研究论文

SDN 中入侵检测方法研究进展

刘瑞[1],王海凤[1*],郑承蔚[1],武文红[1],牛恒茂[2]

摘要 入侵检测作为软件定义网络(software defined networks, SDN)架构的关键安全防护手段,能有效保障 SDN 安全稳定运行。通过汇总基于机器学习、基于深度学习、基于强化学习和基于信息熵的入侵检测方法,总结并分析 SDN 环境中仍存在的问题总结并分析了 SDN 环境中仍存在的问题:单控制器易受网络威胁、缺乏可扩展性、缺乏缓解和预防的方法、缺乏低速率 DDoS 的攻击检测、缺乏用于训练的 SDN 特定数据集、应用层的防御方法较少,并指出了未来的研究方向。

关键词 软件定义网络;入侵检测;机器学习;深度学习;强化学习;信息熵

随着网络的爆炸式发展,网络安全成为当今最引人关注的问题之一,因为它直接影响到国家、企业、个人的利益。由于信息技术的迅速发展,现代网络中的软件定义网络(software defined networks, SDN)系统[1]需要每时每刻处理大量数据。根据文献[2]的预测,全球 SDN 市场的规模预计将从 2020 年的 137 亿美元增长到 2025 年的 327 亿美元。这一增长主要得益于 SDN 动态灵活的架构[3]使网络变得更便捷高效,SDN 架构通过分离数据平面和控制平面展现出比传统网络架构更强大的灵活性和可控性。在传统的基于硬件的网络中,由于需要手动配置大量交换机以进行更新或更改,这不仅容易出错而且效率也低下,使得部署新的协议和服务成为一项挑战。相比之下,SDN 不仅可以通过控制器自动配置所需的服务和协议,还引入了一个集中的身份验证过程,从而极大地简化了网络管理。此外,SDN 还打破了传统网络静态配置的局限,为网络管理员提供了更灵活的编程机制。

随着网络攻击手段和技术的不断进步,入侵检测研究面临着前所未有的挑战,尤其是针对 SDN 架构的特定攻击手段不断涌现,使入侵检测技术在 SDN 中变得尤为关键和重要[4−5]。因此,如何保障 SDN 安全已成为一个亟待解决的重要问题[6]。

1 软件定义网络

SDN 起源于 2006 年斯坦福大学的 Clean Slate 研究课题,2009 年,Mckeown 正式提出 SDN 概念。SDN 的核心思想是将网络的控制平面与数据转发平面分离。传统网络中,路由器和交换机通常同时包含控制逻辑和数据转发功能,而在 SDN 中,这两者被分离开来。控制逻辑集中在一个或多个控制器中,而数据转发则由可编程的交换设备进行,因此,SDN 得以实现更加灵活和高效的网络管理[7]。此外,SDN 的开放性应用程序接口(application program interface, API)使得第三方应用程序能够与网络设备进行交互,提高了网络的可扩展性和适应性。因此,开放网络基

1. 内蒙古工业大学信息工程学院,呼和浩特 010080
2. 内蒙古建筑职业技术学院建筑工程与测绘学院,呼和浩特 010020

收稿日期:2024−05−27;修回日期:2024−09−26
基金项目:内蒙古自治区科技计划项目(2021GG0250);内蒙古自治区自然科学基金(2021MS06029);内蒙古自治区科技计划项目(2020GG0104)
作者简介:刘瑞,硕士研究生,研究方向为计算机网络技术,电子信箱:535426192@qq.com;王海凤(通信作者),副教授,研究方向为计算机网络技术,电子信箱:wanghf@imut.edu.cn
引用格式:刘瑞, 王海凤, 郑承蔚, 等. SDN 中入侵检测方法研究进展[J]. 科技导报, 2025, 43(10): 76−93; doi:10.3981/j.issn.1000-7857.2024.05.00570

金会(open networking foundation, ONF)组织为SDN划分数据层、控制层和应用层这3层架构以及定义了南向接口和北向接口2个关键的接口[8]。SDN体系结构如图1所示。

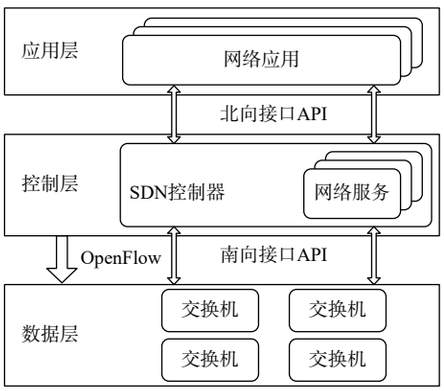

图1 SDN体系架构

1)应用层。SDN应用层遭受的攻击主要源于和控制器通信的北向接口缺乏保护。攻击者可能利用北向接口的漏洞或缺陷,通过发送恶意请求、注入恶意代码或伪造数据等方式,试图获取对应用层的非法访问权限。攻击者在获取网络拓扑、设备配置等敏感信息后,能够篡改网络配置,最终导致网络数据泄露。

2)控制层。作为SDN架构的核心,通过控制器实现对数据平面的精准控制,确保SDN功能的正常运行。控制器在SDN中扮演着网络流量核心管理者的角色,负责执行路由决策、数据包转发与丢弃等关键任务。控制层通过集中管理网络中的交换机和SDN应用程序,提供全面的网络状态信息来支持不同网络服务层的需求。

3)数据层。数据层作为SDN架构的最底层,通过南向接口API接收来自控制层的指令,内置的设备通常被称为网络交换机。数据层通过控制器指示交换机如何转发数据包,当数据包匹配到流表项并执行相应的操作后,交换机就会根据该操作将数据包转发到指定的端口或端口组。

