利用 SDN 进行 DDoS 流量检测通常采用单个控制器作为解决方案,这不仅会造成网络流量的瓶颈,还会导致 SDN 网络出现单点故障.虽然 SDN 可以整合分布式平台,集中控制整个网络,但现有的解决方案还没有充分发挥它的潜力.

2.3 基于人工智能的流量工程

流量工程(traffic engineering,简称 TE)是通过动态分析,预测和调节传输数据的行为来优化数据网络性能的重要机制.迄今为止,结合 SDN 研究的大部分工作都集中在开发 SDN 架构上,而不是为 SDN 开发 TE 工具.SDN 大幅度地简化网络管理,降低运营成本,促进了当前和未来网络的创新和发展.SDN 的这些独特功能为新的 TE 技术提供了巨大的动力,利用相应技术,可以更好地进行流量控制和管理全局网络视图、状态和流模式特征.基于 SDN 的流量工程的优势在于:互联网应用程序要求底层网络架构能够实时地做出反应,并且可以针对大量流量进行扩展.该架构应该能够对来自不同应用的各种流量类型进行分类,并在非常短的时间内,为每种流量类型提供合适的特定服务;其次,面对云计算的快速增长以及大规模数据中心的需求,合适的网络管理应该能够提高资源利用率以获得更好的系统性能.因此,迫切需要新的网络架构和更智能和高效的 TE 工具.结合人工智能技术识别不同的流量类型,为 SDN 网络提供一种细粒度的网络管理方法,网络运营商可以更有效地处理不同的业务和分配网络资源,通过预测流量动态变化情况,设计相应的应对策略,实现高效、准确的网络优化.基于人工智能的流量工程大致分为流量的分类识别以及动态流量调度优化,下面将对基于人工智能流量工程方法的相关研究进行简要概述.

2.3.1 流量分类

基于 SDN 的数据流在不同的情境下具有不同的特征,目前有两种分类方式:一种是将流量分为大象流和老

鼠流^[70],大象流是大量持续的流,而老鼠流是小量且短时间的流;另一种是根据 QoS 将流量分类^[71,72].

在数据中心,80%的流量是老鼠流,但是 20%的大象流却占据了 80%的带宽,因此,识别大象流和老鼠流对于准确识别数据中心流量、实现适宜的网络流量调度具有重要的意义.SDN 通过流量控制为数据中心网络提供灵活的管理,然而这种细粒度管理在数据和控制平面之间消耗了大量带宽,造成基于 SDN 的数据中心的可扩展性的瓶颈.“大象和老鼠现象”表明:只有非常少的大象流量承载了数据中心的大部分字节,因此它可以通过检测和重新路由大象流以提高管理水平.但是,用于大象流检测的现有机制面临着高带宽消耗和检测时间过长的挑战.为了解决上述问题,Tang 等人提出一种有效的采样和分类方法(efficient sampling and classification approach,简称 ESCA)应用于大象流的检测^[73].在第 1 阶段,ESCA 通过估计大象流的到达时间间隔,并使用过滤流表过滤掉冗余样本来提高采样效率;在第 2 阶段,ESCA 基于数据流之间的相关性,使用新的监督分类算法对样本进行分类.通过这两个阶段来实现大象流的检测.因为过滤了冗余部分数据,因此降低了整个系统的带宽消耗与计算时间.但是基于这一方法的缺陷在于:一方面无法满足 SDN 数据中心和校园网的粒度需求;另一方面,巨大的计算开销降低了测量框架的可扩展性.

QoS 感知的流量分类旨在识别流量的 QoS 类.随着 Internet 上应用程序的指数级增长,要识别所有的应用程序是困难和不切实际的.但是,应用程序可以根据其 QoS 需求(如延迟、抖动和丢失率)划分为不同的 QoS 类.许多不同的应用程序可能属于一个 QoS 类,因此,根据流量的 QoS 要求对流量进行分类是一种更为有效的方法^[74].应用人工智能算法可以实现:(a) 多维关键绩效指标(key performance indicators,简称 KPI)分析,并发现新的相关性,执行根本原因分析并预测 QoS 违规行为;(b) 实施数据清理技术,以处理不完整、丢失或损坏的数据;(c) 支持强大且可扩展的架构,可从虚拟和现实世界中收集数据.因此,人工智能算法能够满足大数据情境下的 QoS 预测,发现规则间更多的相关性.

2.3.2 流量调度

现代网络中,高时空流量的可变性需要网络不断改变处理策略,以保持接近最佳网络性能.Geyer 等人提出,当前的电信网络在许多不同的平面和时间尺度上表现出内在的可变性^[75],例如光纤意外失效、无线信道质量因多径衰落而快速波动等.同时,智能手机和平板电脑作为用户的主要互联网接入设备的使用也越来越多,使得流量需求随着内容受欢迎的程度而发生改变,这些因素及其他因素导致了流量需求在时间和空间上的频繁且较大的波动.由此可知,流量具有变异和波动的属性.为了保证网络的稳定,需要在不同输入(即网络和流量)状况保持系统的良好性能.此外,考虑到出现流量涌流的情况,系统的实际性能并不总是遵循优化模型预测的性能.因此,在线网络优化(online networking optimize,简称 ONO)必须满足在实际流量情况与预测情况产生偏差时,大多数预测的流量状况的性能处于最优或至少稳定的状态.

