面向软件定义网络的异常流量检测研究综述

付钰[1]，王坤[1,2]，段雪源[3,4]，刘涛涛[1]

（1. 海军工程大学信息安全系，湖北 武汉 430033；2. 信阳职业技术学院数学与信息工程学院，河南 信阳 464000；
3. 信阳师范大学计算机与信息技术学院，河南 信阳 464000；4. 信阳师范大学河南省教育大数据分析与应用重点实验室，河南 信阳 464000）

摘 要：针对软件定义网络（SDN）较传统网络更易遭受网络攻击的现实，从技术原理和架构特点出发，对近年来面向软件定义网络的异常流量检测研究进展进行综述，分析了 SDN 可能遭受网络攻击的组织形式，讨论了当前 SDN 异常流量检测、异常流量溯源、异常流量缓解相关技术的特点、优势及不足；对当前研究中常用的数据集进行了对比分析，并梳理出一些通用的数据预处理方法；总结并展望了未来 SDN 环境下异常流量检测方法的研究方向。调研结果可以指导实际应用需求中适配方法的选取，提出待解决的问题和矛盾可为后续研究提供引导。

关键词：软件定义网络；深度学习；异常流量检测；异常流量溯源；异常流量缓解

中图分类号：TP393

文献标志码：A

DOI: 10.11959/j.issn.1000−436x.2024016

Survey of research on abnormal traffic detection for software defined networks

FU Yu[1], WANG Kun[1,2], DUAN Xueyuan[3,4], LIU Taotao[1]

1. Department of Information Security, Naval University of Engineering, Wuhan 430033, China
2. School of Mathematics and Information Engineering, Xinyang Vocational and Technical College, Xinyang 464000, China
3. College of Computer and Information Technology, Xinyang Normal University, Xinyang 464000, China
4. Henan Key Laboratory of Analysis and Applications of Education Big Data, Xinyang Normal University, Xinyang 464000, China

Abstract: Since software defined network (SDN) was more vulnerable to network attacks than traditional networks, the research progress of abnormal traffic detection for software defined network in recent years from the technical principle and architecture characteristics was summarized, the possible organizational forms of network attacks on SDN were analyzed, and the characteristics, advantages, and disadvantages of current technologies related to abnormal traffic detection, abnormal traffic traceability, and abnormal traffic mitigation were discussed. The data sets commonly used in current research were compared and analyzed, and some general data preprocessing methods were sorted out. The research direction of abnormal traffic detection methods in the SDN environment in the future was summarized and prospected. The research results can guide the selection of adaptation methods in practical application requirements, and the problems and contradictions to be solved can guide subsequent research.

Keywords: software defined network, deep learning, abnormal traffic detection, abnormal traffic traceability, abnormal traffic mitigation

0 引言

随着信息科技的不断发展，互联网规模持续增长，网络环境也变得更加复杂，传统的网络配置策略难以满足未来网络动态、并发和实时性的需求[1]。软件定义网络（SDN, software defined network）是一种解耦原有网络设备的控制与转发，具有可编程性和扩展性的新型网络架构，其结构可分为三层：

收稿日期：2023−09−06；**修回日期：**2023−11−19

通信作者：王坤，queen@xyvtc.edu.cn

基金项目：国家重点研发计划基金资助项目（No.2018YFB0804104）；基础加强计划技术领域基金资助项目（No.2021-JCJQ-JJ-0990）

Foundation Items: The National Key Research and Development Program of China (No.2018YFB0804104), Foundation Augmentation Program Technical Funding (No.2021-JCJQ-JJ-0990)

转发平面、控制平面和应用平面[2]，如图 1 所示。SDN 采用集中式的控制平面和分布式的转发平面，2 个平面相互分离。控制平面利用控制–转发通信接口（南向接口）对转发平面的网络设备进行集中控制，并通过应用–控制接口（北向接口）向应用平面提供灵活的可编程能力。SDN 包含多种接口协议，如常用 OpenFlow 作为南向接口协议实现控制器与交换机的交互；北向接口支持应用平面与控制平面之间的交互，应用程序通过北向接口定义网络行为，实现 SDN 的自动化管理；东西向接口主要用于多个控制器之间的通信，通常应用于多控制器的大规模 SDN 中[3]。SDN 因其系统化网络架构和对网络的良好感知与管控能力，逐渐受到网络运营商和设备制造商的青睐。

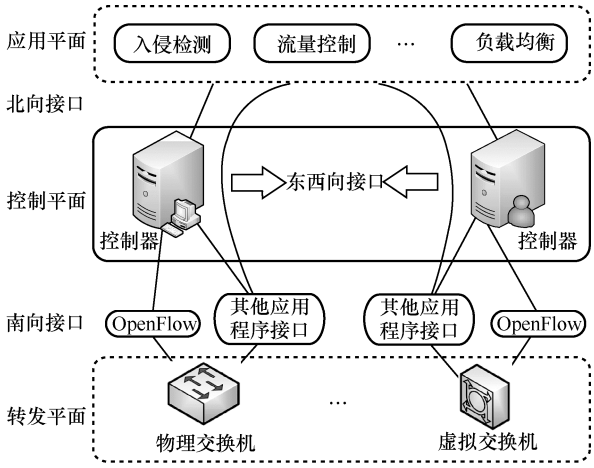

图 1　SDN 结构

SDN 将传统的网络控制功能进行集成，提高了网络的可编程性、简化了网络的配置操作，但这也使其更容易受到网络攻击[4]。如针对控制器可用队列容量的拒绝服务（DoS, denial of service）攻击[5-6]、针对交换机流表、缓存、通信链路的分布式拒绝服务（DDoS, distributed denial of service）攻击[7-10]，以及针对协议漏洞的各种低速率拒绝服务（LDoS, low rate denial of service）攻击[11-13]，此外还有针对网络漏洞的蠕虫、病毒攻击[14]等。网络攻击发生期间常伴随着网络流量的异常，表现为不符合预期的非正常行为模式。异常流量检测可以通过一定手段识别和过滤网络中的异常流量，是一种维护网络安全的基本手段。及时、准确地检测网络中的异常流量，能够有效地发现网络中的攻击行为，减小恶意攻击对网络运营业务的影响。因此，SDN 中的异常流量检测技术研究已成为 SDN 研究领域的前沿热点，研究工作对推动 SDN 技术的应用与发展具有重要的理论意义和实际应用价值。

SDN 有着与传统网络不同的网络架构、工作流程，网络攻击的组织形式也存在显著差异，因此，SDN 环境下的网络异常流量检测方法也具有特殊性。本文在系统分析 SDN 架构特点及遭受网络攻击形式的基础上，通过对现有基于深度学习的 SDN 异常流量检测、溯源及缓解等方法进行分析及归纳，并对常用的攻击检测实验数据集进行分类和描述，进而给出了当前研究工作的不足及未来的研究方向，期望能够为 SDN 环境中的异常流量检测研究提供参考。

1　SDN 的安全性及异常流量特点

SDN 通过集中控制平面与转发平面之间的标准接口为网络提供统一的管理，开放式的操作语义为网络设备的接入提供了便利，同时也降低了针对控制平面和转发平面攻击的难度[15]。以最常用的南向接口——OpenFlow 的 SDN 为例，当 SDN 交换机接收到任何新的数据流（在交换机流表中无匹配规则的流）时，都会向控制器发送消息询问转发规则，这种开放性的处置方式为攻击者带来了极大便利。因此，SDN 遭受的网络攻击也主要是针对转发平面和控制平面发起的，分析它们的安全性、可能遭受的网络攻击，以及流量变化的规律特点，能够为实现 SDN 中网络异常流量检测提供更加有效的支持。

1.1　针对转发平面的威胁及流量特点

转发平面又称数据平面，是由支撑南向接口协议的转发设备抽象出来的概念。由于当前 SDN 大都以 OpenFlow 协议作为南向接口，因此 OpenFlow 交换机是针对转发平面攻击的主要目标，它们可以是来自南向接口以下的网络设备或终端，如恶意交换机或恶意用户主机等。针对 SDN 转发平面的网络攻击如图 2 所示。

交换机作为底层流量数据的转发单元，对数据的存储和运算能力是有限的，因此对交换机的攻击手段主要为洪泛式的 DoS 类攻击（DoS 攻击或 DDoS 攻击），即利用大量的攻击数据包使其流表存储空间或缓冲区过载[16]。例如，恶意主机可以利用 SDN 控制器向交换机下发数据包处理指令这一特性，发送伪造包头的网络攻击流到交换机；由于交换机无法将这些流与自身现有的转发规则相匹配，故而发送 Packet_In 消息给控制器询问处置办法；控制器分析流的信息、生成对应的转发规则下发给

交换机；交换机将新规则形成流表项追加到自身流表[17]。然而，由于交换机流表存储空间有限，攻击流产生的大量新规则会导致交换机流表过载，无法再存储正常数据包的流表规则，损害了合法授权用户的流表可用性[18]。这类攻击的流量特点表现为交换机在短时间内接收大量非匹配流，并且转发给控制器的 Packet_In 消息也突然增多，从交换机到控制器链路中表现出明显的数据量骤增[19]。

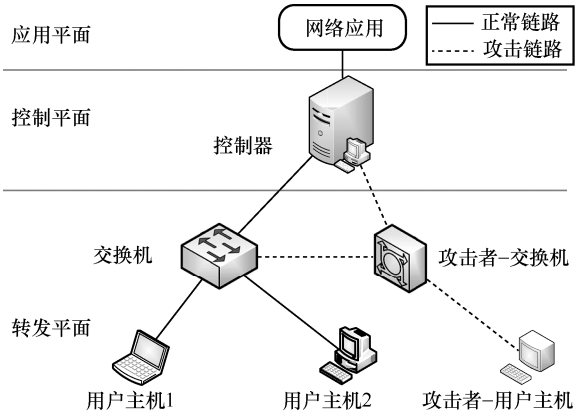

图 2 针对 SDN 转发平面的网络攻击

交换机缓冲区溢出也是网络攻击者的主要手段[20]。由于 OpenFlow 代理负责管理交换机与控制器之间的通信，当交换机接收到无匹配规则的数据包时，OpenFlow 代理会把包头信息封装在 Packet_In 消息中，把数据包负载暂存于缓冲区中。一些运行在低端服务器上的 OpenFlow 代理的数据存储能力有限，接收大量数据包后，缓冲区发生溢出，将无法存储合法的数据包[21]。这种攻击的流量特点表现为流入交换机的数据量多，而流出交换机的数据量少，两者之间存在较大差距[22]。另外，由于转发平面直接与外界用户连接，较其他层遭受的攻击更具多样性，如交换机劫持[23]、SDN 扫描[24]、地址解析协议（ARP）攻击[25]、病毒攻击等[26]。针对 SDN 转发平面的网络攻击类型及流量特征如表 1 所示。

1.2 针对控制平面的威胁及流量特点

控制平面包含若干 SDN 控制器，它们可以是主从关系，也可以是对等关系。控制器作为 SDN 集中化的决策核心，对上层按照各个应用程序制定的规则控制网络，监控网络状态和进行服务管理；对下层管理和调度转发平面的通信单元，实现底层基础设施资源的优化利用。因此控制器的运行状态直接影响着整个网络的服务质量，一旦受损，将导致整个 SDN 难以正常运转[27]。由于 SDN 在设计之初主要关注网络资源的调度与配置，其自身的安全并未作为主要问题被研究，因此控制器常常成为网络攻击者首选的高价值目标[28]。针对 SDN 控制平面的网络攻击如图 3 所示。