2 SDN的攻击方式

尽管SDN以其可编程性和集中控制的优势,成为推动网络创新的关键力量。然而,SDN也伴随着层出不穷的网络安全挑战,其集中化的控制平面和开放的API接口为网络攻击者提供了新的攻击途径。因此,对SDN架构下应用层、控制层和数据层网络攻击进行深入分析,揭示潜在的安全威胁,对于保障网络的安全稳定运行至关重要。表1对主要的网络攻击方式进行归纳和阐述。

表1 网络攻击方式

攻击方式	攻击位置	攻击机制
代码注入	应用层	攻击者通过向应用程序中注入恶意代码,从而实现对应用程序功能的操控。这些恶意代码可以执行窃取用户数据的非法操作
DoS、DDoS	应用层、控制层、数据层	攻击者通过大量请求来拥塞API,使SDN无法处理正常请求,导致SDN控制器无法正常工作,影响整个网络的稳定性
暴力破解	数据层	也称为暴力枚举或暴力穷举。攻击者使用自动化工具或脚本,尝试所有可能的字符组合作为密码,直到找到正确的密码为止
拓扑攻击	控制层	攻击者可能通过篡改网络拓扑信息,误导SDN控制器做出错误的路由决策,从而影响网络的正常通信
流量嗅探	应用层、控制层、数据层	攻击者通过监听或捕获网络中的数据包,从而获取敏感信息或进行恶意活动
数据包注入	控制层、数据层	攻击者向SDN网络中的控制层注入经过篡改或变形的控制数据包
ARP欺骗攻击	控制层、数据层	该攻击通过伪造网络设备的ARP响应,欺骗其他设备发送数据到错误的目标地址
流表洪泛攻击	控制层、数据层	攻击通过向SDN网络中的交换机发送大量的流表项请求,导致交换机的流表资源耗尽,从而无法再处理正常的网络流量

1)应用层攻击。SDN应用层遭受的攻击主要源于和控制器通信的北向接口缺乏保护。攻击者可能利用北向接口的漏洞或缺陷,通过发送恶意请求、注入恶意代码或伪造数据等方式,试图获取对应用层的

非法访问权限。攻击者在获取网络拓扑、设备配置等敏感信息后,能够篡改网络配置,最终导致网络数据泄露。Hamarsheh[9]介绍了攻击者使用应用程序来操纵控制器,在应用程序和控制器之间的交换过程中,恶意代码可以通过北向 API 引入控制软件。Yungaicela-Naula[10]介绍了 DoS 和 DDoS 这类漏洞攻击在应用层资源耗尽时运行,通过注入数据包洪泛使网络增加延迟。

2)控制层攻击。攻击者往往瞄准 SDN 控制器的脆弱点,通过伪造网络流量、利用协议漏洞或 DoS 攻击等手段来控制和破坏控制层的功能。攻击者可以获取网络的完全控制权,导致网络服务的瘫痪。因此,SDN 控制器必须在应用程序使用前对其进行身份验证和授权[11]。如果控制器上的流数量增加,很有可能延迟也会增加,这意味着控制器需要更多的处理性能。当控制器的处理性能被限制时可能会导致整个网络故障[12]。

3)数据层攻击。SDN 数据层由 OpenFlow 交换机组成,这些交换机容易受到流表修改和拓扑欺骗的攻击。在流表修改攻击中,恶意节点可以插入或修改流表规则,来窃取通信信息或进行中间人攻击。拓扑欺骗攻击则通过创建虚假的网络视图,将流量重定向到攻击者的设备。由于 SDN 中 OpenFlow 交换机的决策能力通过控制层和数据层而分离,因此交换机容易在区分真实流规则和虚假流规则时收到攻击[13]。除此之外,OpenFlow 交换机还在处理流表流量时也容易受到饱和攻击[14]。

为了抵御 SDN 中 3 层结构面临的各种攻击。需要采取有效的入侵检测方法来应对这些威胁,确保 SDN 网络的安全稳定运行。下面将详细阐述这些检测方法。

3 SDN 入侵检测方法

3.1 基于机器学习的 SDN 入侵检测方法

在网络安全领域,引入机器学习技术为 SDN 的入侵检测带来了革命性的变革。通过将机器学习算法应用于 SDN 的流量监控和分析中,研究人员能够基于历史流量数据训练出高效的模型,构建出智能的流量分类工具。这些算法不仅能够提取网络流量的关键特征,还能通过精准的模式识别技术有效地识别出异常流量,进而实现对网络攻击的准确检测。机器学习算法的多样性和灵活性为研究人员提供了广阔的选择空间,使 SDN 网络更加安全、高效。

3.1.1 基于 DT 的检测方法

决策树(decision tree, DT)的节点代表特征做出的决策判断,每个叶节点表示为对应类的标签。根节点到特定类的叶子节点的路径进行分类可以对网络攻击进行划分。为了有效提升 SDN 网络安全性,李道全等[15]提出一种基于 DT 的 SDN 网络入侵分类检测模型。该模型利用类间中心距离确定类别分离顺序,将多分类任务分解为多个二分类任务。实验证明,该算法检测性能良好。但是 DT 算法在分类过程中可能出现数据移位的问题,Jeba 等[16]结合贪婪特征选择算法(GFS)和决策树算法提出了决策树检测(DTD)模型来检测 DDoS 攻击,有效解决了数据移位的问题,通过对比其他监督学习算法和无监督学习算法,该算法模型在 Gurekddcup6 测试数据中的准确率达到最优为 98.42%。