在 SDN 网络中的流表匹配策略能够体现网络流量的动态处理情况,基于分类方法,Su 等人对包的结构进行分析^[76],提出一种基于字段的数据包的匹配模型 F-OpenFlow.该方法提出通过分组匹配字段提高表项匹配概率的方法,利用元空间搜索分析现有网络中流表的结构,找到同类型的匹配规则,并利用元空间方法将分析模型与字典树集成,处理动态网络中的字段,得到相应的规则并匹配对应的策略,实现了高效、准确的网络优化.但是上述方法并没有利用以往的历史数据进行匹配,导致分析消息位置和流表之间的关系不够准确,不能保证能够提高流表的命中率和匹配速度.

2.3.3 流量预测

网络流量具有自相似性、多尺度性、长程依赖性和高度非线性的特性(如泊松模型和高斯模型建模的不足),这些统计特性决定了流量的可预测性.对于大多数网络操作管理任务,如流量计算、短时流量调度或重路由、长期容量规划、网络设计和网络异常检测,拥有准确和及时的流量数据是必不可少的.例如:当网络发生拥塞时,传统的路由协议不能立即响应以调整流量分布,导致高延迟、丢包和抖动等情况发生.尤其在高容量流量检测和 DDoS 预测方面,由于早期预警,基于主动预测的方法将更快.同样,在网络被显著影响后,预测网络拥塞比通过测量来检测拥塞的被动方法更有效.考虑到上述情况,Azzouni 等人提出了一种称为 NeuRoute 的动态路由框架^[77].在 NeuRoute 中,长短时记忆模块(long short term memory,简称 LSTM)被用来估计未来的网络流量.该方法

通过输入网络状态和估计的网络流量,以启发式算法计算得到的相应路由解为输出,对神经网络模型进行训练。Polson 等人开发出深度学习模型来预测流量,其主要贡献是开发出结合使用 l_1 正则化和一系列双曲面正切层的线性模型^[78],解决预测流量中自由流量、故障、恢复和拥堵之间急剧的非线性过渡的问题,并证明了深度学习架构可以捕捉到这些非线性的时空效应。因此,通过深度学习的方法预测流量,在获取网络流量数据的同时进行流量预测,从而实现智能路由。尽管人工智能方法可以解决流量预测问题,但是很难说在任何情况下,一种方法明显优于其他方法。其中一个原因是:所提出的模型是利用少量单独的特定流量数据开发的,并且流量预测方法的准确性取决于嵌入在所收集的流量数据中的流量特征。此外,一般而言,将神经网络相关算法应用于流量预测,该模型的预测能力和鲁棒性都会优于一般模型。总体来说,现有的流量预测方法主要使用浅层流量预测模型,并且依旧不能满足许多实际应用。

3 未来挑战及网络场景

尽管目前人工智能技术能够初步解决 SDN 的部分问题,但在人工智能全面结合 SDN 之前仍存在挑战,其中包括高质量数据、跨域通信、可扩展性以及安全预测。此外,本节还将讨论凭借 SDN 集中控制的优势与 5G、网络功能虚拟化、物联网、边缘计算、信息中心网络以及无线网络等领域结合的发展趋势。

3.1 未来挑战

3.1.1 高质量数据

尽管拥有成熟的大数据处理技术以及基于人工智能的数据分析技术,但是人工智能算法是由图像处理领域而不是网络领域提出的,大多数算法不能直接迁移和使用于网络场景。网络数据并不完全符合人工智能算法的数据格式要求,为了将人工智能应用于网络,需要事先将网络数据翻译成矩阵或向量的形式。因此,将人工智能应用于 SDN 进行准确分类预测的前提是,训练准确、高质量的数据以弥补分析数据格式、数据编制等方面的不足。目前存在的问题主要分为两个方面:一方面,关于 SDN 网络数据集大小、SDN 网络特征以及基于人工智能 SDN 网络模型还未成型;另一方面,高质量的数据只能靠人工清洗,没有公开的数据集便于研究人员实验,因此需要各方力量整合出高质量的公开网络数据集。

3.1.2 跨域通信

多控制器的出现,是为了解决网络规模扩大而产生的交换机和控制器之间复杂度增高的弊端。有研究证明,跨域信息共享有利于提高网络性能。但跨域数据流的传输需要多个控制器,这样的跨域设计打破了原有的 SDN 模块化。为了兼顾多控制器以及网络复杂度的增加,传统的优化方法已不足以对网络进行优化。尽管人工智能算法可以用于跨层网络优化,分析收集到的域间信息,包括数据链路层信息、应用平面信息等优化网络,例如路由机制、拥塞控制和负载均衡等等,但是基于多层递归网络的跨层优化方法一方面由于跨域通信没有成熟的模型以便于下一步研究,另一方面,跨域通信涉及的参数太多,往往牵一发而动全身,缺少真正适用于域间通信的优化算法。尽管多目标优化算法能够在较少参数的情况下解决上述问题^[79],但在真实情况中,多目标优化算法就会因为参数太多而导致 Pareto 非支配问题失效,从而致使整个优化方法失效。因此,尽早建立域间通信问题模型以及优化方法,是目前研究的重点。