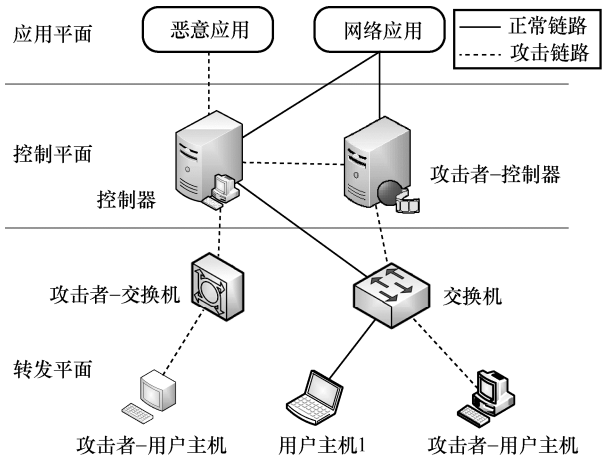

图 3 针对 SDN 控制平面的网络攻击

表 1 针对 SDN 转发平面的网络攻击类型及流量特征

攻击名称	组织方式	流量特点
DoS 类攻击（流表过载）	攻击者利用 DoS 攻击或 DDoS 攻击程序生成大量的非匹配流，控制器为交换机生成大量新的转发规则，导致交换机流表存储空间被耗尽，无法再为新的合法流提供正常的转发服务	短时间内大量非匹配流涌入交换机，交换机集中转发大量的 Packet_In 消息给控制器
DoS 类攻击（缓冲区溢出）	由 DoS 攻击或 DDoS 攻击程序发起，当交换机接收到大量非匹配流时，会将所有数据包的负载暂存于缓冲区；然而在向控制器询问处理办法期间，如果交换机缓冲区被填满，则会发生丢包问题，导致正常流的信息丢失	短时间内大量流传输至交换机，而交换机能正常转发的流量数据相对较少
交换机劫持[23]	将伪造链路注入现有的网络拓扑中，借用生成树服务“杀死”正常交换机端口；将恶意交换机的 MAC 地址与原交换机的 IP 地址映射匹配，并向控制器进行注册，取代原交换机与客户主机建立连接	大量数据流入原交换机，但该交换机无输出数据，而交换机所属网络与控制器之间却有流量的正常传输
SDN 扫描[24]	向目标交换机重复发送同一头域内不同地址的数据包，根据匹配流和非匹配流响应时间不同，确定是否有 SDN 交换机	某些时间段内，会有许多新的流从同一主机发往交换机，并且这些时间段相隔时间几乎相等
ARP 攻击[25]	攻击者发送大量包含 MAC 地址与 IP 地址错误映射关系的 ARP 数据包，使交换机无法保存正确的 MAC 地址信息，进而无法提供正常的转发服务	网络中突然出现大量 ARP 请求和响应数据包
病毒攻击[26]	攻击者产生大量具有随机 IP 地址的数据包对网络进行探测，并对存在的主机进行漏洞扫描，而后针对漏洞进行病毒传播	网络一定时间内产生大量网络流，且这些流中包含了很多空的、不可达的数据包

控制平面的安全威胁可能来自恶意应用、控制器、交换机和用户主机等任意的软件程序或硬件实体，图 3 展示了攻击源的位置。控制平面面对的这些威胁中大多以瘫痪控制器或影响控制器与交换机之间交互为目的，因此攻击者主要以过载控制平面的运算资源和网络链路为手段实现对控制器的攻击。控制器接受不匹配的数据包后，需要对这些数据包进行分析处理，然后形成处置规则下发到所管理的交换机，这个过程需要消耗控制器的运算、存储资源，如 CPU、内存、缓存等。

当攻击者对控制器发起的 DoS 类攻击时，大量的恶意请求数据包会逐渐耗尽控制器可用资源[29]，致使控制器难以及时处置合法的请求，降低整个网络的服务质量[30]。另外，消耗转发平面到控制平面的链路带宽也可以达到影响控制器工作质量的目标[31]。例如，SDN 交换机正常情况下只会将新数据包的包头信息封装后转发给控制器，而将数据包的负载存储在自身的缓冲区中。但当交换机遭受大量数据包的洪泛攻击造成缓冲区溢出时，交换机就会向控制器发送完整的数据包，这将可能引发交换机到控制器的通信链路拥塞[32]，导致合法用户的服务请求被延误甚至无法到达。另外，控制平面还可能遭受恶意应用攻击[33]、控制器劫持[34]、拓扑中毒[35]、控制器属性篡改[36]等网络攻击。针对控制平面的网络攻击类型及流量特征如表 2 所示。

如前文所述，在 SDN 控制平面和转发平面可能遭受的攻击中，DoS 类攻击形式最多、最易组织。攻击者只需操纵傀儡机向交换机发送大量看似正常的传输控制协议（TCP）、用户数据报协议（UDP）、互联网控制报文协议（ICMP）或域名系统（DNS）等攻击数据包，就能轻松地耗尽其资源；或者发送大量欺骗性的数据包到控制器使其过载，而无法再为后续到达的数据包提供服务。可以说 DoS 类攻击是 SDN 面临的最常见、威胁最大的网络攻击，有效地保护 SDN 免受 DoS 类攻击对维护 SDN 正常运行至关重要。

另外，SDN 的应用平面也可能遭受恶意应用的侵害，它们通过向控制器发送恶意指令来实现入侵或攻击。例如，针对控制器侦听机制的攻击，当控制器接收到来自数据平面的特定消息时，恶意应用通过干扰已注册侦听机制应用程序的顺序，使合法的应用程序因丢失控制信息难以正常运行[37]。然而，由于应用平面是由各种诸如入侵检测（防御）、流量控制、访问控制和负载平衡等网络服务和应用程序组成的，对它们的攻击组织复杂、成本较高、网络流量特征不明显，难以单纯地通过分析网络流量的方法检测出来。

2　SDN 中异常流量检测、溯源与缓解

一般来说，异常流量检测的目标是通过分析网络流量数据，发现网络中的攻击行为，为下一步消除攻击影响提供支持。由于 SDN 的可编程性，不少关于 SDN 中异常流量检测机制的研究中，将异常流量溯源与异常流量缓解也纳入其中，形成完整的 SDN 异常流量检测与防护系统，即在执行网络流量分析时，对异常情况也制定了应对策略[38]。为更加系统清晰地了解基于深度学习的 SDN 中异常流量检测的工作过程及特点，本文将分别从异常流量检测、异常流量溯源、异常流量缓解 3 个层次对当前的研究成果进行调研汇总。

表 2　　**针对控制平面的网络攻击类型及流量特征**

攻击名称	组织方式	流量特点
DoS 类攻击[29]（资源耗尽）	攻击者自主生成或者控制傀儡机生成一些无意义的流，以触发交换机发送大量的 Packet_In 消息到控制器，使控制器过载而无法响应正常的服务请求	交换机到控制器的链路中传输着大量的 Packet_In 数据包
DoS 类攻击[32]（链路拥塞）	攻击者发送大量无意义的流或完整的 TCP 数据包到控制器，极大地消耗转发平面到控制平面的链路带宽，使正常的服务请求无法到达控制器	短时间内，交换机到控制器的链路中传输高速率的上行流量
恶意应用攻击[33]	攻击者开发恶意应用通过北向接口操纵控制器，使其无法对外提供正常服务，甚至成为网络攻击的工具	通常表现为控制器将大量网络流量引导至特定的交换机或主机，网络中的流量表现出异常的爆发性、定向性
控制器劫持[34]	攻击者发送虚假信息到交换机，将伪造的控制器迁移至目标网络，对原控制器实施屏蔽	原来合法控制器中没有流量传输，但所管理的交换机中有流量传输
拓扑中毒[35]	攻击者向网络中发送伪造的数据包，或向目标交换机重新投放一些来自另一个目标交换机的真实链路层发现协议（LLDP）数据包，使控制器获得虚假的链路信息，从而建立错误的拓扑结构	控制器建立错误的拓扑结构，交换机能够接收网络流量，但能被正常转发的网络流量很少
控制器属性篡改[36]	恶意应用通过篡改交换机的属性，如配置属性、消息属性等信息，使控制器程序进程出现混乱，无法正常工作	交换机发送给控制器的消息很少得到回应，交换机与控制器间链路中数据流呈现单向性

2.1 SDN 中异常流量检测

经过多年的研究探索，人们对 SDN 中异常流量的检测任务提出许多不同的解决思路。主要有基于统计的检测方法、基于信息论的检测方法、基于机器学习的检测方法，以及当前的研究热点——基于深度学习的检测方法。基于统计的检测方法主要通过统计过去的网络流量信息变化情况来预测当前的网络状态，当发现真实状态与预期的情况不符时，则认为网络中存在异常。通常网络中的数据包都可以被及时准确地转发，Tang 等[39]观察到异常流量在短时间内汇聚到瓶颈链路时，大量数据包因得不到及时转发而被丢弃的现象，于是提出基于端口数据包统计量的异常检测方法。如果检测到流出交换机与流入交换机数据包的数量差距超过某阈值，则判定流经该交换机的流量存在异常。为提升模型的检测精度，李传煌等[40]根据网络流量的统计信息设计出单流增加速率、不同端口增长速率、流表平均数据包量、流表平均比特数以及流平均持续时间等特征向量增强特征的信息量。然而，基于统计的检测方法需要通过对大量数据样本进行统计运算才能得到较准确的结果，否则仅通过少量样本难以实现对异常流量的有效检测；另外，对不能引起明显网络波动的异常流量难以检测。

基于信息论的检测方法主要是利用流量特征的互信息性来计算熵值或散度，从而识别异常分布。Mousavi 等[41]提出基于 IP 地址熵变的检测方法，根据目的 IP 地址的熵变化来检测 SDN 中的 DDoS 攻击，并取得一定效果。Ujjan 等[42]提出了一种基于广义熵的快速有效的 DDoS 流量检测方法。该方法利用香农熵和雷尼熵定义的广义熵来估计 DDoS 流量的特征分布，并帮助 SDN 控制器有效地处理的恶意流量。Kalkan 等[43]首次提出基于联合熵的 SDN 保护方案，由于采用数学解决方法来检测和减轻异常带来的影响，因此该方案理论上不仅可以有效地缓解已知形式的攻击，还能减轻未知攻击造成的影响。不过，基于信息论的检测方法很难检测出流量中的稀疏异常，并且无法处置高速率、大容量的流量数据。

基于机器学习的检测方法则是将机器学习算法应用到 SDN 的异常流量检测中，如支持向量机[44]、决策树[45]、K 近邻[46]、K-Means 聚类[47]、多层感知机[48]以及由它们联合构造出的检测方法[49-50]。例如，Yilmaz 等[51]利用支持向量机的核函数将输入的低维流量数据转换到高维空间，然后利用支持向量机创建最优决策边界，从而提高对异常流量检测的效率和准确率。Ali 等[52]设计出一种基于改进型决策树的轻量级 DDoS 攻击检测与缓解系统，采用杂质剔除和错误修剪策略来检测流量中的 DDoS 攻击流，并结合动态白名单机制，阻止攻击流量进入 SDN。Madathi 等[53]使用攻击流量的特征子集训练 K 近邻算法，该算法可以对流量数据中的攻击流量进行聚合分类；另外，他们通过一定策略在 SDN 的网络服务功能和异常检测效果之间实现平衡。Cui 等[54]提出基于流量分布不均衡的 K-Means 聚类算法，该算法实现对 SDN 中的 DDoS 攻击流量的实时检测。Wei 等[55]针对浅层机器学习方法无法应对携带恶意载荷的 DDoS 攻击的问题，提出一种基于多层感知机的深度学习模型，该模型使用自编码器压缩和简化特征，这样可以减少有噪声数据的计算开支和结果偏差。联合方法则是将几种检测方法进行集成，它们可以单独训练也可作为整体统一训练，并按策略汇总每种检测方法的结果作为最终检测结论。文献[56]将支持向量机、随机森林、梯度增强机器分类器 3 种方法集成后对 SDN 中 DDoS 攻击流量进行检测，并利用优化后加权投票集成方法得到最终结果。

然而，无论是基于独立机器学习的检测方法还是联合的检测方法，所用的特征数据依赖人工完成，导致异常流量的检测效果受限于特征设计人员的专业素质和工作经验。另外，大多数基于机器学习的研究还会结合特征选择技术来选取最佳特征，以提高对网络异常流量检测的准确率，然而这种做法给控制器增加了大量的额外开销。

深度学习属于机器学习的一个分支，是一种基于神经网络算法的机器学习，它能够利用多层神经网络从非结构化的数据中逐层学习数据的高层次特征。不同于传统的机器学习需要特征工程配合才能完成对数据的分析与处理，深度学习能够实现以原始流量数据为输入、最终分类结果为输出的端到端工作模式。目前，深度学习被广泛应用于自然语言处理、机器视觉、序列数据预测等领域，在 SDN 异常流量检测的研究活动中也取得许多成果。

根据深度学习模型训练时使用的流量数据是否有标签，可以将基于深度学习的 SDN 异常流量检测方法分为基于有监督学习的异常流量检测、无监督学习的异常流量检测、半监督学习的异常流量

检测 3 种方法[57]；另外，根据所用的神经网络模型不同，还可分为基于卷积神经网络（CNN, convolutional neural network）[58]、循环神经网络（RNN, recurrent neural network）[59]、自编码器（AE, autoencoder）网络[60]、深度信念网络（DBN, deep belief network）[61]以及生成对抗网络（GAN, generative adversarial network）[62]等方法，具体如图 4 所示。