3.1.2 基于 NB 的检测方法

朴素贝叶斯(naive bayes, NB)可以通过计算条件概率来推断网络流量中潜在的安全威胁。在训练阶段,NB 从已知的数据集中学习特征与类别之间的关系,然后得到每个特征在特定类别下的条件概率。当新的流量数据进入网络系统时,通过比较贝叶斯定理计算正常流量和异常流量的后验概率。因此,NB 能够判断当前流量是否属于异常流量。NB 成为机器学习中有效对网络攻击进行检测的方法,Janabi 等[17]提出基于 NB 的新 SDN 网络安全系统模型 NB-PSDP。该模型设独立通道用于交换机和控制器间数据传输,去除了 SDN 流表冗余数据,通过 NB 算法进行特征选择以减少特征提取量、降低通道数据传输量,有效防护 SDN 网络各类网络攻击。

3.1.3 基于 SVM 的检测方法

支持向量机(support vector machine, SVM)通过寻找最大间隔超平面将正常流量与异常流量相分离,能够有效帮助基于 SDN 的入侵检测方法对网络流量分类。为了处理非线性数据的问题,SVM 引入了核函数(kernel function)。核函数将原始数据映射到一个更高维的特征空间,使得原本线性不可分的数据在

映射后的空间中变得线性可分。Hadem 等[18]为了能够处理更复杂的网络攻击模式,在基于 SVM 算法的基础上设计了一种 SDN 平台下的日志 IP(Internet Protocol)溯源系统。SDN 控制器在 PACKET_IN 事件中检测异常流量时,通过选择性记录可疑数据包或数据流能够在发生攻击后执行 IP 追溯,网络管理员便可以利用基于 HTTP 的 Web 控制台发起攻击检测。此外,该日志记录方法是在 SDN 的控制器上执行的,相比在交换机中执行节省了内存资源。因此 SVM 不但在缩减了计算开销的前提下保持了较高的检测精度,还使日志记录方法节省了大约 90%~95% 内存资源。

3.1.4 基于 KNN 的检测方法

在网络安全领域,K 最近邻(k-nearest neighbor,KNN)通过比较新数据与训练样本集中数据点距离,找出与新数据最相近的 k 个邻居并分类,判断其是否为潜在入侵行为。Madathi 等[19]为应对控制器遭受的 DDoS 攻击,把 DDoS 攻击特征输入 CSV 文件,经 KNN 算法训练分类后,使控制器在主机接收 DDoS 流量模式时可检测攻击,有效预防网络中断。

3.1.5 基于 K-means 的检测方法

K-means 能够对网络流量进行聚类分析,通过对比实时流量与聚类中心的差异在 SDN 环境中及时发现异常流量,从而有效判断潜在的入侵行为。Qian 等[20]针对基于 K-means 算法检测 DDoS 攻击精度不稳定的问题,提出基于密度选择的改进型 MIK-means 检测方案,该方案能在不同攻击类型和速率下使入侵检测平均准确率超 96%,提升检测效果且降低计算开销。Xu 等[21]将 K-means 算法与 FKNN 算法结合得到 K-FKNN 算法,该算法在 SDN 环境检测 DDoS 攻击时具备高效率、高精度和稳定性。

3.1.6 基于 PCA 的检测方法

主成分分析方法(principal component analysis,PCA)能够保留数据中的主要变化方向,这便是 PCA 的主成分,这些主成分往往对应着入侵行为的关键特征,因此可以更准确地识别出异常流量。Sahoo 等[22]为提升 PCA 在 SDN 中的检测精度,将可处理非线性可分数据的核主成分分析方法 KPCA 与遗传算法(genetic algorithm, GA)相结合辅助 SVM 检测,先以 KPCA 降维特征向量,再用 GA 优化 SVM 参数,实验表明该模型采用核函数主成分分析,较一般 PCA 减少主成分个数、性能更优。

本节分析和阐述了典型的 SDN 环境中机器学习的入侵检测方法及表现。表 2 的其他文献也汇总多种其他机器学习的应用。

表 2 基于机器学习的入侵检测方法

方法	数据集	运行机制	局限	文献
KPCA+SVM	NSL-KDD	相比前一方法,该方法则是使用KPCA算法对特征向量进行降维,然后采用遗传算法对不同的SVM参数进行优化	该模型结合的两种算法,在处理大规模网络流量时,会导致检测延迟或实时性能下降	[22]
DT、SVM	KDD99	在SDN架构中结合DT和SVM方法,构建一个高效、智能的入侵检测系统	SDN控制器可能成为单点故障点,影响系统稳定性和安全性	[23]
ID3	自定义数据集	该方法融合了机器学习与遗传算法,构建了入侵检测系统以实时监控网络流量、精准检测并有效分类网络攻击		[24]
XGBoost+BF	自定义数据集	首先,使用P4编程收集定制数据包,提取优化攻击特征。其次,借助XGBoost分类器识别异常包并定位攻击源。最后,BF快速识别后续攻击	自定义数据集可能没法反映真实的网络环境,存在误报和漏报的风险,除了可能存在漏报和误报的风险外,当大量数据进入网络时检测效率可能偏低	[25]
SVM+RF	自定义数据集	比对了8种机器学习算法做入侵攻击检测得出SVM+RF的效果最佳。接着使用丢弃非法流量和重定向非法流量2种方法来缓解网络攻击		[26]

表 2 基于机器学习的入侵检测方法 (续)

方法	数据集	运行机制	局限	文献
SVM+DNN	自定义数据集	针对物联网医疗生态环境,作者在SDN架构下使用了机器学习SVM和深度学习DNN的混合算法来保障医疗网络系统的安全性	除了以上自定义数据集的问题外,在资源受限的偏远地区部署这样的系统可能造成网络不稳定	[27]
RF、NB	NSL-KDD	该方法通过机器学习技术监控网络行为以检测异常,并采用预留带宽的策略,确保优先级较高的应用能够获得高效带宽	机器学习模型可能面临数据质量和计算资源的挑战,预留带宽策略会影响网络灵活性	[28]
ML+Entropy	DARPA数据集和自定义数据集	该方法融合了机器学习和熵两种方法来识别攻击。先使用信息熵作为过滤器,接着使用机器学习算法SVM+RF来识别攻击	新型的攻击检测可能不够准确	[29]