3.1.3 可扩展性

SDN 集中控制管理的优势,吸引了越来越多学术界和工业界的研究人员投身于此。SDN 带来的优势为网络开发带来更多的机遇,但在实践过程中却遇到了很多屏障,例如:随着网络规模的扩大,为了扩展平面需要增加控制器的数量分担任务以提升集中控制器的性能,但是随着控制器数量的增加,又会带来控制器的放置以及动态调控的问题^[35]。从这个角度来看,为了提高 SDN 网络的可扩展性,可以考虑采用多级强化学习方案,其中,根控制器为高级学习代理,局部控制器为低级学习代理。每个低层学习代理根据其本地网络状态信息学习如何对域内的流量进行路由,从而做出最优决策;而高层学习代理则基于整个网络的全局视图来处理域间的流量。为了缩短系统响应时间,根控制器可以周期性地将其训练好的强化学习模型部署到本地控制器上。训练后的强化模型将指导本地控制器直接处理域间的流量。多级强化学习方案不仅降低了业务流的处理延迟,而且提高了 SDN 网络

的可扩展性.基于强化学习方案尽管考虑将控制器分级来提高 SDN 可扩展性,但是目前,研究仍仅限于理论,并没有实际的场景验证算法的实用性,因此应考虑实际情况以保证整个系统的鲁棒性.

3.1.4 安全预测

在之前的网络安全部分,我们讨论了 SDN 控制器使用人工智能分析历史数据,对网络异常进行检测并处理网络攻击.但是异常检测是一个对抗过程,尽管通过历史数据可以构建一个成熟的模型来预测下一次攻击,但是恶意攻击者很少以相同的方式来完成,他们会不断尝试创建新的攻击以逃避控制器检测^[69].在这种情况下,使用历史数据来训练人工智能模型不是检测攻击的有效方法,因为要为此创建新的攻击.为了解决上述问题,可以采用两种解决方式.

- 一种是生成式对抗网络(generative adversarial network,简称 GAN)^[80],GAN 是一种通过预测新的攻击来解决问题的方法.GAN 由两个神经网络组成:一个神经网络,称为生成器,生成新的数据;而另一个神经网络,称为识别器,负责根据真实的训练数据集评估新数据的真实性.生成器和识别器一起训练,使生成的新数据更加真实.GAN 可以根据历史数据生成可能的新攻击数据.利用生成的新数据和历史数据对机器学习模型进行训练,训练后的机器学习(machine learning,简称 ML)模型可以检测已知的攻击和可能的新攻击.基于攻击检测,控制器能够提前修改交换机中的流表,防止网络攻击,限制控制平面与数据平面之间的通信;
- 另一种方法采用先验-后验经验模型^[81],先验经验和后验经验可以在模型中分别代表网络历史数据信息和检测过程中实时反馈的信息.这种方法保留了历史信息对控制器检测的影响,同时在模型中考虑了实时反馈信息以更正模型.这种方法能够准确、实时地分析网络攻击,以确保网络不会因为陷入新的攻击而造成严重的后果.

3.2 不同网络场景应用

3.2.1 5G

5G 将支持越来越多的连接设备,提供更高的用户数据速率,使每个地理区域的移动数据流量更高,降低传输延迟和网络能耗.5G 除了具有特定的性能要求外,还需要支持异构服务、设备和接入网^[82,83].SDN 通过分离控制和数据平面,网络结构得到极大的简化,并且减少了网络节点之间的控制信令,增强了网络的负载均衡和移动性管理以及提高网络控制的灵活性.文献[84]提出了一种基于 SDN 的集中式无线网络控制器,用于控制核心网络中的多节点和网关.基于 SDN 的 5G 网络可塑架构旨在满足新一代服务和设备的功能和性能要求,关键特性是灵活性,需要有效地支持异构服务集,包括机器类型通信和物联网通信.这些应用程序在端到端延迟、可靠性和可伸缩性方面增加了具有挑战性的目标.为了应对 5G 移动网络中异构的无线环境、网络管理的复杂性、不断增长的移动通信需求和多样化的服务需求带来的挑战,人工智能技术应被用于在移动中部署更多的智能网络^[85].

3.2.2 网络功能虚拟化

网络功能虚拟化(network function virtualization,简称 NFV)允许在网络中部署虚拟网络功能(virtual network functions,简称 VNFs),以增强性能、安全性和管理.通过 VNF 将网络功能与底层专用硬件解耦,使网络体系结构更加灵活.VNFs 是在商业现实设备上运行的软件中实现的,可由 ISDN 控制器集中控制.与传统的由专用硬件设备实现的网络功能相比,VNFs 具有显著降低运营和资本支出、提高服务敏捷性的潜力.随着 VNF 的应用,有许多相关性的研究成为促进网络灵活性和成本效率的重要服务,例如,强化学习用于根据资源使用情况动态创建服务功能链(service function chain,简称 SFC)以支持高效的服务提供^[86,87].结合人工智能思想,可以将 SDNFV 的在线路由问题描述为线性规划模型,并基于该架构,根据网络中的资源条件获得需要的延迟、负载、带资源利用率等数据,促进动态服务提供和网络资源利用优化.例如,将网络功能分配问题描述为一个两阶段的 Stackelberg 博弈,其中,服务器作为网络功能的卖家,用户作为网络功能的买家,应用强化学习算法得到了最优的网络函数分配策略^[88].

3.2.3 物联网

物联网(Internet of things,简称 IoT)已成为一种全球网络基础设施,通过使用异构(有线/无线)通信技术连接大量不同的异构设备.由于这些设备的高移动性和广泛覆盖,不同类型的无线电接入技术已广泛用于 IoT.然而,异构通信技术和设备基础结构的复杂性涉及到许多关键问题,例如:随着设备数量的增加,交换机的流量负载可能变得非常繁重,并且需要将多个信道适当地分配给链路.此外,异构设备在数据感知和收集方面具有不同的策略,这导致会发生突发流量到达交换机不均匀的情况^[89,90].为了更好地适应异构大规模 IoT,智能软件定义网络成为将分布式异构设备连接到集中共享工作系统的新颖的解决方案,我们称这样的方案为智能 SDN-IoT.在智能 SDN-IoT 中,各种设备广泛部署在传感平面中,由传感平面收集的所有传感数据通过数据平面中的交换机转发传送到网关,利用人工智能技术结合部分重叠信道分配解决自适应的分配信道问题,以确保无线网络中的通信服务质量.