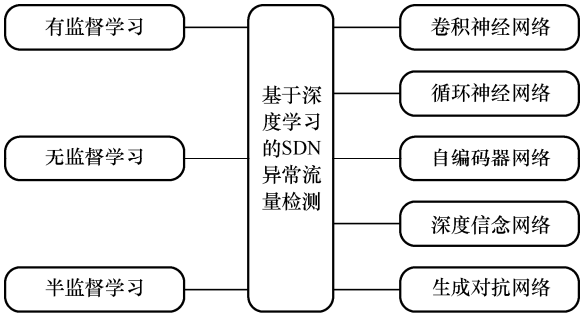

图 4　基于深度学习的 SDN 异常流量检测方法分类

1) 有监督学习的异常流量检测又被称为预测或定向分类，使用大量有标签样本训练，模型可以预先识别样本所属的类别并从中学习到分离的边界，因此有监督学习的检测方法通常比无监督学习方法具有更好的检测精度。CNN 和 RNN 都是典型的有监督学习模型，它们分别凭借自身出色的空间特征提取能力和时间特征提取能力在异常流量检测中发挥作用。例如，文献[63]提出基于正则化 CNN 和长短期记忆（LSTM）网络的流量异常检测模型，先把 SDN 流量数据分析的专用数据集——InSDN 中每条网络流的 48 个特征转换为的二维图像格式，利用 CNN 学习网络流的空间特征，再利用 LSTM 网络学习网络流的时序特征，从而准确地刻画网络流量行为的时空特征，这个方法比单独使用 CNN 或 LSTM 模型具有更好的异常流量检测效果。然而，由于原始样本类别是不平衡的，需要人工对训练数据进行平衡化处理，这导致有监督学习的检测模型得到的总是次优解[64]。此外，现实中难以获得大规模清晰可用的有标签数据，因此有监督学习的异常流量检测技术不如无监督学习或半监督学习的方法受欢迎。

2) 无监督学习的异常流量检测更专注于对数据内在特征的理解和解释，由于有标签数据很难获得，因此通常利用无监督异常检测技术对无标签数据样本进行自动标注[65]。常用的模型结构有深度信念网络、自编码器网络、生成对抗网络等，它们假设正常实例比异常实例有更高的普适性。Wang 等[66]提出了一种基于 DBN 的 DDoS 攻击检测方法，通过提取 OpenFlow 交换机流表条目的特征，训练 DBN 算法来检测网络中是否存在 DDoS 攻击。Shone 等[67]提出基于无监督特征学习的非对称深度自编码器（NDAE）的异常流量检测模型，利用多隐层自编码器逐层提取流量数据的高阶特征，最后利用分类器实现对异常流量的自动识别。然而，由于需要对数据分布进行先验假设，无监督学习的异常流量检测算法的准确率通常比较低。

3) 半监督学习的异常流量检测是有监督学习和无监督学习方法的结合，其思想是利用学习到的有限样本分布对未标注样本进行分类，通常可分为 2 种情况。一种情况是仅有少量有标签数据而大部分为无标签数据，通常利用少量有标签数据和部分无标签数据共同建模。Wang 等[68]利用少量有标签数据和大量无标签数据进行模型训练，首先将 SDN 流量数据包的数据截断或用 0 填充转换为长度一致的数据包字节向量；然后把多个标准化数据包字节向量样本输入半监督模型 ByteSGAN 中，对生成器和判别器进行交替训练，这种多样本同时训练的方式可以有效克服样本标签数量不足难以建模的问题。另一种情况是仅使用正常数据建模，利用正常样本数据对深度自编码模型进行充分的半监督训练[69]，训练好的模型可以对正常样本进行很好的重构，重构样本与输入样本的重构误差较小；而对于输入的异常样本则难以有效重构，会出现较大的重构误差，将该误差与判定阈值比较，即可完成对样本是否为异常的判定[70]。

由于正常样本的标签比异常样本的标签更容易获取，因此，融合有监督学习和无监督学习优点的半监督学习异常流量检测方法正在被越来越多的研究者关注。另外，集合了多种模型结构的混合型异常流量检测算法，通过检测阶段任务分工或检测结果综合集成的策略，可以明显提升对异常流量的检测能力，已成为网络安全领域的研究热点。基于深度学习的 SDN 异常流量检测方法的性能与特点如表 3 所示。从表 3 可以看出，有监督的异常流量检测方法[71-78]的精度总体高于半监督或者无监督的检测方法，半监督的检测方法总体高于无监督的检测方法；另外，由于半监督的检测方法[79-80]不需要使用大量带标签的样本，节省了人工标记的成本，且具有较高的检测精度，因此广大研究人员期望在半监督的检测方法的研究中取得突破。

表 3　　基于深度学习的 SDN 异常流量检测方法的性能与特点

算法名称	年份	监督类型	算法描述	数据集	准确率	召回率	精确率	优势	不足
DCNN[58]	2020 年	有监督	利用深度卷积神经网络提取流量数据空间特征，根据特征实现对流量的分类	CIC-IDS2017	0.994 5	0.996 4	0.995 7	检测准确率较高、计算开支小	非真实 SDN 环境中数据，需要提前对训练数据进行标注
DNN-LSTM[59]	2023 年	有监督	利用深度 LSTM 分类器，学习流量数据的时间关联性，检测僵尸网络	CIC-IDS2017	0.993 2	0.993 0	0.993 0	检测准确率较高、误报率低，可检测对多类恶意软件产生的流量	算法复杂、非真实 SDN 环境中数据
SSAE-SVM[60]	2022 年	有监督	两阶段检测，先用信息熵方法快速识别可疑流量，再用堆叠稀疏自动编码器与支持向量机架构对可疑的异常流量进行确认	自采数据集	>0.98	—	—	检测数据符合 SDN 环境特点，检测精度较高	模型复杂、计算和网络开销大
DBN-TWD[61]	2022 年	无监督	OpenFlow 流表中手动提取的特征字段构造特征形成流表特征集，利用 DBN 提取特征，然后使用三向决策检测模型来执行流的入侵检测	自采数据集	0.957 0	—	0.943 0	利用 K 近邻算法对深度学习模型检测的边界结果进行再分类，提升检测的准确率和减少误报率	模型设计复杂，计算开销大
GAN[62]	2021 年	无监督	使用 GAN 对 IP 流进行连续监控，以检测 DDoS 攻击，并用对抗性训练降低系统对攻击扰动的敏感性	CIC-DDoS2019	0.943 8	0.978 9	0.940 8	能够有效地检测出常见类型的 DDoS 攻击，具有一定的抗干扰能力	非真实 SDN 环境中数据，系统部署在控制器上运行，增加了额外的负载和开销
CNN-LSTM[63]	2021 年	有监督	将检测数据结构化，利用 CNN 和 LSTM 提取时空特征，使用 Softmax 完成检测	InSDN	0.963 2	0.972 4	0.976 0	检测精度比单独使用 CNN 或 LSTM 模型的精度高	算法相对复杂，吞吐量小和时延高，难以适应在线检测需求
DBN[66]	2023 年	无监督	提取 OpenFlow 交换机流表条目的特征，训练 DBN 算法模型来检测是否存在 DDoS 攻击	自采数据集	0.996 0	0.946 0	0.973 0	检测精度较传统方法有一定提升	检测时间开销较大
S-NDAE[67]	2018 年	无监督	多隐层自编码器逐层提取流量数据高阶特征，利用重构误差实现对异常流量的检测	NSL-KDD	0.892 2	0.892 2	0.929 7	检测数据容易获取，可提取数据的高阶特征，检测时间减少	非真实 SDN 环境中数据，模型结构复杂，检测准确率较低
ByteSGAN[68]	2021 年	半监督	将数据截断或填充为标准字节向量，利用有标签和无标签数据组成的多样本同时对模型交替训练，克服标记数据不足的问题	ISCX2012	0.991 8	—	—	有效地利用未标记样本和生成样本进行训练，对加密流量检测时可以取得较好的检测效果	非真实 SDN 环境中数据，当样本充足时优势不明显，且算法较为复杂
GRU[71]	2023 年	有监督	使用门控递归单元对单个 IP 流进行分析，检测 DDoS 攻击	CIC-DDoS2019 CSE-CIC-IDS 2018	0.999 4 0.970 9	0.999 4 0.947 0	0.999 4 0.999 4	对流进行细粒度检测，准确率较高	非真实 SDN 环境中数据，计算开销大
DL-EWPS[72]	2022 年	有监督	利用新的快速转换数值方法，将流量数据转为 RGB 图像数据，使用 RNN 进行准确分类	InSDN	0.989 4	0.984 0	0.980 0	检测准确率高，时延低，适于大规模网络中异常的检测	算法复杂，安装在控制器上，增加了额外开销
Bi-LSTM[73]	2023 年	有监督	将数据包特征转换为窗口特征，利用双向 LSTM 学习数据特征，分类器实现异常判定	ISCX-IDS2012	0.998 7	0.997 4	0.998 7	高准确率和低损失率	非真实 SDN 环境中数据，需要提前对训练数据进行标注
CNN\LSTM\GRU[74]	2022 年	有监督	集成 CNN、LSTM、GRU 等多个深度学习模型，构建多阶段的异常流量检测框架	CIC-IDS2017	0.997 7	0.970 0	0.980 0	集成多个深度模型的特征提取优势，提升了对 SDN 流量的分类效果	数据不能反映 SDN 环境特征，算法复杂，检测耗时长
DDosNet[75]	2020 年	有监督	利用 RNN-AE 与 Softmax 函数构建回归模型用于对流量分类	CIC-DDoS2019	0.990 0	0.990 0	0.990 0	模型易训练、检测准确率高	数据不能反映 SDN 环境特征，计算开销大
DeepIDS[76]	2020 年	有监督	在 SDN 架构中搭建入侵检测系统，分别用 DNN 和 RNN 进行测试	NSL-KDD	0.807 0（DNN） 0.900 0（RNN）	0.810 0（DNN） 0.890 0（RNN）	0.850 0（DNN） 0.890 0（RNN）	验证了深度学习方法能够用于 SDN 环境中基于流的异常检测	数据不能反映 SDN 环境特征，检测精度低，耗时短
Cu-DNNGRU&Cu-BLSTM[77]	2021 年	有监督	使用 DNNGRU 和 BLSTM 混合框架检测物联网环境中复杂的威胁和恶意软件，并支持 Cuda 的 GPU 提升运算性能	CIC-IDS2018	0.998 7	0.999 6	0.998 7	检测精确度高，速度较快	数据不能反映 SDN 环境特征，模型庞大，参数多
DCNN[78]	2023 年	有监督	构建基于深度 CNN 优化模型的网络流量分类器	InSDN	0.999 9	0.999 9	0.999 9	检测速度快，准确率较高	使用带标签的数据训练，无法检测未知异常
GRU-DAE[79]	2022 年	半监督	GRU 和 DAE 结合，利用有选择机制的监督异常检测来辅助半监督异常检测	NSL-KDD	0.902 1	0.909 7	0.888 0	能够检测未知网络攻击	数据不能反映 SDN 环境特征，且检测准确率低
BDLSTM-AE[80]	2022 年	半监督	将双向长短期记忆网络和自编码网络结合，构建深度堆栈自编码异常检测模型	ISCX-IDS2012 UNSW-NB15	0.993 0 0.999 4	0.999 9 0.999 9	0.999 9 0.999 9	模型稳定性强、检测精度高	数据不能反映 SDN 环境特征，模型较复杂，检测耗时长

从表 3 还可以看出，当前基于深度学习的 SDN 异常流量检测的研究成果具有模型结构多样、检测精度较高的特点。但每种检测方法也都存在着各自的缺点和不足，总体表现为以下几点：一是检测系统部署在控制器上，虽然取得了较高的检测精度，但存在算法复杂、计算开销大、带宽消耗多的问题；二是大多数模型检测能力单一，它们在特定数据集上表现出良好的检测能力，但在其他网络环境中检测效果未知，而且有些检测方法在理论上不具备检测新的未知攻击的能力；三是建模过程依赖有限的离线数据，检测策略更新滞后，且所用数据集难以反映 SDN 环境特征，检测方法很难满足海量、多变的 SDN 中在线流量数据的检测需求；四是大部分检测模型局限于单节点设备，缺少对 SDN 整体系统性的检测防护需求和体系化处置策略的考虑。

2.2　SDN 中异常流量溯源

异常流量溯源是当系统检测到异常流量后，对异常流量源头的追溯，是实现网络体系安全防护的必要环节。SDN 中异常流量溯源是利用一定的技术与方法，根据 SDN 的拓扑结构，通过分析网络中不同节点间的驱动数据，追溯异常流量的传输路径，确定网络攻击发起的确切位置，对阻止网络攻击威胁、提高网络安全防护水平、调查取证网络安全事件具有重要意义。SDN 中异常流量溯源的一般模型如图 5 所示。