机器学习在 SDN 中的入侵检测中展现了显著的效果,它能保障网络安全稳定地运作。机器学习算法擅长在海量数据中提取特征然后自动构建模型来识别潜在的攻击威胁。实现更广泛、更灵活的入侵检测,提高了监测系统的适应性和准确性。然而,机器学习在处理高纬度和复杂环境的网络时,会产生计算复杂度和性能瓶颈的问题。在资源条件适宜的情况下,选择机器学习算法能够应对潜在的网络威胁。

3.2 基于深度学习的 SDN 入侵检测方法

深度学习以其强大的特征学习能力和层级抽象能力,为 SDN 网络的安全防护注入了新的活力。通过将深度学习算法应用于 SDN 的流量监控和分析中,研究人员基于海量的网络流量数据训练出高准确性的模型,从而构建出智能且高效的入侵检测模型。深度学习模型能够自动学习和提取网络流量的深层次特征,通过复杂的模式识别机制,精准地识别出异常流量,实现对网络攻击的及时预警和准确检测。

3.2.1 基于 DNN 的检测方法

深度学习神经网络(deep-learning neural network, DNN)是一个具有许多隐藏层的前馈架构。DNN 能够在 SDN 中自动学习网络流量的深层特征,通过逐层地分析提取出有效的入侵攻击行为。为了缓解大量的攻击入侵 SDN 网络,Makuvaza 等[30]使用 DNN 实时检测 SDN 中 DDoS 攻击,利用较少的资源和时间使入侵检测的检测准确率达到了 97.59%。Razib 等[31]提出了 DNN+LSTM 相结合的模型应对大量网络攻击威胁,该模型在 CICIDS2018 数据集上训练,对准确率、精度、召回率和 F1-Score 这 4 个重要参数进行评估。

3.2.2 基于 RNN 的检测方法

循环神经网络(recurrent neural network, RNN)是一种特殊的神经网络结构,专门设计来处理序列数据,如时间序列、文本或语音等。与传统的前馈神经网络不同,RNN 具有内部记忆功能,能够在处理序列时捕捉和利用之前的信息。其核心原理在于其循环连接的特性,因此,网络能够记住并应用之前的信息到当前的计算中。基于此,Razib 等[31]基于相关需求提出基于正则化技术的 RNN 模型(RNN+SDR),其中正则化用于泛化机器学习模型使数据集达最佳测试效果,与其他模型相比,该方法采用特征数量最少,对 SDN 控制器性能影响极小。

Albahar[32]利用卷积神经网络(convolutional neural networks, CNN)和 LSTM 混合网络来提取网络流量的时空特征。首先采用 L2 正则化和 dropout 两种正则化技术解决了过拟合问题,然后对 InSDN 数据集训练和测试 CNN+LSTM 方法。实验结果表明,将 CNN+LSTM 相结合提高了入侵检测性能,准确率达到 96.32%,精度高于单独的模型。

Ravi 等[33]设计了一个基于 GRU 的模型来对 SDN 的物联网环境进行入侵检测。模型在 GRU 中提取网络数据的内部特征,然后利用核主成分分析方法[22]提取最优特征,最后将特征融合在一起后利用全连接网络进行攻击检测和分类。该方法可以实时有效地监控 SDN 下物联网环境的网络流量,主动预警可能发生的攻击。

3.2.3 基于 CNN 的检测方法

由于 SDN 集中管理的特点,CNN 能够通过训练网络流量的正常模式识别出潜在的入侵行为。通过

内部的卷积层、池化层和全连接层对网络流量数据进行特征提取以及降维等操作,CNN 为网络的安全防护提供了有力保障。为了提高入侵检测的准确率,ElSayed 等[34]开发了基于 CNN 算法的混合模型,采用基于权矩阵标准差的新正则化方法 SD-Reg 解决过拟合,增强网络入侵防御系统检测未知事件能力并提升 CNN 预测效率。实验显示,CNN 与 RF 算法结合能提高入侵检测精度,有效解决轻量级入侵检测性能不足问题。

3.2.4 基于 AE 的检测方法

堆叠自动编码器(autoencoder, AE)通过编码器将输入的网络流量数据映射到低维空间,再由解码器从低维空间重构回原始输入流量空间。模型依靠训练过程中的最小化重构误差来优化其参数,进而可以学习到网络数据的特征表示。Lee[35]运用 AE 算法,在无监督学习的网络运行时用自动收集的恶意数据包训练深度学习模型,取得了良好的效果,AE 模型能借对比重构误差识别异常流量,还可结合其他算法提升网络防御能力。Yao 等[36]提出了一个基于 AE+LightGBM 的入侵检测混合方法。该模型首先利用 Borderline-SMOTE 过采样算法平衡数据样本分布,然后使用 AE 减少冗余特征的影响,最后利用 LightGBM 完成最终分类。该模型不仅减少了数据分布不平衡的负面影响,而且增强了模型的泛化能力。此外,它还保留了 LightGBM 的高实时性优势。在 KDDCup99 和 NSL-KDD 数据集上的实验结果均表明,该模型的准确率、精密度和 f1 分数性能均优于传统模型,在实时性方面具有显著优势。