3.2.4 边缘计算

边缘计算(edge computing,简称 EC)将计算和存储推至网络边缘.在边缘计算中,“边缘”定义为沿着数据源和云数据中心之间路径的任何计算和网络资源^[91].智能 SDN 与边缘计算结合,可以使如下领域受益:高分辨率和有效控制、灵活性和创新的低障碍、以服务为中心的、虚拟机流动性、适应性、互操作性、低成本解决方案以及范围的多样性.但是智能 SDN 及其当前事实上的 OpenFlow 标准化都不够成熟,无法处理所指出的所有可能的用例和管理操作.由于需求正在快速变化,即使是基于基础架构即服务的相对更为标准的域也在不断发展.面对越来越复杂的需求,仅部署支持 SDN 的网络设备将无法轻松实现将 SDN 集成到现有网络中.另一方面,硬件投资成本非常昂贵,因此,支持智能 SDN 的硬件无法在功能和部署方面达到所需水平.而利用人工智能技术提供更精细的控制粒度与抽象粒度,在用例和管理上提供了更多的可能性.

3.2.5 信息中心网络

信息中心网络(information-centric networking,简称 ICN)是一种通过名称向用户提供对内容的访问,而不是在主机之间提供通信信道的架构^[92].ICN 集成 SDN 特征将网络的控制平面和数据平面分开,使网络能够从全局视图进行编程和集中控制.结合 ICN 和 SDN 的集成框架 SDN-ICN 有利于利用 ICN 中数据平面的数据独立性和 SDN 中控制平面的集中控制,更好地控制全局网络.首先,ICN 中不受地址限制的内容在网络层作为独立实体进行路由和转发,SDN 中的集中调度可以优化网络资源的分配^[93-95].在 SDN-ICN 中存在大量计算节点,利用人工智能能够与 ICN 同时学习,降低了 ICN 因处理数据而造成的时延.因此,由于使用分散在各种 SDN 节点上的丰富计算资源,可以解决人工智能模型训练过程中由于计算时间产生的挑战.其次,基于全局视图中数据的收集和分析的统一,可以实现具有更高精度导向的流特征的多尺度流量预测.分布式 SDN 中的多个交换机收集所请求的目标内容的特征,其包含固有的时空和社交相关性,深度学习网络可以在全局视图中理解这些功能,然后,由于其深度学习网络的无监督学习能力,可以找到内容流行度的分布模式,并且不会错过该模式的微小变化以提高预测的准确性.最重要的是,SDN-ICN 可以重新配置深度学习网络的结构.由于 SDN 的可编程性和 SDN 控制器在全局视图中控制网络的能力,每层中的隐藏层和神经元都可以轻松调整.受益于这种可编程网络,我们可以通过网络轻松部署各种网络模型,以解决 SDN-ICN 模型中遇到的计算问题.

3.2.6 无线网络

无线网络(wireless network,简称 WN)由许多节点组成,通过无线信道进行传输.与有线网络不同,无线网络的信道总是随着用户的移动性、信道衰落和干扰而发生改变.在移动用户密集的无线网络中,由于小区规模小,信道容量变化更加难以处理^[96,97].基于 SDN 的集成解决方案能够支持密集无线网络中的用户移动性,因此,传统和新兴无线环境中的无线软件定义网络(wireless software defined networking,简称 WSDN)引发了对 WSDN 架构中固有安全性的担忧^[98-100].WSDN 范例遇到与有线 SDN 框架非常相似的安全问题,无线介质带来了额外的攻击手段,并为攻击者提供了瞄准控制平面、数据转发元件以及各个无线应用的机会.控制器功能仍然是一个中心故障点,可以动态地移动到网络中的不同服务器,使得潜在的攻击者难以破坏控制平面.全局网络可见性为安全管理员提供了一个中心优势,可以根据需要观察实时流量统计信息并更改安全策略.此外,WSDN 环境可以

利用各个节点的能力,在网络的不同部分之间实现安全链,以实现分层安全模型,而不会使单个网络实体负担过重.因此,如果适当使用现有的集中式 WSDN 设计,可将框架本身转变为可编程安全屏障,其包括可以改变功能的可编程数据平面设备.将人工智能的相关技术与 WSDN 结合,以解决 WSDN 的安全问题,整合历史数据分析预测恶意攻击,能够准确、有效地提升 WSDN 的安全可靠性.在 WSDN 中,机器学习算法对于管理大量异构传感器节点、优化每个节点的资源利用率、灵活且高效地调度通信链路起着至关重要的作用.目前,无线传感器网络中的路由优化、节点聚类与数据聚合、事件检测与查询处理、定位、入侵检测、故障检测等问题都采用了机器学习技术^[10].