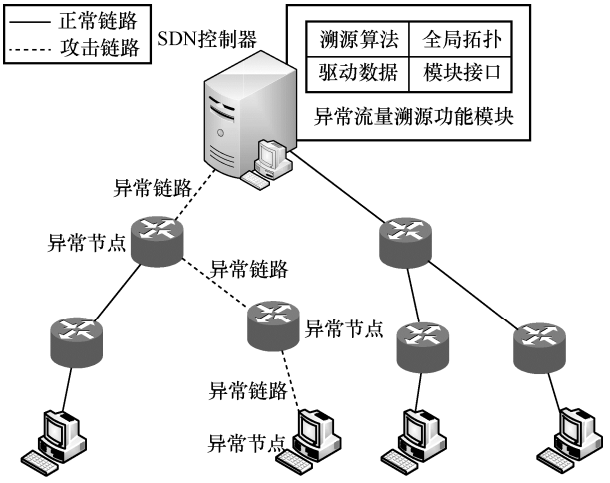

图 5　SDN 中异常流量溯源一般模型

SDN 对网络集中控制的可编程性为实现异常流量溯源提供了丰富的技术手段，目前研究中对 SDN 中异常流量进行溯源的方法可以分为数据包追踪法、链路测试法和日志分析法等 3 种。

1) 数据包追踪法是最常用的异常流量溯源方法，主要通过分析流量数据包头部的相关字段，然后按照一定策略进行分类，逐层判断出异常数据包经过的网络链路及节点，进而查找到发出异常流量的终端设备，最终形成完整的异常流量传输途径。豆健[81]在利用自定义的数据结构获取存储 SDN 拓扑信息的基础上，提出了根据 OpenFlow 交换机流表提取端口信息进行攻击追踪的溯源办法，该方法通过聚合交换机内转发路径的数量，找到攻击数据包进入交换机的端口；利用网络拓扑信息，定位该端口连接的上一跳设备，如设备为交换机则作为攻击路径中的一个节点，再向上寻找；如此循环，直到找到攻击主机。Wang 等[82]利用发送给控制器 Packet_In 消息的交换机 ID 和 in_port 编号，定位交换机的位置及异常流量进入交换机的端口，然后以时间戳 t_stamp 字段为标准，对到达控制器的 Packet_In 消息进行排序；根据 Origin 字段值判断攻击源是否属于当前控制器管理区；再利用 src_ip、dst_ip、protocol、eth_type、src_mac 和 dst_mac 等 6 项数据包的头部字段确定攻击者所在的控制器，以及为异常流量提供转发服务的第一个交换机和流入端口。郭笛[83]提出一种基于核度理论与基于标记的攻击源追溯方法。首先获取 SDN 中各交换机信息并持续分析它们，通过比较恶意流量数量和恶意流量比例确定是否将交换机标记为恶意交换机；结合全局网络拓扑结构，追溯恶意流量通过的路径；再分别利用核度理论和图论知识定位攻击核，并生成有向赋权的攻击路径图；同时，对交换机是否被标记为恶意交换机的结果进行统计分析和制定追溯策略，以达到追溯攻击源头的目的，这种方法避免了数据的重复调用，具有算法复杂度低、溯源效率高的优势。Nadeem 等[84]借助图论的方法，找到攻击流量进行 SDN 时所经过的交换机，从而复刻出攻击流的传输路径。

2) 链路测试法是先构建出全局拓扑结构，再利用一定方法对网络中的链路或节点的相关特征进行检测，从而实现异常流量传输路径的刻画。例如，魏松杰等[85]提出的利用探测流表项进行欺骗数据追踪的方法，通过控制器向交换机中添加与欺骗数据包精确匹配的探测流表项；当欺骗数据包经过该交换机时，交换机就会向控制器发送 Packet-in 消息，控制器则根据该消息并结合全局拓扑信息获得其上一跳节点信息，并将其加入溯源路径树中；如

果上一跳节点是交换机，则将其作为当前交换机，继续发送探测流表项到它的下一跳节点，当查找到交换机连接的主机时，溯源结束并返回该条路径。Chen 等[86]把溯源作为 DDoS 攻击检测与防御的主要过程，监控 SDN 中的所有基站（BS）节点的吞吐量特征值的变化情况，将变化量超过阈值的节点添加到异常树中；然后，遍历异常树中的节点，并利用 DDoS 检测算法对其进行检测，只保留检测结果为 DDoS 攻击的节点，将流量突变对应的正常节点从异常树中移除；最后，返回 DDoS 的攻击路径。由于该溯源工作只将吞吐量作为特征值避免了多流表问题，与逐条检测网络流的方法相比，该方法只检测异常树中的 BS 节点，有效地减少了时间和资源上的消耗。

3) 日志分析法也是通过分析数据包信息实现溯源目标的方法。与数据包追踪法的不同之处在于，日志分析法的数据包信息通常是从主机或网络的日志记录中获取，而不是直接从网络中采集得到。传统的日志分析法通过路由器记录完整的数据包信息，在受害主机发出溯源请求时，递归地向上游路由器发送查询消息，逐层完成溯源路径的重构。但这种方法需要路由器有很大的存储空间，并且路由器的性能会随着存储空间的不断消耗而下降[87]。Hadem 等[88]改进了传统的由路由器执行日志文件记录的做法，利用 SDN 集中控制的优势，在控制器内存上利用轻型数据库 SQLite 执行选择性的日志记录操作。控制器只记录被检测为异常流量的首个数据包的 dpid、in_port、src_ip、dst_ip、protocol、eth_type、src_port、dst_port、origin 和 t_stamp 等 10 个字段的信息。进行回溯操作时，网络管理员只需分析这些选择性的日志记录，即可还原出异常数据包的实际传输路径，该方法相比传统的基于文件日志记录的方法存储空间减小 90%～95%，响应时间缩短 9.76%。但该方法对来自 SDN 外部的数据包的支持效果不好，只能追溯到异常数据包进入 SDN 时经过的第一个 OpenFlow 交换机。

表 4 展示了几种 SDN 中异常流量溯源方法。

2.3 SDN 中异常流量缓解

SDN 中大多数网络攻击都是通过不断消耗 SDN 的计算、存储、带宽等可用资源，使其无法为合法用户提供正常服务。如果 SDN 有充足可用资源，那么即使网络中存在攻击也不会降低网络用户的使用体验[89]。因此，缓解异常流量对网络的影响是 SDN 安全防护任务的根本目标。SDN 中异常流量缓解是为阻止或减缓异常流量对网络进一步破坏，维护网络的正常运行而采取的应对措施，是阻止异常流量影响网络服务质量的有效手段。当前异常流量缓解的思路可以归纳为两类：1) 对异常流量进行限制，主要方法有阻止或减少异常流量在 SDN 中的传播，如丢弃异常流量[90]、限制异常流量的传输速率以及将异常流量转发至特定路径等；2) 对网

表 4 SDN 中异常流量溯源方法

文献	类别	算法描述	优点	不足
文献[81]	数据包追踪法	利用自定义的数据结构获取当前网络完整的拓扑结构；根据 OpenFlow 交换机端口信息，逐跳查找攻击源	溯源算法简单，不产生额外网络流量，计算开支小	错误率高，可能会将正常的大批量分布式传输的数据当作异常流量进行溯源
文献[82]	数据包追踪法	根据 Packet_In 消息定位攻击交换机，再利用数据包头部的 IP、Mac 等字段信息回溯转发恶意流量的第一个交换机及端口	利用控制器自带功能提取特征字段，不需要复杂运算，即可实现对发出恶意流量的交换机的定位	仅能实现交换机级别的恶意流量的粗粒度溯源
文献[83]	数据包追踪法	核度理论与图论知识定位攻击核，生成赋权的攻击图；利用标记的恶意交换机，追溯攻击源头	溯源的同时可有效地阻止网络攻击流量进入 SDN	溯源的精确度不高，可能将正常的高速率流量误作为异常流量。
文献[84]	数据包追踪法	基于图论概念刻画网络中的攻击路径，并根据路径找到攻击流进入 SDN 时所经过的边缘交换机	算法简单，易于实现	无法实现对复杂攻击源的追溯，并且无法甄别虚假路由信息
文献[85]	链路测试法	在交换机添加与欺骗数据包匹配的探测流表项；目标欺骗数据包经过交换机触发 Packet_In 消息，控制器据此获得攻击路径	不影响其他正常数据流的转发，可动态查找欺骗数据包的转发路径；准确率高，系统开销小	数据特征需要人工分析提取；缺乏 Packet_In 消息限速方案，可能引发通信链路拥塞。
文献[86]	链路测试法	基于基站流量的变化建立异常节点树，检测并裁剪正常的节点，最后生成攻击路径	溯源机制仅在发现异常时被调用，占用 CPU 和内存资源较少	剪枝过程中容易将真实的异常流量源头剔除，造成较高的漏报。
文献[87]	日志分析法	根据日志分析经过路由器完整的数据包信息记录，递归地向上游路由器发送查询消息	逐层溯源路径，准确完成攻击路线重构	消耗路由器空间，路由器性能会随存储空间消耗而不断下降。
文献[88]	日志分析法	控制器选择性地记录日志信息；分析部分相关的溯源参数，建立异常流量传输路径	控制器存储选择性的日志文件，节省存储空间，回溯效率高	当异常数据包来自于受支持网络之外，追溯操作只能执行到受支持网络的最后一个节点

络资源进行均衡，利用 SDN 集中控制的优势动态调配网络资源，增强 SDN 对异常流量的容忍度，如动态调整控制器或交换机的任务分配，将过载设备的网络任务迁移到轻负载设备上。

在限制异常流量的策略中，直接丢弃异常流量是最直接的办法，具有操作简单、效率高的特点。如 Wang 等[82]在进行异常流量检测和溯源时，同时建立了异常流黑名单，通过控制器向交换机下发丢弃黑名单中异常流的规则，当黑名单中的数据流经交换机时将被直接丢弃。类似地，Cao 等[91]分别对合法流建立白名单，交换机对不符合白名单的流量数据直接丢弃。对攻击主机进行传输限制就是根据检测结果，对不同的流赋予不同的转发优先级或权重，如对于合法的正常流赋予较高的转发优先级或权重，而对于异常的流则赋予较低的优先级或权重，以减少异常流量在网络中的存在，从而保证合法流可以得到更多的网络资源和服务。例如，Yungaicelanaula 等[92]根据控制器对用户的响应时间不同判定流的属性，并对流进行优先等级区分，对合法流给予高质量的转发路由，将非法流引导到特定路径进行丢弃。Sudar 等[93]通过分配不同转发时长来达到抑制非法流的目标，对可信源 IP 发出的流量数据分配较长的转发时长，而对可疑源 IP 发出的流量数据只给予较短的转发时长。Kamel 等[94]利用图神经网络，对链路的发送权重进行动态调整，将权重变化过大的链路判定为异常链路，并在一定时间内将异常链路发出的新流引入默认端口进行丢弃处理。

均衡网络资源就是通过一定措施，对所有控制器或交换机的任务进行统一调配，把重负载设备上的任务迁移到轻负载设备上，以缓解攻击对 SDN 中部分设备的压力。Filali 等[95]利用博弈论的思想，把控制器对交换机分配任务的问题转化为一对多的匹配博弈问题，将交换机动态分配给控制器，并确保每个控制器必须达到一定的最小配额，从而实现网络负载的平衡。Kamel 等[96]利用最小二分法对交换机与控制器之间的往返时间和控制器负载性能进行折中，把流建立时间和设备负载平衡进行统一调度。Yuan 等[97]提出一种在 SDN 中应对 DDoS 攻击的网络资源管理机制，结合 SDN 拓扑结构，利用排队模型评估 SDN 对 DDoS 攻击抵抗力，网络管理员通过对 SDN 交换机和控制器资源的合理调配，实现对 DDoS 攻击的防御来保证 SDN 的网络服务质量。Gillani 等[98]提出了一种能够弹性控制网络的架构（ReCON），其核心思想是最大限度地减少控制平面和数据平面之间的关键链路的共享，并利用空闲的 OpenFlow 代理来弹性地增加其 SDN 总的可用容量，从而缓解异常流量对网络传输质量的影响。