3.2.5 基于 GAN 的检测方法

基于 SDN 可编程的特点,在应用层引入生成对抗网络可以提高入侵检测模型的判别能力。生成对抗网络(generative adversarial networks, GAN)通过生成器和判别器多次的迭代训练自动地学习攻击数据的特征。在入侵检测模型中可以有效降低模型的误报率。Ezeh 等[37]在 SDN 的控制器上通过 GAN 算法迭代学习的方式来检测网络的异常行为,作者使用生成数据集中的正常、DDoS、DoS 和枚举这 4 种网络流量类型验证 GAN 模型的效果。使用的数据集就像新数据一样,在两个数据集中的平均检测准确率都在 90% 以上,这证明了基于 GAN 的算法在训练一个网络后用于异常检测有着巨大的潜力。在此基础上,Khekare 等[38]结合了 GAN 和 RNN 的优点解决了网络管理的 2 个重要方面:流量优化和访问控制。GAN 由于其强大的模型生成能力几乎完美地复制了真实网络流量的复杂性,网络管理员便可以更灵活地分配资源和路由方法,RNN 则是可以持续学习网络的数据特征。通过 GAN+RNN 混合算法自适应地访问安全协议和真实的网络数据,实验结果得出了 99.4% 的准确率,优于其他方法。表 3 列举了其他应用于 SDN 的深度学习技术的相关文献。

表 3 基于深度学习的入侵检测方法

方法	数据集	运行机制	局限	文献
DNN+PCA	UNSWNB15	提出了一种SDN环境下基于DNN+PCA的扫描攻击检测模型。通过实验选择适当的降维数据作为DNN输入,引入2个额外参数来改进ReLU函数	在处理大规模网络流量时,该方法会导致检测延迟或实时性能下降	[39]
LSTM+CNN	NSL-KDD	该算法先是融合了正弦余弦算法和金枪鱼优化算法对数据集进行特征选择,然后使用LSTM和CNN方法对SDN中的网络攻击进行分类检测	正弦余弦算法在搜索过程中可能容易陷入局部最优解,该算法通过LSTM+CNN结合会显著增加模型复杂度,可能出现过拟合的现象	[40]
Hybrid LSTM	InSDN	与上一方法同样针对于高维数据,使用特征选择方法进行降维,降低了不利特征对检测的影响。然后区别于以上二分类的方法,提出了一种基于多分类的混合LSTM的入侵检测模型	针对多分类算法的性能较好,但对于二分类的检测效果可能性能效果不佳	[41]
BiLSTM	CSECICIDS2018	该算法是在无线网络环境中,建立了一种BiLSTM模型,BiLSTM模型允许两个独立的LSTM一起在向前和向后方向上执行并行操作,在特定的时间框架内按顺序存储信息。每个LSTM有3个门:输入门、遗忘门、输出门	虽然BiLSTM通过双向LSTM的堆叠可以一定程度上缓解长序列的局限性,但是对于过长序列的处理能力依然有限	[42]

表 3 基于深度学习的入侵检测方法 (续)

方法	数据集	运行机制	局限	文献
DNN+LSTM+GRU	CICDDoS2019	该方法则是分别结合了DNN+LSTM和DNN+GRU算法对SDN的可编程控制平面进行检测	该方法主要针对控制层进行防御检测,对于应用层的入侵攻击可能会检测不到位	[43]
CNN+LSTM	CICIDS2017	利用LSTM和CNN的预测能力来检测SDN控制平面中的网络威胁	LSTM和CNN的性能高度依赖于训练数据的质量和数量。训练数据不足以覆盖所有可能的网络威胁场景	[44]
CNN+Transformer	CICDDoS2019	该架构结合了CNN和Transformer模型,其中Transformer层提供计算能力和可扩展性,以处理网络流量的全局特征;CNN层则利用卷积操作捕捉局部特征,提供强大的分析能力	虽然Transformer在捕捉全局信息优于上一方法的LSTM,但是如果混合DDoSTC架构中的关键组件(如控制器或数据处理单元)出现故障,整个系统会受到影响	[45]
CNN+GRU	CICDDoS2019、CICIDS2017、InSDN	数据经过预处理后,使用CNN从数据中提取出空间特征,这些特征随后被输入到多层GRU中,用于对与输入数据相关的时间特征进行建模,GRU相比其他算法可以有效避免过拟合	对整体的特征提取效果不如CNN+Transformer方法,忽略了部分和整体的关联性	[46]
CNN、LSTM、MLP、SAE	自定义数据集	将SDN交换机中的数据包长度作为序列收集,用于深度学习模型识别异常和恶意数据包	网络攻击和异常行为往往不仅体现在数据包长度上,还会涉及其他多个维度的特征,无法全面反映网络流量的多样性	[47]
GAN+DBN+LSTM	CICDDoS2019	首先,通过SDN控制器实现IP流记录的细粒度监控与采集,其次,通过归一化和香农熵预处理数据。最后,设计了一种GAN−DBN−LSTM异常检测方法识别DDoS攻击	DBN和LSTM都是复杂的深度学习模型,需要大量的计算资源进行训练	[48]
Transformer、Inception−BiGRU−SA	CICIDS2017和CICddos2019	提出了基于Transformer和Inception−BiGRU−SA网络的入侵检测模型TIBS。首先,TIBS由Transformer的Encoder部分用于全局捕获连接,并对输入数据进行初步的特征提取。其次,利用改进的Inception模块提取多尺度特征。利用SA对提取的不同尺度空间特征进行加权,使用BiGRU提高模型提取时间特征的能力,最后,使用Softmax激活函数进行最终分类	TIBS模型结合了多种先进的深度学习技术,因此,模型具有较高的复杂度和较多的参数	[49]