4 结 论

本文对人工智能技术应用于软件定义网络进行了综述性分析与研究.首先对人工智能技术与软件定义网络的背景进行讨论,分别对以上两个方向的研究现状进行详细的论述,分层次地描述人工智能应用于软件定义网络数据平面、控制平面以及应用平面的相关研究.然后从应用背景及标准化的角度,详细讨论了目前人工智能应用于 SDN 智能路由优化方法、网络安全智能方法以及基于人工智能流量工程的相关研究,比较以上研究领域内现有方法的优缺点,并给出目前较为权威的国际标准化组织对基于人工智能的 SDN 标准化定义.最后总结基于人工智能的 SDN 在高质量数据、跨域通信、可扩展性以及网络安全预测方面所面临的挑战,并在此基础上讨论基于人工智能的 SDN 与一些新兴领域,包括 5G、网络功能虚拟化、物联网、边缘计算、信息中心网络以及无线网络领域结合的发展趋势.综上所述,人工智能的相关算法在 SDN 网络中的应用研究非常广泛,同时面临着许多挑战,然而这些挑战却推动着 SDN 向着更好的方向发展.希望通过本文的讨论和探索,为基于人工智能的 SDN 网络的发展和更加智能化的网络的实现开辟一条新的途径.

References:

- [1] Clark DD, Partridge C, Ramming JC, *et al.* A knowledge plane for the Internet. In: Proc. of the SIGCOMM. 2003. 3–10.
- [2] Xia W, Wen Y, Foh CH. A survey on software-defined networking. *Communications Surveys & Tutorials IEEE*, 2015,17(1):27–51.
- [3] Kreutz D, *et al.* Software-defined networking: A comprehensive survey. *Proc. of the IEEE*, 2015,103(1):14–76. [doi: 10.1109/JPROC.2014.2371999]
- [4] Cui L, Yu FR, Yan Q. When big data meets software-defined networking: SDN for big data and big data for SDN. *IEEE Network*, 2016,30(1):58–65.
- [5] Yu S, Lin X, Mistic J. Networking for big data. *IEEE Network*, 2014,28(4):4.
- [6] Wang M, Cui Y, Wang X. Machine learning for networking: Workflow, advances and opportunities. *IEEE Network*, 2018,32(2): 92–99.
- [7] Latah M, Toker L. Artificial intelligence enabled software defined networking: A comprehensive overview. *IET Networks*, 2018, 8(2). [doi: 10.1049/iet-net.2018.5082]
- [8] Peng MG, Sun YH, Li XL. Recent advances in cloud radio access networks: System architectures, key techniques, and open issues. *IEEE Communications Surveys & Tutorials*, 2016,18(3):2282–2308.
- [9] Zheng K, Yang Z, Zhang K. Big data-driven optimization for mobile networks toward 5G. *IEEE Network*, 2016,30(1):44–51.
- [10] Hong W, Wang K, Hsu Y-H. Application-aware resource allocation for SDN-based cloud datacenters. In: Proc. of the Int'l Conf. on Cloud Computing and Big Data 2013. Fuzhou, 2013. 106–110.
- [11] Han Y, Seo SS, Li J. Software defined networking-based traffic engineering for data center networks. In: Proc. of the Network Operations & Management Symp. IEEE, 2014. 1–6.
- [12] Shenker S. The future of networking, and the past of protocols. In: Proc. of the Open Networking Summit. 2011.
- [13] Casado M, Freedman MJ, Pettit J, Luo JY, McKeown N, Shenker S. Ethane: Taking control of the enterprise. *Computer Communication Review*, 2007,37(4):1–12.
- [14] Floriachpigem M, Xercavinstorregrosa G, Gelonch-Bosch A, Marojevic V. Creating tailored and adaptive network services with the open orchestration C-RAN framework. In: Proc. of the 2018 IEEE 5G World Forum (5GWF). Silicon Valley, 2018. 89–92.
- [15] Seng KP, Ang LM, Schmidtke LM, *et al.* Computer vision and machine learning for viticulture technology. *IEEE Access*, 2018,6:1.