表 5　　SDN 中异常流量缓解方法

文献	算法描述	优点	不足
文献[81,90-91]	异常流量检测时建立黑名单（白名单），交换机直接丢弃黑名单中（不在白名单）的流数据	操作简单，不产生额外通信开支，处置效率高	操作依赖异常检测结果，可能造成正常流量数据的误丢弃
文献[92]	控制器根据响应时间判定流的属性，进行优先级划分，对合法流给予高质量的转发路由，将非法流引致特殊路径丢弃	可以保证合法流得到优质的网络服务	可能会将持续时间较长的合法流误判为非法流，造成误丢弃
文献[93]	对可信源 IP 发出的流量分配较长的转发时间，对可疑源 IP 流量给予较短的转发时长	被误报的正常流也有一定的转发权限，保证了正常流量开展业务	不能从根本上禁止非法流进入 SDN，网络设备仍存在过载风险。
文献[94]	利用图神经网络，对链路的发送权重进行动态调整，将权重变化大于阈值的链路判定为异常链路，并将其发出的新流引入到默认端口丢弃	可以根据链路中流量的传输速率动态调整网络资源，有利于资源优化配置，可实现异常流量的在线检测	进行异常链路判定的阈值需根据 SDN 环境的变化适时调整，目前只能凭经验由人工完成
文献[95]	将控制器对交换机分配任务的问题转化为一对多的匹配博弈问题，并要求每个控制器必须达到一定的最小配额	从控制层面实现网络负载的平衡	增加网络通信量，无法缓解对交换机端攻击带来的影响
文献[96]	利用最小二分法对交换机与控制器之间的往返时间和控制器负载性能进行折中	在流建立时间和设备负载平衡之间统一调度，保证网络稳定运行	难以实现对大规模分布式 SDN 中设备的负载均衡
文献[97]	利用的排队模型评估 SDN 对 DDoS 攻击抵抗力，网络管理员通过对 SDN 交换机和控制器资源的合理调配，保证 DDoS 攻击发生期间网络服务质量不发生明显下降	静态的资源分配方法可以保证持续的正常网络服务	需要根据交换机的位置和数量综合考虑计算开支，配备性能相匹配的服务器
文献[98]	建立弹性控制网络架构，最大限度地减少控制平面和数据平面之间的关键链路共享，并利用空闲的 OpenFlow 代理来弹性地增加容量	资源优化配置，平均计算开支小	无法满足业务繁忙的 SDN 中异常流量的缓解需求

从表 5 展示的几种异常流量缓解方法的性能特点可以看出，无论是对主机传输限制还是采用设备负载均衡的方法，虽然都可以对异常流量进行有效的限制，但却难以隔离所有的异常流量，因此 SDN 中的网络设备仍存在过载风险。攻击流在交换机中的流表项不会立即自动删除，需要等待其过期，或者与攻击溯源配合把恶意攻击流的相关流表项删除，才能释放交换机的存储空间。另外，目前大多数的解决方案都需要添加新组件，或通过交换机控制消息实现，增加了网络中的通信量和控制器运算开支。

3 常用的实验数据集及预处理方法

3.1 常用的数据集

从表 3 可以看出，当前基于深度学习的 SDN 异常流量检测研究中除一些自采数据集，常用的数据集有 NSL-KDD、UNSW-NB15、ISCX-IDS2012、CIC-IDS2017、CIC-IDS2018、CIC-DDoS2019 和 InSDN 等。

NSL-KDD 是网络安全领域中最著名和最常用的网络流量数据集，它对 KDD99 进行了改进和修正，删除了重复、缺损的数据，并进行样本类别平衡[99]。KDD99 是从 DARPA 数据集进行特征提取后得到的，每条记录包含 41 个不同的属性特征，其中连接特征 9 个、内容特征 13 个、时间网络流量特征 19 个、主机流量特征 10 个，而 NSL-KDD 比 KDD99 还多了一个关于流量严重性的特征[100]。NSL-KDD 中的攻击类型有 4 种，包括 DoS 攻击、Probe、远程到本地非法访问（R2L）和普通用户对本地超级用户特权的非法访问（U2R）。长久以来，NSL-KDD 一直作为 Benchmark 被广泛应用于入侵检测系统或异常流量检测方法的性能评估，有时也作为时间序列数据参与其他模型的检测实验[101]。

UNSW-NB15 的原始数据集是澳大利亚网络安全中心使用 IXIA 网络流量工具创建的，后来经过 Bro IDS 分析工具处理，形成.csv 格式的入侵检测数据集[102]。整个数据集共有 2 540 044 条数据记录，每条记录有 46 个属性特征，其中 4 个流特征、13 个基本特征、8 个内容特征、9 个时间特征、5 个生成通用特征和 7 个生成连接特征。攻击流量主要由蠕虫、侦察、端口扫描、后门利用、DoS 攻击和模糊攻击等 9 种攻击产生。UNSW-NB15 的训练集和测试集具有的样本分布相似、数据友好性使其成为入侵检测研究中较为常用的数据集。

ISCX-IDS2012 是加拿大网络安全研究所（CIC）于 2012 年开发的入侵检测数据集，研究人员使用了 2 个配置文件，一个用来生成超文本传送协议（HTTP）、简单邮件传送协议（SMTP）、邮局协议版本 3（POP3）、因特网信息访问协议（IMAP）、文件传输协议（FTP）、安全外壳（SSH）协议等协议产生的正常流量；另一个用来生成针对 HTTP 的 DoS、DDoS 攻击、SSH 暴力攻击产生的恶意流量[103]。由于网络配置环境单一，ISCX-IDS2012 的流量数据比较“纯净”，并且它还提供以.pacp 格式获取和存储原始流量，包含完整的有效载荷信息。数据的纯净性和完整性使 ISCX-IDS2012 成为早期至现在都较受欢迎的异常检测（入侵检测）实验数据集[104]。

后来，加拿大网络安全研究所还陆续推出了 CIC-IDS2017、CIC-IDS2018、CIC-DDoS2019 入侵检测数据集，它们的正常流量是利用 HTTP、HTTPS、FTP、SSH、email 等协议构造出的 25 个抽象用户行为来模拟真实网络产生的，攻击（异常）流量则由不同的网络攻击程序生成。例如，CIC-IDS2017 的异常流量使用 DoS、DDoS、Web Attack、Botnet、Brute Force、Heartbleed 和内网渗透等 7 种攻击行为产生[105]。CSE-CIC-IDS2018 是对 CIC-IDS2017 的升级，原始数据从更大规模的网络（30 台服务器、420 台主机）中获取，并且增加了低速率的网络攻击[106]。而 CIC-DDoS2019 的攻击流量则由针对 TCP（MSSQL、SSDP）和 UDP（CharGen、NTP、TFTP）的反射攻击以及利用它们协议漏洞的 SYN 和 UDP 洪泛攻击所产生[107]。3 个数据集都提供.pcap 格式的原始数据流文件，以及经 FlowMeter 工具分析后形成的.csv 格式的特征文件。由于流量协议及分析工具版本不同，各数据集的特征数略有差别，但总体特征中都包括 6 个基本特征和 70 多个基于流和数据包的统计特征。近些年，随着深度学习技术的发展，基于深度学习异常检测或入侵检测模型[108]更喜欢选用它们提供的.pcap 格式的原始文件作为测试数据，以显示深度学习模型对原始数据的强大表征能力。

InSDN 是由爱尔兰都柏林大学研究人员于 2020 年发布的一个专门针对 SDN 环境下进行流量分析实验的新数据集，它包括 Botnet、DoS 攻击、DDoS 攻击、密码猜测、探测攻击等多种攻击生成的流量；正常流量则由当前常用的 HTTPS、HTTP、SSH、email、DNS 等各种协议产生[109]。数据集提

供原始数据流文件（.pacp）和提取特征后的.csv 形式文件。InSDN 是第一款真正的 SDN 环境下生成的流量数据集，可以有效反映 SDN 的真实特点。

另外，虽然几个数据集都给出了提取特征后的数据形式，但这些特征数据的提取（统计）标准并不相同，总体可以分为基于数据包、基于流和基于其他标准。其中，基于数据包的特征数据，通常有数据包的数量、长度、大小、方向等，如 CIC-IDS2017 数据集中提供正向数据包的平均长度、反向数据包长度的标准差、每秒传输的数据包数等特征数据。用于数据包特征统计的元数据与所在网络和传输协议有关，如 TCP、UDP、ICMP 和 IP 等。基于流的特征通常根据流的大小（包含数据包数、字节数）和流的方向等信息统计得出。CIC-IDS2017 提供的流包率、正向子流平均字节数、反向子流的平均数据包数等特征都是基于流的统计特征。流通常是按源 IP、源端口、目的 IP、目的端口、传输协议等五元组信息聚合的。此外，还有一些利用其他标准统计出的特征数据，它们并不是单纯的数据包型或流型，可能既包含基于网络连接的属性，如传输的字节数或 TCP 标志等；又包含基于主机状态的属性，如登录失败的数量，这类数据集的代表为 NSL-KDD。SDN 环境下异常流量检测研究中常用数据集的基本信息及其优势和不足如表 6 所示。

3.2　数据集的预处理操作

事实上，无论是从网络中捕获的原始流量数据，还是经过流量分析程序处理后的特征数据，都存在数据缺损、格式不正确、量纲差异大等问题。在输入深度学习异常流量检测模型前，需要进行一定的预处理操作，通常包括数据清洗、数据集划分、特征值编码、数据标准化、特征维度变换等操作。

1) 数据清洗

通常情况下，无论是公开数据集，还是自采数据，都可能存在数据缺损、数据重复、格式错误等问题，这种有问题的数据被称为“脏数据”，数据预处理的第一步应该是先将这些“脏数据”清洗掉。对于重复的数据以及格式错误的数据一般直接删除。对于缺损的数据，如果缺损率很高（大于 80%）且重要性较低，一般可以直接删除；对于缺损率不大的数据，可采取均值插补法、相似填充法等方法对缺损数据进行填补，以确保数据的完整性。

2)　数据集划分

数据集划分的主要原因有 2 个：一是自采数据需要构建训练集和测试集；二是原来已经划分好训练集和测试集的数据集，不能满足建模的需求，如有些原始数据集样本类别不平衡，为防止模型在训

表 6　　SDN 环境下异常流量检测研究中常用数据集的基本信息及其优势和不足

数据集名称	数据来源（年份）	数据类型	数据形式	特征数量	攻击类型	优势	不足
NSL-KDD	美国 MIT 林肯实验室（1998 年）	基于连接、主机	.csv	41	DoS、U2R、R2L、Probe	删除了缺损的数据；不同类别样本相对平衡	样本陈旧，且部分特征可由 OpenFlow 协议直接获取
UNSW-NB15	澳大利亚网络安全中心（2015 年）	基于数据包、内容、连接	.csv	46	DoS、Fuzzers、Analysis、Reconnaissance、Worms、Shellcode、Exploits、Generic、Backdoors	包含真实的正常网络活动流量，训练集与测试集分布相似	样本类别不平衡
ISCX-IDS2012	加拿大新不伦瑞克大学（2012 年）	基于流、数据包	.xml .pcap	—	DoS、DDoS、Bruteforce、Infiltration	样本“纯净”、噪声少；包含多种入侵场景	攻击类型分布不符合实际统计规律，无 HTTPS 的流量
CIC-IDS2017	加拿大网络安全研究所（2017 年）	基于流、数据包	.csv .pcap	80+	Brute force、Portscan、Botnet、DoS、DDoS、Web、Infiltration	提供原始流量和经 CICFlowMeter 提取特征的数据形式	样本标签缺失、流构建错误[109]
CIC-IDS2018	加拿大网络安全研究所（2018 年）	基于流、数据包	.csv .pcap	80+	Brute force、Portscan、SlowHTTPTest、DoS、LOIC、SQL Injection、Infiltration、、DDoS、Botnet、Web Attack	以真实网络为攻击目标，攻击主机数量多、攻击手段多样	流构建错误，使用了合成流量
CIC-DDoS2019	加拿大网络安全研究所（2019 年）	基于流、数据包	.csv .pcap	80+	MSSQL、NetBIOS、NTP、SNMP、SSDP、SYN、TFTP、UDP、UDP-Lag、WebDDoS、DNS、LDAP	包含多种基于 TCP/UDP 协议的新型攻击方法	样本类别不平衡
InSDN	爱尔兰都柏林大学（2020 年）	基于流、数据包	.csv .pcap	80+	DoS、Brute force、Botnet、Web Attack、Probe	全面的 SDN 环境下的攻击数据集	网络攻击种类偏少

练中出现某种偏好，常常会对原数据集进行重新调整，构造相对平衡的数据集。

3) 特征值编码

原始网络流量数据的特征可能是以文本或布尔值表示的，为了使其能够被计算机识别需要对这些非数值型的特征进行编码，常用的编码方法有独热编码、顺序编码。其中，独热编码法可在一定程度上扩充特征维度，并且产生大量 0 分量，使编码后的特征数据具有稀疏性。

4) 数值标准化

数值标准化主要为了消除特征数据量纲不一致对数据分析结果的不利影响，而对数据按照一定比例进行缩放，使它们的值落在一定的区域。常用的标准化方法有 Min-Max 标准化、MaxAbs 归一化、Z-Sore 标准化（规范化）、正则化、取对数等。