深度学习在 SDN 环境中的入侵检测展现了卓越能力。它能高效处理大规模、高维度数据,精确分辨复杂攻击,为网络安全提供有力保障。然而,该方法需要大量训练数据和高资源投入,限制了其在资源有限场景的应用。尽管如此,对于复杂多变的攻击模式和大规模数据处理需求,深度学习仍有较好的效果。因此,在资源充足的条件下,深度学习为 SDN 环境中的入侵检测提供了强有力的技术支持。

3.3 基于强化学习的 SDN 入侵检测方法

通过不断地在网络环境中试错和学习,强化学习有利于入侵检测方法自动优化其行为策略,使基于 SDN 的入侵检测方法更有效地检测和应对各种网络攻击。强化学习在构建入侵检测方法时,首先对数据包的源 IP 地址、目标 IP 地址、端口号等各种网络状态特征进行建模,然后设计奖励函数用于监控系统状态的变化以及是否检测到网络攻击等指标,最后表示出网络入侵攻击的概率以及系统该如何响应这些入侵攻击。

Q−learning 是一种 Off−policy 强化学习算法[50],用于确定在给定当前情况下的最佳行动方案。由于 Q−learning 函数是从其自身的行为中学习,而不依赖于任何特定的现有策略,因此被称为 Off−policy。这样的特点使得 Q−learning 具有更高的灵活性,能够在学习过程中不断优化其决策方案。根据以上特点,Nguyen 等[51]开发了一种基于 Q−learning 的算法 CARS(竞争性自适应重加权算法)来提升优化效果,方案得到了最优的网络攻击反应策略。以 DoS 为例,研究结果验证了 CARS 在所有 DoS 攻击中都能有效阻止恶

意数据包到达受害服务器,约 80% 的异常数据包被丢弃。此外,通过实施最优网络攻击反应策略,CARS 与现有的 2 种解决方案相比,可显著降低服务质量(quality of service, QoS)中违规流量比例。Phan 等[52]同样为了确保大规模物联网 SDN 优质的服务质量和体验质量(quality of experience, QoE),基于马尔可夫决策过程(Markov decision process, MDP)方法提出一种新的深度强化学习 DQQS 算法,该算法模型通过强化学习算法从底层网络生成优化的路由策略,在过去的网络历史中提取动态防御模式。而 Arif 等[53]基于马尔可夫决策过程方法对入侵响应系统进行建模,开发了一种基于双 Q 网络的入侵响应控制算法,帮助入侵响应系统快速获得最优的入侵响应策略。

Mnih 等[54]将 Q-learning 与 DNN 相结合,提出了在离散动作空间内运行的 DQN(深度 Q 网络)算法。DQN 智能体是一种基于价值的强化学习智能体,在训练好函数后可以预测未来的奖励或回报,可以有效提升入侵检测的预测能力。在前辈的基础上,Phan 等[55]还提出了一种深度 DQN(Deep DQN)算法,该方法在主动保护 SDN 数据平面不过载的同时,还学习流量匹配策略,最大限度地提高流量粒度。随后,通过实施学习到的最优流量匹配控制策略,在运行时获取对异常检测最有利的流量信息,提高了网络攻击检测性能。OpenAI 团队在 2017 年推出了 PPO(近端策略优化)算法[56],它超越了 DQN 成为最受欢迎的强化学习方法之一。这是一种策略梯度方法,用于各种基于强化学习的应用中训练决策策略。它收集环境的小样本,并使用该样本来更新决策策略。为了针对洪泛攻击的入侵,Shen 等[57]使用了 PPO 算法来缓解洪泛攻击,将 PPO 算法与可编程交换机结合使用有助于将网络的自动化攻击检测得以优化,Zolotukhin 等[58]进而提出了一种基于 DQN+PPO 的强化学习算法,该技术通过 K-Means、SOM(自组织映射)、FCM(模糊 C 均值聚类)算法强化了学习代理,计算 SDN 中主机数据包的最大数量,并设定了进程阈值规则,采用质心聚类方法检测异常负载。保障了 SDN 的稳定运行。

针对 SDN 受网络攻击致系统性能降低的问题,Li 等[59]提出闭环安全架构(SFCSA),该架构组合检测方法形成检测路径,不同路径对安全性能影响各异,该文章将路径选择问题建模为马尔可夫决策过程,利用奖励机制平衡恶意流量检测能力与端到端延迟,进而提出集成深度强化学习和 CNN 的路径选择算法(CNNQ),实验结果显示,组合多个检测模块的检测性能优于单个基于检测的模块。Allakany 等[60]使用了基于强化学习的 LFA 防御系统,该系统有效地转发了网络中的数据流量。LFA 还引入了贝叶斯统计来检测 IP 行为的新检测算法,监视并识别响应重路由事件的源 IP。在前文基础上,Wang 等[61]针对物联网 SDN 中的 LFA 问题,提出了一种新的 LFA 缓解方案 ReLFA。在文章的方案中,根据告警阈值确定目标链路,使用 Renyi 熵可以定位数据平面的拥塞链路。当目标链路检测到 LFA 时,控制平面采用基于 DRL 的方法进行流量工程的检测。

在应对 SDN 环境中的网络安全挑战时,研究者引入基于强化学习的入侵检测方法。其他强化学习方法通过智能试错和自适应学习,不断提升检测能力,为 SDN 网络提供更为高效和精准的安全防护,具体如表 4 所示。

强化学习在 SDN 环境中的入侵检测领域展现出了显著的优势和独特的适应性。它通过优化目标函数来自主寻找最佳策略,能够做出最智能的决策,有效应对各种网络入侵行为且显著减少了人工干预的需求。然而,强化学习在某些复杂或不稳定的环境下可能难以找到最优策略,导致检测效果有所波动。尽管如此,对于需要实时检测网络环境变化的场景,强化学习依然展现出了强大的潜力,能够迅速适应网络变化并做出相应调整。因此,在 SDN 环境中,强化学习为入侵检测提供了一种高效、智能的解决方案。