- [16] Chen Y, Su L, Xu J. Distributed statistical machine learning in adversarial settings: Byzantine gradient descent. arXiv: 1705.05491, 2017.
- [17] Azizian M, Cherkaoui S, Hafid AS. Vehicle software updates distribution with SDN and cloud computing. *IEEE Communications Magazine*, 2017,55(8):74–79.
- [18] Young T, Hazarika D, Poria S, *et al.* Recent trends in deep learning based natural language processing. *IEEE Computational Intelligence Magazine*, 2018,13(3):55–75.
- [19] Mckeown N, Anderson T, Balakrishnan H, *et al.* OpenFlow: Enabling innovation in campus networks. *ACM SIGCOMM Computer Communication Review*, 2008,38(2):69–74.
- [20] Zhang W, Paudel B, Wang L, *et al.* Iteratively learning embeddings and rules for knowledge graph reasoning. arXiv: 1903.08948, 2019.
- [21] Wachi A. Failure-scenario maker for rule-based agent using multi-agent adversarial reinforcement learning and its application to autonomous driving. arXiv: 1903.10654, 2019.
- [22] Tang H, Liu X, Xie X. An end-to-end framework for integrated pulmonary nodule detection and false positive reduction. In: *Proc. of the 16th IEEE Int'l Symp. on Biomedical Imaging (ISBI 2019)*. Venice, 2019. 859–862.
- [23] Rosenfeld A, Zemel R, Tsotsos JK. High-level perceptual similarity is enabled by learning diverse tasks. arXiv: 1903.10920, 2019.
- [24] Young T, Hazarika D, Poria S, *et al.* Recent trends in deep learning based natural language processing. *IEEE Computational Intelligence Magazine*, 2018,13(3):55–75.
- [25] Brunetti A, Buongiorno D, Trotta GF, *et al.* Computer vision and deep learning techniques for pedestrian detection and tracking: A survey. *Neurocomputing*, 2018,300(Jul.26):17–33.
- [26] Chen Y, Su L, Xu J. Distributed statistical machine learning in adversarial settings: Byzantine gradient descent. arXiv: 1705.05491, 2017.
- [27] Gu WY, Xu X, Yang J. Path following with supervised deep reinforcement learning. In: *Proc. of the 4th IAPR Asian Conf. on Pattern Recognition (ACPR)*. IEEE Computer Society, 2017. 448–452.
- [28] Zhou T, Brown M, Snavely N, *et al.* Unsupervised learning of depth and ego-motion from video. arXiv: 1704.07813, 2017.
- [29] Hu T, Yu J. Generalized entropy based semi-supervised learning. In: *Proc. of the IEEE/ACIS Int'l Conf. on Computer & Information Science*. IEEE Computer Society, 2015. 259–263.
- [30] Low Y, Bickson D, Gonzalez J, *et al.* Distributed GraphLab: A framework for machine learning and data mining in the cloud. *Proc. of the VIDB Endowment*, 2012,5(8):716–727.
- [31] Hamidinekoo A, Denton E, Rampun A, *et al.* Deep learning in mammography and breast histology, an overview and future trends. *Medical Image Analysis*, 2018,47:45–67.
- [32] Zhang Z, Geiger J, Pohjalainen J, *et al.* Deep learning for environmentally robust speech recognition: An overview of recent developments. *ACM Trans. on Intelligent Systems & Technology*, 2017,9(5):1–28.
- [33] Litjens G, Kooi T, Bejnordi BE, *et al.* A survey on deep learning in medical image analysis. *Medical Image Analysis*, 2017,42(9):60–88.
- [34] Lopez MM, Kalita J. Deep learning applied to NLP. arXiv: 1703.03091, 2017.
- [35] Xie J, Yu FR, Huang T, *et al.* A survey of machine learning techniques applied to software defined networking (SDN): Research issues and challenges. *IEEE Communications Surveys & Tutorials*, 2018,PP(99):1.
- [36] Rahimi R, Veeraraghavan M, Nakajima Y, *et al.* A high-performance OpenFlow software switch. In: *Proc. of the 17th IEEE Int'l Conf. on High Performance Switching and Routing (HPSR)*. IEEE, 2016. 93–99.
- [37] Rodriguez-Natal A, Portoles-Comeras M, Ermagan V, *et al.* LISP: A southbound SDN protocol? *IEEE Communications Magazine*, 2015,53(7):201–207.
- [38] Zheng P, Hu CC, Li H. Reducing the southbound interface overhead for OpenFlow based on the flow volume characteristics. *Journal of Computer Research and Development*, 2018,55(2):346–357 (in Chinese with English abstract).
- [39] Junhua B, Ying W, Zhong XX, *et al.* An SDN energy saving method based on topology switch and rerouting. In: *Proc. of the 2018 IEEE/IFIP Network Operations and Management Symp. (NOMS)*. 2018. 1–5.
- [40] Tang F, Fadlullah ZM, Mao B, *et al.* An intelligent traffic load prediction based adaptive channel assignment algorithm in SDN-IoT: A deep learning approach. *IEEE Internet of Things Journal*, 2018,1.