Min-Max 标准化能将特征数据映射到[0,1]区间，最大特征值为 1，最小特征值为 0，其他特征值分布其中，计算方法可表示为

$$x_i^{'} = \frac{x_i - x_{\min}}{x_{\max} - x_{\min}} \tag{1}$$

这种方法改变了原始数据的正负性和稀疏性。因此，人们又提出了 MaxAbs 归一化，将特征值绝对值最大的设置为 1，通过单独地缩放每个特征，使它们落在[−1, 1]区间，计算方法为

$$x_i^{'} = \frac{x_i}{\max\{x_i\}} \tag{2}$$

这 2 种缩放方法的共同缺陷就是当有新数据加入时，可能会引起最大值或最小值变化，需要重新定义整个数据集。

Z-Score 标准化操作可将特征数据变换为均值为 0、方差为 1 的统一标准形式，具体方法为

$$x_i^{'} = \frac{x_i - \mu}{\sigma} \tag{3}$$

其中，$\mu = \frac{1}{N}\sum_{i=1}^{N} x_i$，$\sigma = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i - \mu)^2}$。此方法适用于最大值和最小值未知，或有超范围的离群数据的情况。但是所需的整体均值和方差在实际中很难得到，大多数情况用样本的均值和方差替代。

数据的正则化是将样本的某个范数缩放到 1，该方法是针对单个样本的，将其缩放到单位范数。因此首先需要计算出样本向量 $\vec{x}_i = (x_i^{(1)}, x_i^{(2)}, \cdots, x_i^{(d)})^{\mathrm{T}}$ 的某个范数，计算式为

$$L_p(\vec{x}_i) = \left(\left|x_i^{(1)}\right|^p + \left|x_i^{(2)}\right|^p + \cdots + \left|x_i^{(d)}\right|^p \right)^{\frac{1}{p}}$$

正则化后的结果为

$$\vec{x}_i^{'} = \left(\frac{x_i^{(1)}}{L_p(\vec{x}_i)}, \frac{x_i^{(2)}}{L_p(\vec{x}_i)}, \cdots, \frac{x_i^{(d)}}{L_p(\vec{x}_i)} \right)^{\mathrm{T}} \tag{4}$$

此外，还有取对数的变换操作，如特殊数据量级相差较大，通常可以通过 log 函数变换的方法缩小差距，例如

$$x' = \log x \tag{5}$$

数据标准化是数据集预处理工作中一个重要环节，合适的标准化不仅可以使模型平缓地收敛到最优解，还能够加快迭代收敛的速度，这对于基于样本距离的算法尤其重要。

5) 特征维度变换

特征维度变换主要是为了提升运算效率或提高检测精度而进行的降维或升维操作。常用的降维操作包括主成分分析（PCA, principal component analysis）、奇异值分解（SVD, singular value decomposition）、聚类、线性组合等方法，如 Krishnan 等[110]在模拟 SDN 入侵检测时，为避免太多无用特征混淆检测结果，从 CIC-IDS2017 数据集的 80 多个流量特征中仅选择 48 个特征就完成建模和检测实验，并取得比较满意的检测效果。然而，有时为了提升检测的精度也会对特征数据进行升维，如 Chouhan 等[111]利用增强信道的方式，将数据样本维度扩充到原来的 8 倍后，再输入深度模型中进行检测，获得了比原数据样本更好的效果。对数据集的特征维度变换是可选择的，需要根据检测环境、检测对象、检测目标及方法，以及检测设备计算能力进行合理的特征数据变换策略，最终确保检测结果的准确性和时效性。

数据预处理工作虽然不是 SDN 异常流量检测的主要研究内容，但数据处理的好坏直接影响到异常检测的准确率和时间消耗，科学合理的数据处理可为检测模型提供丰富的特征信息而不会有冗余信息干扰检测结果，并且有利于缩减计算开支减小时间消耗。因此，数据预处理是 SDN 异常流量检测活动中的一个非常重要的环节。

4 下一步研究展望

目前，许多学者对 SDN 环境下异常流量检测进行了大量的研究和探索，也提出了一些有针对性

的解决方案。然而，由于网络攻击者不断改变攻击手段，传统的检测策略的适用性受到严格限制；另一方面，SDN 技术持续更新发展，在弥补已知缺陷的同时，也不断引入新的未知漏洞，现有的检测技术越来越难以满足日益发展的 SDN 异常流量检测需求，主要体现在以下几个方面。首先，现有的检测模型大都部署在 SDN 控制器所在服务器上，检测时会消耗大量的计算和网络资源，这对本身就存在资源匮乏隐患的 SDN 是一种极大的负担，检测时会影响控制器运行，甚至可能造成 SDN 控制器停止工作。其次，当前检测模型泛化能力和稳健性不强，对特定数据集中的异常流量能够很好地鉴别，但对由多种异常流量构成的复杂 SDN 检测能力欠佳。再次，检测方法过度依赖现有数据集，检测策略更新滞后，很难满足大规模 SDN 的在线异常流量检测需求；检测设计局限于单节点设备的异常流量检测，缺少对 SDN 全局防护的系统性应对机制和体系化处置能力。针对以上所提出的基于深度学习的 SDN 中异常流量检测模型存在的问题，给出下一阶段创新性研究工作展望。

1) 研究轻量型 SDN 异常流量检测技术

当前的检测方法大都将传统网络的检测机制迁移部署到 SDN 控制器上，通过不间断抓取和分析流量数据，从而实现对网络中异常流量的识别。这种做法显然没有充分考虑到 SDN 的特点。一方面，SDN 交换机每次收到新流量都要向控制器发送消息以获取转发规则；控制器还需要定期收集和监控网络流量，这些都会增加网络的通信开销，因此应考虑 SDN 环境中异常流量检测的抽样频率与通信效率之间的平衡。另一方面，异常流量检测模型大都部署在控制器所在的服务器上，模型的设计需要考虑数据预处理、检测特征提取、异常特征识别等检测过程的算法优化与计算资源的消耗控制。但在实际的检测研究中，人们为了获得更好的检测效果，通常会将检测流程规划得很“全”，将检测模型设计得比较“大”，而这种设计的代价是消耗大量的计算资源，进而造成 SDN 控制器服务质量下降或者所在服务器因过载而停止运行。因此，如何针对 SDN 流量数据特点，将传统检测步骤中的数据预处理、特征提取等运算开支进行缩减，减少服务器资源的额外消耗，构建出准确性、迅捷性及适用性相统一的轻量型 SDN 异常流量检测模型，是未来 SDN 异常流量检测的一个重要研究方向。

2) 探索具有自适应能力的 SDN 异常流量检测技术

当前大多数的 SDN 流量异常检测方法都是针对 DoS 攻击或 DDoS 攻击设计的，这类攻击会产生高速率的网络流量，能够引起网络明显波动。然而对于流量特征变化不明显的其他类型攻击，其流量模式与合法流相似，传统方法很难对其进行有效的检测。此外，网络技术快速发展，而攻击手段也在不断变化，这就需要一种具有自我进化能力、适应性更强的检测机制来满足复杂环境下 SDN 对异常流量检测的需求。因此未来的 SDN 异常流量检测方法应该比现有检测方法具有更强的组织灵活性、功能完整性和检测准确性等特点，以适应不断变化的 SDN 中复杂的网络攻击。这种检测方法应能够根据异常流量检测任务的不同，自主地制定流量数据采样方法和特征提取加工方式；而核心检测功能模块则应具有可扩展性和自学习性，以便适应未来不断进化的网络攻击手段。此外，检测系统应包含具有自主更新能力的知识库，以便在发现新的网络攻击时，可及时将新的攻击流量特征添加到共享知识库，进而规划出具有针对性的层次化检测任务；还应支持人机交互功能，可执行网络管理人员定制的检测任务。因此，探索具有自适应能力可应对多样性攻击的异常流量检测技术成为未来 SDN 异常流量检测的一个重要研究方向。

3) 构建面向大数据的 SDN 异常流量检测及评价体系

随着的网络规模不断扩大，流量数据呈几何级增长，对网络的安全性要求也不断提升，这就需要能够支持大数据环境下实现 SDN 异常流量检测的可靠方法。而现行的检测方法大都要经过控制器实现安全控制，控制器要处理很多应用数据；另外，存储空间有限的交换机上部署着庞大的规则，面向连接的安全检测会影响转发平面的性能。因此，需要对现有 SDN 的通信协议和架构进行改进，使其能够对海量数据进行快速处置。另一方面，动态复杂的大规模流量会对网络设备带来巨大的压力，在局部关键节点可能产生瓶颈效应。因此，在保证各种异常流量检测算法并行运算的基础上，应对异常检测的运算开支进行全网均衡，并且建立智能化的采样机制，避免检测时因频繁采样而导致服务器过载或网络拥塞。另外，从前面的研究分析中可以发现，许多取得较高性能指

标的研究使用有限的离线数据来分析评估其性能，当面对大规模真实 SDN 环境时，其检测方法的性能指标可能会大打折扣；并且当前的检测评估指标大多局限于准确率、召回率等指标，很少讨论网络的吞吐量、丢包率、检测时延等指标。然而在大数据背景下，这些性能指标也是衡量检测方法优劣的关键。因此，构建面向大数据环境下的异常流量检测方法及评价体系也是未来的 SDN 异常流量检测的一个研究方向。

4) 建立分布式的 SDN 异常流量检测与缓解机制

当前许多 SDN 的异常流量检测方法都是基于单控制器或控制器集中部署的 SDN，这种结构仅适用于小规模网络。事实上，随着互联网技术的不断发展，网络模型日趋庞大，为提升网络的稳健性和容灾能力，未来 SDN 逐渐呈现出跨区域、分布式部署的发展趋势。因此未来异常流量检测方法需要具备应对 SDN 中有组织的跨区域攻击的能力，可以考虑“中心+代理”的运行机制，由代理完成对本控制器所属网络域中异常流量的检测与溯源任务，并在域内先进行异常流量缓解操作；同时将执行信息，如检测到的攻击源信息、负载冗余量、负载分流请求等信息发送到中心控制器。中心控制器将代理检测到的攻击源信息同步到各从属控制器，由它们制定转发策略更新各自交换机流表信息。同时对无法通过调整域内资源、缓解网络攻击影响的，由主机控制器根据各控制器的负载冗余量、传输带宽、响应时间的指标综合衡量，将负载按比例调配到其他轻负载的控制器上。另外，还应考虑与云计算技术结合，设计部署在云端的并行式异常流量检测算法，通过云服务器和各控制器间的有效通信实现分布式 SDN 中的异常流量检测与缓解。所以，建立分布式异常流量检测及缓解机制，同样会成为未来 SDN 异常流量检测一个重要的研究方向。

5 结束语

随着互联网和云计算技术的不断发展，SDN 的开发与应用日渐广泛，在强化网络扩展的灵活性和管理的集中性的同时，也将面临比传统网络更多的威胁。SDN 异常流量检测是识别异常流量、发现网络攻击、维护网络安全的支撑手段。本文在深入分析 SDN 面临的威胁以及引起流量变化的基础上，对现有基于深度学习的 SDN 环境下异常流量检测技术进行系统分析和探讨。首先，分析了基于监督学习、无监督学习和半监督学习的异常流量检测机理；接着，总结了当前 SDN 中异常流量检测、异常流量溯源及异常流量缓解的实现方法、优势与不足；然后，梳理了现有研究中常用的数据集以及数据预处理一般流程；最后，通过分析当前 SDN 中异常流量检测方法存在的问题，提出未来基于深度学习的 SDN 中异常流量检测的研究方向，并对全文进行总结。

参考文献：

[1] ALI T E, MORAD A H, ABDALA M A. Load balance in data center SDN networks[J]. International Journal of Electrical and Computer Engineering (IJECE), 2018, 8(5): 3086-3092.

[2] ALHIJAWI B, ALMAJALI S, ELGALA H, et al. A survey on DoS/DDoS mitigation techniques in SDNs: classification, comparison, solutions, testing tools and datasets[J]. Computers and Electrical Engineering, 2022, 99: 107706.

[3] BIANCHI G, BONOLA M, CAPONE A, et al. Openstate: programming platform-independent stateful OpenFlow applications inside the switch[J]. ACM SIGCOMM Computer Communication Review, 2014, 44(2): 44-51.

[4] RASOOL R U, WANG H, ASHRAF U, et al. A survey of link flooding attacks in software defined network ecosystems[J]. Journal of Network and Computer Applications, 2020, 172: 102803.