3.4 基于信息熵的 SDN 入侵检测方法

在网络安全领域,熵可以用来度量网络系统的随机性。这种随机性可能由网络流量的变化带来的、也可能是用户行为的异常或潜在的攻击引起的。基于熵的方法通过计算这些随机性能够帮助网络管理员更好地评估基于 SDN 网络环境下系统的安全状态和增强系统的防御能力。基于熵的方法在特征选择和权重分配上发挥重要作用[67]。在入侵检测中,特征选择是构建有效检测模型的关键步骤。通过计算各个特征的熵值,可以评估区分正常和异常行为的重要度。具有较高熵值的特征通常包含更多的信息量,因此更可能与攻击行为相关。基于这些熵值,可以为不

表 4 基于强化学习的入侵检测方法

方法	数据集	运行机制	局限	文献
RL	Mininet平台生成的数据	通过收集网络指标分类为配置文件,利用强化学习指导SDN控制器处理操作,并根据动作奖励设置异常检测策略。该模型以在线方式平衡流量负载,并通过Linux机器人检测蜜罐	虽然通过Linux机器人检测蜜罐可以提高安全性,但这也会引入新的安全风险	[62]
神经网络拟合Q-learning	模拟的流量	基于神经拟合Q-learning代理的威胁检测机制ATMoS通过在模拟实验床上部署恶意主机和良性主机的变种来检测APT和TCP SYN-flood攻击	攻击者破坏或操纵ATMoS的训练过程或决策过程会导致系统失效或产生错误的响应	[50]
DQN	自生成常规网络流量	DQN代理基于价值学习,利用神经网络预测未来回报,指导智能体作出更优决策	DQN算法在连续动作控制问题上表现不佳。这限制了其在某些需要连续动作决策的场景中的应用	[54]
DQN+PPO	自生成常规网络流量	该方法在上一方法的基础上,先计算出主机数据包的最大量,并据此为不同进程设定阈值规则。随后,利用Snort虚拟设备监控网络流量,一旦检测到超过阈值的异常流量,立即触发警报	解决了上一方法的不足,但在重定向SDN流和实时分析网络流量在网络环境的可扩展性不足	[58]
DDPG+MDP	使用Iperf和Hping3工具生成	该方法采用DDPG算法为SDN网络的多个流量分析器设计了一种低侵入性的流量采样机制	尽管该方法旨在减少流量监控开销,但将采样流量发送到多个流量分析器仍然会产生额外的网络传输开销	[63]
MADDPG+DNN	模拟的流量	提出了一种新的MADDPG集成多代理框架,2个MARL代理在同一环境中相互协作,在较短的时间内完成网络优化任务。使用马尔可夫决策过程进一步对所提出框架的状态、行为和奖励进行数学建模,并随后集成到MADDPG算法中	随着代理数量的增加,每个代理的策略梯度估计的方差也会增大,这可能会降低算法的学习效率和稳定性	[64]
GCN+DRL	NSL-KDD	算法结合了GCN图神经网络和DRL强化学习方法来模拟提取最优空间序列特征	使用的深度学习算法缺乏对时间序列特征的提取	[65]
ABO-DRL	自定义数据集	提出了一种MMEDRL-ADM技术,该方法首先设计了基于非洲水牛优化算法的特征选择(ABO-FS),降低了计算复杂度,提高了检测率。然后采用多层集成深度强化学习技术,为了调整MEDRL技术的超参数值,提出了一种改进的IGOA优化算法,根据IGOA的超参数整定模型来检测SDN云环境中的DDoS攻击进行检测	超参数的优化结果可能受到初始值、数据集特性等多种因素的影响,导致优化结果的不稳定性	[66]

同的特征分配不同的权重,从而在构建检测模型时更加关注那些与攻击行为高度相关的特征。但是,传统的基于熵的攻击检测方法存在攻击检测速度慢、检测效果差等缺陷。因此,Yadav 等[68]提出了一种新的状态判定标准,利用未发生攻击时熵值的正态分布特征,对熵值所代表的正常和异常范围进行细分,提高了攻击判定的准确性,通过数值分析验证了该方法的有效性。而 Mohammad 等[69]则是提出了一种基于 RYU 控制器的 DDoS 攻击检测和缓解的方法。该方法通过设置控制器的熵值来阻塞交换机中的特定关口,然后关闭该端口来检测和缓解 DDoS 攻击。

在 SDN 环境中,基于熵的入侵检测方法通常依赖于网络流量的熵值变化来检测异常。然而,当网络流量本身就存在较大的不确定性或随机性时,熵值的计算可能会受到影响,导致难以准确区分正常流量和异常流量。Santos-Neto 等[29]为了避免大量数据造成检测效率的降低,该方法融合了机器学习和熵 2 种方法来识别攻击。先使用信息熵作为过滤器,接着使用机器学习算法 SVM+RF 来识别攻击。而 Zhang 等[70]针对 SDN 网络对 DDoS 攻击的独特敏感性,提出结

合基于信息熵的初始检测与基于 SSAE+SVM 架构的机器学习二次检测的混合 DDoS 攻击检测方法。首先初始检测模块借信息熵快速识别异常流量,接着二次检测模块确认可疑流量。仿真显示,检测到 DDoS 流量时防御模块能依流量表恢复网络通信;且两模块顺序使用,相比单独使用 SSAE+SVM 检测模块,CPU 利用率和时间成本更低,计算效率更高。