- [41] Leguay J, Maggi L, Draief M, *et al.* Admission control with online algorithms in SDN. In: Proc. of the Network Operations & Management Symp. IEEE, 2016. 718–721.
- [42] Nanda S, Zafari F, Decusatis C, *et al.* Predicting network attack patterns in SDN using machine learning approach. In: Proc. of the Network Function Virtualization & Software Defined Networks. IEEE, 2017. 167–172.
- [43] Jain S, Kumar A, Mandal S, *et al.* B4: Experience with a globally-deployed software defined WAN. In: Proc. of the ACM 2013 Conf. on SIGCOMM. 2013. 3–14.
- [44] Shi H, Li H, Zhang D, *et al.* Efficient and robust feature extraction and selection for traffic classification. Computer Networks, the Int'l Journal of Computer & Telecommunications Networking, 2017,119(C):1–16.
- [45] Shi H, Li H, Zhang D, *et al.* An efficient feature generation approach based on deep learning and feature selection techniques for traffic classification. Computer Networks, 2018,132(26):81–98.
- [46] Ertam F, Engin A. A new approach for internet traffic classification: GA-WK-ELM. Measurement, 2017,95:135–142.
- [47] Soysal M, Schmidt EG. Machine learning algorithms for accurate flow-based network traffic classification: Evaluation and comparison. Performance Evaluation, 2010,67(6):451–467.
- [48] https://static.sched.com/hosted_files/onfconnect2018/81/ONF%20Connect%20-%20P4%20INT%20and%20ML%20Monster.pdf
- [49] ETSI Press Release. New ETSI group on improving operator experience using AI. 2017. <https://www.etsi.org/newsroom/news/1171-2017-02-new-etsi-group-on-improving-operator-experience-using-artificial-intelligence>
- [50] Ullman DG. OO-OO-OO! The sound of a broken OODA loop. CrossTalk Journal of Defense Software Engineering, 2007,22–25.
- [51] IETF Internet-draft, a general considerations of intelligence driven network. 2017.
- [52] <https://engage2demand.cisco.com/LP=18308?ccid=cc001244&oid=rpten018612&dtid=odicdc000673>
- [53] Mhdawi AKA, Al-Raweshidy HS. iPRDR: Intelligent power reduction decision routing protocol for big traffic flood in hybrid-SDN architecture. IEEE Access, 2018,1.
- [54] Kim S, Son J, Talukder A, *et al.* Congestion prevention mechanism based on Q-leaning for efficient routing in SDN. In: Proc. of the Int'l Conf. on Information Networking. IEEE Computer Society, 2016. 124–128.
- [55] Pasca STV, Prasad SS, Kataoka K. AMPF: Application-aware multipath packet forwarding using machine learning and SDN. arXiv: 1606.05743, 2016.
- [56] Tang F, Mao B, Fadlullah ZM, *et al.* On removing routing protocol from future wireless networks: A real-time deep learning approach for intelligent traffic control. IEEE Wireless Communications, 2017,99:1–7.
- [57] Mao B, Tang FX, Fadlullah ZM. A novel non-supervised deep-learning-based network traffic control method for software defined wireless networks. IEEE Wireless Communications, 2018,25(4):74–81.
- [58] Pinto EMDL, Lachowski R, Pellenz ME, *et al.* A machine learning approach for detecting spoofing attacks in wireless sensor networks. In: Proc. of the 32nd IEEE Int'l Conf. on Advanced Information Networking and Applications (AINA). IEEE, 2018. 752–758.
- [59] Huang H, Guo S, Li P, Ye B, Stojmenovic I. Joint optimization of rule placement and traffic engineering for QoS provisioning in software defined network. IEEE Trans. on Computers, 2015,64(12):3488–3499.
- [60] Mao B, Fadlullah ZM, Tang F, *et al.* Routing or computing? The paradigm shift towards intelligent computer network packet transmission based on deep learning. IEEE Trans. on Computers, 2017,1.
- [61] Geyer F, Carle G. Learning and generating distributed routing protocols using graph-based deep learning. In: Proc. of the 2018 Workshop on Big Data Analytics and Machine Learning for Data Communication Networks. 2018. 40–45.
- [62] Lin I, Akyildiz F, Wang P, Luo M. QoS-aware adaptive routing in multi-layer hierarchical software defined networks: A reinforcement learning approach. In: Proc. of the 2016 IEEE Int'l Conf. on Services Computing (SCC). San Francisco, 2016. 25–33.
- [63] Nanda S, Zafari F, Decusatis C, *et al.* Predicting network attack patterns in SDN using machine learning approach. In: Proc. of the Network Function Virtualization & Software Defined Networks. IEEE, 2017. 167–172.
- [64] Song C, Park Y, Golani K, *et al.* Machine-learning based threat-aware system in software defined networks. In: Proc. of the 26th Int'l Conf. on Computer Communication and Networks (ICCCN). IEEE, 2017. 1–9.
- [65] Silva ASD. Atlantic: A framework for anomaly traffic detection, classification, and mitigation in SDN. In: Proc. of the Network Operations & Management Symp. IEEE, 2016. 27–35.