[5] LI J S, TU T F, LI Y S, et al. DoSGuard: mitigating denial-of-service attacks in software-defined networks[J]. Sensors, 2022, 22(3): 1061.

[6] VERGARA J, GARZÓN C, BOTERO J F. A hybrid strategy for DoS attacks detection and mitigation on SDN enabled real scenarios[C]//Proceedings of International Congress on Information and Communication Technology. Berlin: Springer, 2023: 705-714.

[7] FOULADI R F, ERMIŞ O, ANARIM E. A DDoS attack detection and countermeasure scheme based on DWT and auto-encoder neural network for SDN[J]. Computer Networks, 2022, 214: 109140.

[8] SINGH J, BEHAL S. Detection and mitigation of DDoS attacks in SDN: a comprehensive review, research challenges and future directions[J]. Computer Science Review, 2020, 37: 100279.

[9] ANYANWU G O, NWAKANMA C I, LEE J M, et al. RBF-SVM kernel-based model for detecting DDoS attacks in SDN integrated vehicular network[J]. Ad Hoc Networks, 2023, 140: 103026.

[10] BHAYO J, SHAH S A, HAMEED S, et al. Towards a machine learning-based framework for DDOS attack detection in software-defined IoT (SD-IoT) networks[J]. Engineering Applications of Artificial Intelligence, 2023, 123: 106432.

[11] 段雪源, 付钰, 王坤, 等. 基于简单统计特征的 LDoS 攻击检测方法[J]. 通信学报, 2022, 43(11): 53-64.
DUAN X Y, FU Y, WANG K, et al. LDoS attack detection method based on simple statistical features[J]. Journal on Communications, 2022, 43(11): 53-64.

[12] SUN W W, GUAN S P, WANG P, et al. A hybrid deep learning model

based low-rate DoS attack detection method for software defined network[J]. Transactions on Emerging Telecommunications Technologies, 2022: doi.org/10.1002/ett.4443.

[13] ALASHHAB A A, ZAHID M S M, MUNEER A, et al. Low-rate DDoS attack detection using deep learning for SDN-enabled IoT networks[J]. International Journal of Advanced Computer Science and Applications, 2022, 13(11): 371-377.

[14] JAFARIAN T, MASDARI M, GHAFFARI A, et al. A survey and classification of the security anomaly detection mechanisms in software defined networks[J]. Cluster Computing, 2021, 24: 1235-1253.

[15] BAHASHWAN A A, ANBAR M, MANICKAM S, et al. A systematic literature review on machine learning and deep learning approaches for detecting DDoS attacks in software-defined networking[J]. Sensors, 2023, 23(9): 4441.

[16] 徐玉华, 孙知信. 软件定义网络中的异常流量检测研究进展[J]. 软件学报, 2020, 31(1): 183-207.
XU Y H, SUN Z X. Research development of abnormal traffic detection in software defined networking[J]. Journal of Software, 2020, 31(1): 183-207.

[17] LATIF Z, SHARIF K, LI F, et al. A comprehensive survey of interface protocols for software defined networks[J]. Journal of Network and Computer Applications, 2020, 156: 102563.

[18] SADKHAN S B, ABBAS M S, MAHDI S S, et al. Software-defined network security - status, challenges, and future trends[C]//Proceedings of the 2022 Muthanna International Conference on Engineering Science and Technology (MICEST). Piscataway: IEEE Press, 2022: 10-15.

[19] ALADAILEH M A, ANBAR M, HASBULLAH I H, et al. Detection techniques of distributed denial of service attacks on software-defined networking controller —— a review[J]. IEEE Access, 2020, 8: 143985-143995.

[20] SINGH M, BHANDARI A. New-flow based DDoS attacks in SDN: taxonomy, rationales, and research challenges[J]. Computer Communications, 2020, 154: 509-527.

[21] 罗智勇, 张玉, 王青, 等. 基于贝叶斯攻击图的 SDN 入侵意图识别算法的研究[J]. 通信学报, 2023, 44(4): 216-225.
LUO Z Y, ZHANG Y, WANG Q, et al. Study of SDN intrusion intent identification algorithm based on Bayesian attack graph[J]. Journal on Communications, 2023, 44(4): 216-225.

[22] 左志斌. 基于密码标识的软件定义网络数据面安全关键技术研究[D]. 郑州: 信息工程大学, 2021.
ZUO Z B. Research on key issues of software-defined networking data plane security based on cipher identifier[D]. Zhengzhou: Information Engineering University, 2021.

[23] FALAYI A, WANG Q L, LIAO W X, et al. Survey of distributed and decentralized IoT securities: approaches using deep learning and blockchain technology[J]. Future Internet, 2023, 15(5): 178.

[24] HUANG J H, CHEN J X, LU X H, et al. Research on detection techniques for scanning attacks in software-defined network environments[C]//Proceedings of the 2023 4th International Conference on Computer Engineering and Application (ICCEA). Piscataway: IEEE Press, 2023: 115-118.

[25] RANGISETTI A K, DWIVEDI R, SINGH P. Denial of ARP spoofing in SDN and NFV enabled cloud-fog-edge platforms[J]. Cluster Computing, 2021, 24(4): 3147-3172.

[26] ZHANG Q S, CHO J H, MOORE T J, et al. EVADE: efficient moving target defense for autonomous network topology shuffling using deep reinforcement learning[C]//Proceedings of the International Conference on Applied Cryptography and Network Security. Berlin: Springer, 2023: 555-582.

[27] ABDOU A, OORSCHOT P C V, WAN T. Comparative analysis of control plane security of SDN and conventional networks[J]. IEEE Communications Surveys & Tutorials, 2018, 20(4): 3542-3559.

[28] VALDOVINOS I A, PÉREZ-DÍAZ J A, CHOO K K R, et al. Emerging DDoS attack detection and mitigation strategies in software-defined networks: taxonomy, challenges and future directions[J]. Journal of Network and Computer Applications, 2021, 187: 103093.

[29] BALAREZO J F, WANG S, CHAVEZ K G, et al. A survey on DoS/DDoS attacks mathematical modelling for traditional, SDN and virtual networks[J]. Engineering Science and Technology, an International Journal, 2022, 31: 101065.

[30] ELEJLA O E, ANBAR M, HAMOUDA S, et al. Deep-learning-based approach to detect ICMPv6 flooding DDoS attacks on IPv6 networks[J]. Applied Sciences, 2022, 12(12): 6150.

[31] ALADAILEH M A, ANBAR M, HASBULLAH I H, et al. Dynamic threshold-based approach to detect low-rate DDoS attacks on software-defined networking controller[J]. Computers, Materials & Continua, 2022, 73(1): 1403-1416.

[32] XIE R J, CAO J H, LI Q, et al. Disrupting the SDN control channel via shared links: attacks and countermeasures[J]. IEEE/ACM Transactions on Networking, 2022, 30(5): 2158-2172.

[33] YUNGAICELA-NAULA N M, VARGAS-ROSALES C, PÉREZ-DÍAZ J A, et al. Towards security automation in software defined networks[J]. Computer Communications, 2022, 183(C): 64-82.

[34] SIDDIQUI S, HAMEED S, SHAH S A, et al. Toward software-defined networking-based IoT frameworks: a systematic literature review, taxonomy, open challenges and prospects[J]. IEEE Access, 2022, 10: 70850-70901.

[35] NAGARATHNA R, SHALINIE S M. SLAMHHA: a supervised learning approach to mitigate host location hijacking attack on SDN controllers[C]//Proceedings of the 2017 Fourth International Conference on Signal Processing, Communication and Networking (ICSCN). Piscataway: IEEE Press, 2017: 1-7.

[36] LEE S, KIM J, WOO S, et al. A comprehensive security assessment framework for software-defined networks[J]. Computers & Security, 2020, 91: 101720.

[37] ALHAJ A N, DUTTA N. Analysis of security attacks in SDN network: a comprehensive survey[C]//Proceedings of the Contemporary Issues in Communication, Cloud and Big Data Analytics. Berlin: Springer, 2022: 27-37.

[38] MALEH Y, QASMAOUI Y, GHOLAMI K E, et al. A comprehensive survey on SDN security: threats, mitigations, and future directions[J]. Journal of Reliable Intelligent Environments, 2023, 9(2): 201-239.

[39] TANG D, WANG X Y, YAN Y D, et al. ADMS: an online attack detection and mitigation system for LDoS attacks via SDN[J]. Computer Communications, 2022, 181: 454-471.

[40] 李传煌, 吴艳, 钱正哲, 等. SDN 下基于深度学习混合模型的 DDoS 攻击检测与防御[J]. 通信学报, 2018, 39(7): 176-187.
LI C H, WU Y, QIAN Z Z, et al. DDoS attack detection and defense based on hybrid deep learning model in SDN[J]. Journal on Communications, 2018, 39(7): 176-187.

[41] MOUSAVI S M, ST-HILAIRE M. Early detection of DDoS attacks against SDN controllers[C]//Proceedings of the 2015 International Conference on Computing, Networking and Communications (ICNC). Piscataway: IEEE Press, 2015: 77-81.

[42] UJJAN R M A, PERVEZ Z, DAHAL K, et al. Entropy based features distribution for anti-DDoS model in SDN[J]. Sustainability, 2021, 13(3): 1522.

[43] KALKAN K, ALTAY L, GÜR G, et al. JESS: joint entropy-based DDoS defense scheme in SDN[J]. IEEE Journal on Selected Areas in Communications, 2018, 36(10): 2358-2372.

[44] OO M M, KAMOLPHIWONG S, KAMOLPHIWONG T, et al. Analysis of features dataset for DDoS detection by using ASVM method on software defined networking[J]. International Journal of Networked and Distributed Computing, 2020, 8(2): 86-93.

[45] KOUSAR H, MULLA M M, SHETTAR P, et al. Detection of DDoS attacks in software defined network using decision tree[C]//Proceedings of the 2021 10th IEEE International Conference on Communication Systems and Network Technologies (CSNT). Piscataway: IEEE Press, 2021: 783-788.

[46] XU Y, SUN H, XIANG F, et al. Efficient DDoS detection based on K-FKNN in software defined networks[J]. IEEE access, 2019, 7: 160536-160545.

[47] NANDA S, ZAFARI F, DECUSATIS C, et al. Predicting network attack patterns in SDN using machine learning approach[C]//Proceedings of the 2016 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN). Piscataway: IEEE Press, 2016: 167-172.

[48] BAHASHWAN A A, ANBAR M, MANICKAM S, et al. HLD-DDoSDN: high and low-rates dataset-based DDoS attacks against SDN[J]. Plos One, 2024, 19(2): e0297548.

[49] SWAMI R, DAVE M, RANGA V. Voting-based intrusion detection framework for securing software-defined networks[J]. Concurrency and Computation: Practice and Experience, 2020: doi.org/10.1002/cpe.5927.

[50] DEEPA V, SUDAR K M, DEEPALAKSHMI P. Design of ensemble learning methods for DDoS detection in SDN environment[C]//Proceedings of the 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN). Piscataway: IEEE Press, 2019: 1-6.

[51] YILMAZ A, KÜÇÜKER A, BAYRAK G, et al. An improved automated PQD classification method for distributed generators with hybrid SVM-based approach using un-decimated wavelet transform[J]. International Journal of Electrical Power & Energy Systems, 2022, 136: 107763.

[52] ALI J, SHAN G Y, GUL N, et al. An intelligent blockchain-based secure link failure recovery framework for software-defined internet-of-things[J]. Journal of Grid Computing, 2023, 21(4): 57.

[53] MADATHI M, HARINI R, MONIKAA R, et al. Detection of DDoS attack in SDN environment using KNN algorithm[J]. IJRAR-International Journal of Research and Analytical Reviews (IJRAR), 2022, 9(2): 252-257.

[54] CUI J, ZHANG J, HE J T, et al. DDoS detection and defense mechanism for SDN controllers with K-Means[C]//Proceedings of the 2020 IEEE/ACM 13th International Conference on Utility and Cloud Computing (UCC). Piscataway: IEEE Press, 2020: 394-401.

[55] WEI Y Y, JANG-JACCARD J, SABRINA F, et al. AE-MLP: a hybrid deep learning approach for DDoS detection and classification[J]. IEEE Access, 2021, 9: 146810-146821.

[56] MAHESHWARI A, MEHRAJ B, KHAN M S, et al. An optimized weighted voting based ensemble model for DDoS attack detection and mitigation in SDN environment[J]. Microprocessors and Microsystems, 2022, 89: 104412.

[57] KUMAR R, AGRAWAL N. Software defined networks (SDNs) for environmental surveillance: a survey[J]. Multimedia Tools and Applications, 2024, 83(4): 11323-11365.