- [66] Bawany NZ, Shamsi JA, Salah K. DDoS attack detection and mitigation using SDN: Methods practices and solutions. *Arabian Journal for Science and Engineering*, 2017,42(2):425–441.
- [67] Dayal N, Srivastava S. Analyzing behavior of DDoS attacks to identify DDoS detection features in SDN. In: *Proc. of the Int'l Conf. on Communication Systems and Networks (COMSNETS)*. 2017. 274–281.
- [68] Niyaz Q, Sun W, Javd AY. A deep learning based DDoS detection system in software-defined networking (SDN). arXiv: 1611.07400, 2016.
- [69] Chen Z, Jiang F, Cheng Y, *et al.* XGBoost classifier for DDoS attack detection and analysis in SDN-based cloud. In: *Proc. of the 2018 IEEE Int'l Conf. on Big Data and Smart Computing (BigComp)*. IEEE Computer Society, 2018. 251–256.
- [70] Hegde S, Koolagudi SG, Bhattacharya S. Scalable and fair forwarding of elephant and mice traffic in software defined networks. *Computer Networks*, 2015,92(2):1389–1286.
- [71] Namdev N, Agrawal S, Silkari S. Recent advancement in machine learning based internet traffic classification. *Procedia Computer Science*, 2015,60(1):784–791.
- [72] Li D, Hu G, Wang Y, *et al.* Network traffic classification via non-convex multi-task feature learning. *Neurocomputing*, 2015,152:322–332.
- [73] Tang F, Li L, Barolli L, *et al.* An efficient sampling and classification approach for flow detection in SDN-based big data centers. In: *Proc. of the 31st IEEE Int'l Conf. on Advanced Information Networking and Applications (AINA)*. IEEE Computer Society, 2017. 1106–1115.
- [74] Jain S, Khandelwal M, Katkar A, *et al.* Applying big data technologies to manage QoS in an SDN. In: *Proc. of the Int'l Conf. on Network & Service Management*. IEEE, 2017. 302–306.
- [75] Geyer F. Routing optimization for SDN networks based on pivoting rules for the simplex algorithm. In: *Proc. of the 13th Int'l Conf. on Design of Reliable Communication Networks (DRCN 2017)*. Munich, 2017. 1–8.
- [76] Su Y, Peng T, Zhong X, *et al.* Matching model of flow table for networked big data. arXiv: 1712.09158, 2017.
- [77] Azzouni A, Boutaba R, Pujolle G. NeuRoute: Predictive dynamic routing for software-defined networks. arXiv: 1709.06002, 2017.
- [78] Polson NG, Sokolov VO. Deep learning for short-term traffic flow prediction. *Transportation Research Part C: Emerging Technologies*, 2017,79:1–17.
- [79] Zhang B, Wang XW, Huang M. Multi-objective optimization controller placement problem in Internet-oriented software defined network. *Computer Communications*, 2018,123:24–35.
- [80] Goodfellow I, Pouget AJ, Mirza M, Xu B, *et al.* Generative adversarial nets. In: *Advances in Neural Information Processing Systems*. 2014. 2672–2680.
- [81] Breyhi A, Müller RR. Maximum-a-posteriori signal recovery with prior information: Applications to compressive sensing. arXiv: 1802.05776, 2018.
- [82] Trivisonno R, Guerzoni R, Vaishnavi I, *et al.* SDN-based 5G mobile networks: Architecture, functions, procedures and backward compatibility. *Trans. on Emerging Telecommunications Technologies*, 2014,26(1):82–92.
- [83] Yang J, Qiao Y, Zhang X, He H, *et al.* Characterizing user behavior in mobile Internet. *IEEE Trans. on Emerging Topics in Computing*, 2015,3(1):95–106.
- [84] Nayak A, Jha P, Karandikar K. A centralized SDN architecture for the 5G cellular network. arXiv Preprint arXiv: 1801.03824, 2018.
- [85] Karandikar A, Jha P, Nayak A, *et al.* Methods and systems for controlling a SDN-based multi-RAT communication network. 2017. <http://www.freepatentsonline.com/y2017/0238362.html>
- [86] Pei JN, Hong PL, Li DF. Virtual network function selection and chaining based on deep learning in SDN and NFV-enabled networks. In: *Proc. of the 2018 IEEE Int'l Conf. on Communications Workshops (ICC Workshops)*. 2018. 1–6.
- [87] Ahrens J, Strufe M, Ahrens L, *et al.* An AI-driven malfunction detection concept for NFV instances in 5G. arXiv: 1804.05796, 2018.
- [88] DOro S, Galluccio L, Palazzo S, Schembra G. A gametheoretic approach for distributed resource allocation and orchestration of software defined networks. *IEEE Journal on Selected Areas in Communications*, 2017,35(3):721–735.
- [89] Zhao L, Sun W, Shi YP, Liu JJ. Optimal placement of cloudlets for access delay minimization in SDN-based Internet of things networks. *Internet of Things Journal IEEE*, 2018,5(2):1334–1344.

- [90] Tang FX, Mao BM, Md Fadlullah Z, Kato N. On a novel deep-learning-based intelligent partially overlapping channel assignment in SDN-IoT. *Communications Magazine of IEEE*, 2018,56(9):80–86.
- [91] Baktir AC, Ozgovde A, Ersoy C. How can edge computing benefit from software-defined networking: A survey, use cases & future directions. *IEEE Communications Surveys & Tutorials*, 2017,19(4):2359–2391.
- [92] Zhang QY, Wang XW, Huang M, *et al.* Software defined networking meets information centric networking: A survey. *IEEE Access*, 2018,39547–39563.
- [93] Liu WX, Zhang J, Liang ZW, Peng LX, Cai J. Content popularity prediction and caching for ICN: A deep learning approach with SDN. *Access IEEE*, 2018,6:5075–5089.
- [94] Wen J, Li K. Big-data-enabled software-defined cellular network management. In: *Proc. of the Int'l Conf. on Software Networking*. IEEE, 2016. 1–5.
- [95] Zhang QY, Wang XW, Huang M, *et al.* Compressed sensing-based cached content locating for ICN. *IEEE Communications Letters*, 2018,20(10):2020–2023.
- [96] Bogale TE, Wang X, Le LB. Machine intelligence techniques for next-generation context-aware wireless networks. *arXiv: 1801.04223*, 2018.
- [97] Kobo HI, Abu-Mahfouz AM, Hancke GP. A survey on software-defined wireless sensor networks: Challenges and design requirements. *IEEE Access*, 2017,5:1872–1899.
- [98] Mao Q, Hu F, Hao Q. Deep learning for intelligent wireless networks: A comprehensive survey. *Communications Surveys & Tutorials of IEEE*, 2018,20(4):2595–2621.
- [99] Bakhshi T. Securing wireless software defined networks: Appraising threats, defenses & research challenges. In: *Proc. of the Int'l Conf. on Advancements in Computational Sciences*. IEEE, 2018. 1–6.
- [100] Xu S, Wang XW, Huang M. Software-defined next-generation satellite networks: Architecture, challenges, and solutions. *IEEE Access*, 2018,6:4027–4041.
- [101] Fadlullah ZM, Tang F, Mao B, *et al.* State-of-the-art deep learning: Evolving machine intelligence toward tomorrow's intelligent network traffic control systems. *IEEE Communications Surveys & Tutorials*, 2017,19(4):2432–2455.



李可欣(1993—),女,博士生,主要研究领域为人工智能,边缘计算,软件定义网络.



黄敏(1968—),女,博士,教授,博士生导师,主要研究领域为智能算法设计与优化,调度理论与方法.



王兴伟(1968—),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为未来互联网,云计算,网络空间安全.



刘小洁(1994—),女,博士生,CCF 学生会会员,主要研究领域为机器人网络.



易波(1988—),男,博士,讲师,CCF 专业会员,主要研究领域为下一代互联网,网络功能虚拟化,服务链.