[58] HAIDER S, AKHUNZADA A, MUSTAFA I, et al. A deep CNN ensemble framework for efficient DDoS attack detection in software defined networks[J]. IEEE Access, 2020, 8: 53972-53983.

[59] TAYFOUR O E, MUBARAKALI A, TAYFOUR A E, et al. Adapting deep learning-LSTM method using optimized dataset in SDN controller for secure IoT[J]. Soft Computing, 2023, 5: 1-9.

[60] ZHANG L, WANG J S. A hybrid method of entropy and SSAE-SVM based DDoS detection and mitigation mechanism in SDN[J]. Computers & Security, 2022, 115: 102604.

[61] SHEN Y J. An intrusion detection algorithm for DDoS attacks based on DBN and three-way decisions[J]. Journal of Physics: Conference Series, 2022, 2356(1): 012044.

[62] NOVAES M P, CARVALHO L F, LLORET J, et al. Adversarial deep learning approach detection and defense against DDoS attacks in SDN environments[J]. Future Generation Computer Systems, 2021, 125: 156-167.

[63] ABDALLAH M, LE K N A, JAHROMI H, et al. A hybrid CNN-LSTM based approach for anomaly detection systems in SDNs[C]//Proceedings of the Proceedings of the 16th International Conference on Availability, Reliability and Security. New York: ACM Press, 2021: 1-7.

[64] PATTERSON J, GIBSON A. Deep learning: a practitioner's approach[M]. California: O'Reilly Media, Inc, 2017.

[65] PANG G S, SHEN C H, CAO L B, et al. Deep learning for anomaly detection: a review[J]. ACM Computing Surveys, 2021, 54(2): 38.

[66] WANG C, ZHU T. DDoS attack detection methods based on deep learning in healthcare[J]. Journal of Mechanics in Medicine and Biology, 2023: doi.org/10.1142/S0219519423400080.

[67] SHONE N, NGOC T N, PHAI V D, et al. A deep learning approach to network intrusion detection[J]. IEEE Transactions on Emerging Topics in Computational Intelligence, 2018, 2(1): 41-50.

[68] WANG P, WANG Z X, YE F, et al. ByteSGAN: a semi-supervised generative adversarial network for encrypted traffic classification in SDN Edge Gateway[J]. Computer Networks, 2021, 200: 108535.

[69] SONG H C, JIANG Z Q, MEN A D, et al. A hybrid semi-supervised anomaly detection model for high-dimensional data[J]. Computational

Intelligence and Neuroscience, 2017, 2017: 8501683.

[70] AHMAD Z, SHAHID K A, WAI S C, et al. Network intrusion detection system: a systematic study of machine learning and deep learning approaches[J]. Transactions on Emerging Telecommunications Technologies, 2021: doi.org/10.1002/ett.4150.

[71] ASSIS M V O, CARVALHO L F, LLORET J, et al. A GRU deep learning system against attacks in software defined networks[J]. Journal of Network and Computer Applications, 2021, 177: 102942.

[72] JANABI A H, KANAKIS T, JOHNSON M. Convolutional neural network based algorithm for early warning proactive system security in software defined networks[J]. IEEE Access, 2022, 10: 14301-14310.

[73] 白坚镜, 顾瑞春, 刘清河. SDN 环境中基于 Bi-LSTM 的 DDoS 攻击检测方案[J]. 计算机工程与科学, 2023, 45(2): 277-285.
BAI J J, GU R C, LIU Q H. A DDoS attack detection scheme based on Bi-LSTM in SDN[J]. Computer Engineering & Science, 2023, 45(2): 277-285.

[74] ALANAZI F, JAMBI K, EASSA F, et al. Ensemble deep learning models for mitigating DDoS attack in software-defined network[J]. Intelligent Automation & Soft Computing, 2022, 33(2): 923-938.

[75] ELSAYED M S, LE-KHAC N A, DEV S, et al. DDoSNet: a deep-learning model for detecting network attacks[C]//Proceedings of the 2020 IEEE 21st International Symposium on a World of Wireless, Mobile and Multimedia Networks. Piscataway: IEEE Press, 2020: 391-396.

[76] TANG T A, MHAMDI L, MCLERNON D, et al. DeepIDS: deep learning approach for intrusion detection in software defined networking[J]. Electronics, 2020, 9(9): 1533.

[77] JAVEED D, GAO T H, KHAN M T, et al. A hybrid deep learning-driven SDN enabled mechanism for secure communication in Internet of things (IoT)[J]. Sensors, 2021, 21(14): 4884.

[78] HNAMTE V, HUSSAIN J. An efficient DDoS attack detection mechanism in SDN environment[J]. International Journal of Information Technology, 2023, 15(5): 2623-2636.

[79] KAO M T, SUNG D Y, KAO S J, et al. A novel two-stage deep learning structure for network flow anomaly detection[J]. Electronics, 2022, 11(10): 1531.

[80] YASER A L, MOUSA H M, HUSSEIN M. Improved DDoS detection utilizing deep neural networks and feedforward neural networks as autoencoder[J]. Future Internet, 2022, 14(8): 240.

[81] 豆健. 基于 SDN 的 DDRS 攻击检测与溯源技术的研究与应用[D]. 西安: 西安电子科技大学, 2021.
DOU J. Research and application of DDRS attack detection and traceability technology based on SDN[D]. Xi'an: Xidian University, 2021.

[82] WANG J, WANG L P. SDN-defend: a lightweight online attack detection and mitigation system for DDoS attacks in SDN[J]. Sensors, 2022, 22(21): 8287.

[83] 郭笛. 面向 SDN 的 DDoS 攻击检测与防御技术研究[D]. 长沙: 国防科技大学, 2020.
GUO D. Research on DDoS attack detection and defense technology for SDN[D]. Changsha: National University of Defense Technology, 2020.

[84] NADEEM M W, GOH H G, AUN Y, et al. Detecting and mitigating Botnet attacks in software-defined networks using deep learning techniques[J]. IEEE Access, 2023, 11: 49153-49171.

[85] 魏松杰, 孙鑫, 赵茹东, 等. SDN 中 IP 欺骗数据分组网络溯源方法研究[J]. 通信学报, 2018, 39(11): 181-189.
WEI S J, SUN X, ZHAO R D, et al. Tracing IP-spoofed packets in software defined network[J]. Journal on Communications, 2018, 39(11): 181-189.

[86] CHEN W, XIAO S C, LIU L J, et al. A DDoS attacks traceback scheme for SDN-based smart city[J]. Computers & Electrical Engineering, 2020, 81: 106503.

[87] NUR A Y, TOZAL M E. Single packet AS traceback against DoS attacks[C]//Proceedings of the 2021 IEEE International Systems Conference (SysCon). Piscataway: IEEE Press, 2021: 1-8.

[88] HADEM P, SAIKIA D K, MOULIK S. An SDN-based Intrusion detection system using svm with selective logging for ip traceback[J]. Computer Networks, 2021, 191: 108015.

[89] JOSEPH K, EYOBU O S, KASYOKA P, et al. A link fabrication attack mitigation approach (LiFAMA) for software defined networks[J]. Electronics, 2022, 11(10): 1581.

[90] 陈怡欣. SDN 环境下的流量异常检测技术研究[D]. 合肥: 中国科学技术大学, 2021.
CHEN Y X. Abnormal traffic detection technology in software-defined network[D]. Hefei: University of Science and Technology of China, 2021.

[91] CAO Y Y, JIANG H, DENG Y C, et al. Detecting and mitigating DDoS attacks in SDN using spatial-temporal graph convolutional network[J]. IEEE Transactions on Dependable and Secure Computing, 2022, 19(6): 3855-3872.

[92] YUNGAICELA-NAULA N M, VARGAS-ROSALES C, PÉREZ-DÍAZ J A, et al. A flexible SDN-based framework for slow-rate DDoS attack mitigation by using deep reinforcement learning[J]. Journal of Network and Computer Applications, 2022, 205: 103444.

[93] SUDAR K M, DEEPALAKSHMI P. Flow-based detection and mitigation of low-rate DDoS attack in SDN environment using machine learning techniques[C]//Proceedings of the IoT and Analytics for Sensor Networks. Berlin: Springer, 2022: 193-205.

[94] KAMEL A E, ELTAIEF H, YOUSSEF H. On-the-fly (D)DoS attack mitigation in SDN using deep neural network-based rate limiting[J]. Computer Communications, 2022, 182(C): 153-169.

[95] FILALI A, KOBBANE A, ELMACHKOUR M, et al. SDN controller assignment and load balancing with minimum quota of processing capacity[C]//Proceedings of the 2018 IEEE International Conference on Communications (ICC). Piscataway: IEEE Press, 2018: 1-6.

[96] KAMEL E A, YOUSSEF H. Improving switch-to-controller assignment with load balancing in multi-controller software defined WAN (SD-WAN)[J]. Journal of Network and Systems Management, 2020, 28(3): 553-575.

[97] YUAN B, ZHANG F, WAN J, et al. Resource investment for DDoS attack resistant SDN: a practical assessment[J]. Science China Information Sciences, 2023, 66(7): 172103.

[98] GILLANI F, AL-SHAER E, DUAN Q. In-design resilient SDN control plane and elastic forwarding against aggressive DDoS attacks[C]//Proceedings of the 5th ACM Workshop on Moving Target Defense. New York: ACM Press, 2018: 80-89.

[99] PROTIĆ D. Review of KDD cup'99, NSL-KDD and Kyoto 2006+ datasets[J]. Vojnotehnicki Glasnik, 2018, 66(3): 580-596.

[100] SIDDIQUE K, AKHTAR Z, KHAN F A, et al. KDD cup 99 data sets:a perspective on the role of data sets in network intrusion detection research[J]. Computer, 2019, 52(2): 41-51.

[101] ZONG B, SONG Q, MIN M R, et al. Deep autoencoding gaussian mixture model for unsupervised anomaly detection[C]//Proceedings of the 2018 International Conference on Learning Representations. Vancouver: ICLR, 2018: 1-19.

[102] SARHAN M, LAYEGHY S, MOUSTAFA N, et al. Netflow datasets for machine learning-based network intrusion detection systems[C]//Proceedings of the 2020 Big Data Technologies and Applications: 10th EAI International Conference, BDTA 2020, and 13th EAI International Conference on Wireless Internet. Berlin: Springer, 2020: 117-135.

[103] SHIRAVI A, SHIRAVI H, TAVALLAEE M, et al. Toward developing a systematic approach to generate benchmark datasets for intrusion detection[J]. Computers and Security, 2012, 31(3): 357-374.

[104] KHAN M A, KARIM M R, KIM Y. A scalable and hybrid intrusion detection system based on the convolutional-LSTM network[J]. Symmetry, 2019, 11(4): 583.

[105] SHARAFALDIN I, LASHKARI A H, GHORBANI A A. Toward generating a new intrusion detection dataset and intrusion traffic characterization[C]//Proceedings of the 2018 International Conference on Information Science and Systems(ICISS). Piscataway: IEEE Press, 2018: 108-116.

[106] RING M, WUNDERLICH S, SCHEURING D, et al. A survey of network-based intrusion detection data sets[J]. Computers and Security, 2019, 86(C): 147-167.

[107] SHARAFALDIN I, LASHKARI A H, HAKAK S, et al. Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy[C]//Proceedings of the 2019 International Carnahan Conference on Security Technology (ICCST). Piscataway: IEEE Press, 2019: 1-8.

[108] 许聪源. 基于深度学习的网络入侵检测方法研究[D]. 杭州: 浙江大学, 2019.
XU C Y. Research of network intrusion detection method based on deep learning[D]. Hangzhou: Zhejiang University, 2019.

[109] ELSAYED M S, LE-KHAC N A, JURCUT A D. InSDN: a novel SDN intrusion dataset[J]. IEEE Access, 2020, 8: 165263-165284.

[110] KRISHNAN P, DUTTAGUPTA S, ACHUTHAN K. VARMAN: multi-plane security framework for software defined networks[J]. Computer Communications, 2019, 148(C): 215-239.

[111] CHOUHAN N, KHAN A, KHAN H U R. Network anomaly detection using channel boosted and residual learning based deep convolutional neural network[J]. Applied Soft Computing, 2019, 83: 105612.

[作者简介]

付钰（1982− ），女，湖北武汉人，博士，海军工程大学教授、博士生导师，主要研究方向为信息安全、人工智能。

王坤（1981− ），女，河南信阳人，海军工程大学博士生，主要研究方向为网络安全、人工智能、信息对抗。

段雪源（1981− ），男，河南开封人，博士，信阳师范大学讲师，主要研究方向为人工智能、信息处理、网络安全。

刘涛涛（1996− ），男，江西吉水人，海军工程大学博士生，主要研究方向为网络安全、网络信息对抗。