SDN 环境的网络流量是动态变化的,包括流量类型、速率、方向等。基于熵的入侵检测方法在原理上可能难以适应这种动态变化。当网络流量模式发生显著变化时,熵值的计算可能不再准确,从而影响入侵检测准确性。Shohani 等[71]鉴于现有基于信息熵和 PCA 的方法在 SDN 环境下检测 DDoS 攻击效率不足,提出新网络流量检测框架应对 DDoS 攻击。该框架含 4 个阶段:先在 SDN 测试平台大量实验,分析正常与攻击流量行为;接着提出统计梯形模型估计控制器表缺失数;再用线性回归估算规则时间间隔内表缺失阈值;最后以导出模型为参照检测 DDoS 攻击异常偏差。评估显示,此方法能在早期检测针对 SDN 网络的 DDoS 攻击,几乎无误报,不受攻击具体情况影响。

基于熵的入侵检测方法通常需要根据经验或实验设定一个或多个阈值来判断是否发生了入侵。然而,阈值的设定是一个复杂且主观的过程,可能受到多种因素的影响,如网络规模、流量特性等。不恰当的阈值设定可能导致检测效果不佳。所以,Fan 等[72]提出了一种创新的熵融合方法,该方法巧妙地结合了信息熵和对数能量熵的优势,实现了 2 种熵的互补效应。这种融合熵不仅检测速度快,而且熵值变化显著,能够在最短的时间内迅速检测到攻击。此外,当攻击发生时,其熵值相比正常情况下降了约 91.25%,因此,能够高效地识别出攻击行为。与其他攻击检测方法相比,这种融合熵方法在保护 SDN 控制器免受 DDoS 攻击方面具有显著的优势。Niknami 等[73]讨论了一种结合机器学习和熵的检测入侵攻击的方法,该组合方法被称为熵−KL−ML 方法,该方法利用熵与 KL−散度和集成机器学习来检测时隙内传入数据包中的异常情况,可以解决因阈值设定不准带来的系统准确率下降的问题。文章中还提出了一种新的基于特征分组的特征选择方法,减少了控制器的计算开销。最后,KL 散度和 ML 分类器使检测更加准确。Liu 等[74]结合了深度学习和信息熵的监测机制,该方法首先对可疑部件和端口进行粗粒度检测。随后,通过 CNN 模型执行基于细粒度数据包的监测来区分正常流量和可疑流量,控制器最后执行防御策略进行拦截攻击。实验结果表明,该方法的检测准确率达到 98.98%,显示了在 SDN 环境中有效检测 DDoS 攻击流量的潜力。

在控制器发生故障的情况下,交换机将尝试根据转发表中的最后一组表项继续转发流量。因此,当某个控制器由于转发表的过期时间或容量限制而失效时,该控制器将无法处理新到达的数据包,这将导致整个网络瘫痪。由于控制平面和数据平面之间存在漏洞,所以 DoS 攻击和 DDoS 攻击往往是 SDN 面临的最大风险。Aladaileh 等[75]提出基于 Renyi 联合熵的检测方法,将其用于网络流量分析,该方法结合两个包头特征及广义 Renyi 联合熵,能有效识别针对 SDN 控制器的不同速率 DDoS 攻击,规避控制器故障风险。Ujjan 等[76]通过结合 Shannon 熵和 Renyi 熵的方法来检测 DDoS 攻击,可以降低 SDN 的资源开销。这种组合熵技术可以减少控制器的开销,当检测 30% 的攻击流量时,熵计算过程使用了大约 25% 的 CPU。当攻击强度为 60% 时,分配的流量特征只使用了 5% 的 CPU。

基于熵的入侵检测方法通常通过比较熵值的变化来识别攻击模式。然而,对于某些复杂的攻击模式,尤其是那些能够伪装成正常流量的攻击,仅依靠熵值的变化可能难以有效识别。这可能导致漏报或误报的情况增加。使用融合熵方法提高检测的效果。Ladigatti 等[77]提出利用无监督学习结合融合熵的方法,先通过访问控制列表过滤 IP 以减轻控制器攻击负荷,再用融合熵检测 DDoS 攻击、识别可疑主机,最后在可疑主机上采用基于工作量证明的计算谜题检测并缓解攻击,实验显示该方法能有效检测、缓解 DDoS 攻击且误报率较低。

在 SDN 网络安全领域,研究者运用基于信息熵的入侵检测新策略。如表 5 所示,通过信息熵对网络流量不确定性的精确度量,这些方法能够敏锐地捕捉异常流量模式。

信息熵在 SDN 环境中的入侵检测具有显著优势

表 5 基于信息熵的入侵检测方法

方法	数据集	运行机制	局限	文献
联合熵	hping3工具生成	通过识别未受攻击时熵值的正态分布特性,对熵值所指示的正常与异常状态进行了更为细致的区分	如果数据收集不完整、不准确或存在偏差,计算出的熵值会偏离真实情况	[68]
联合熵		该方法首先利用信息熵的初始模块快速识别异常流量,然后使用基于SSAE+SVM架构的二次模块进行进一步确认	随着网络规模的扩大和复杂性的增加,该方法面临可扩展性不佳的问题	[70]
联合熵	Python脚本生成	通过分析网络流量特征,结合了包头特征和Renyi联合熵,有效提高了DDoS攻击流量的检测率	对于新型或变种的DDoS攻击,需要进行模型更新	[75]
联合熵	Scapy工具生成	利用信息熵和对数能量熵的互补性,通过测量网络事件的随机性来检测攻击,有效解决上一方法对新型攻击检测率较低的问题	该方法主要关注网络事件的随机性,缺乏关于网络流量上下文信息的深入分析	[72]
联合熵		首先运用广义熵计算识别DDoS流量的特征来辅助SDN控制器处理恶意流量。然后使用Snort检测收集数据平面流量以降低开销进而分析基于熵的流量特征	方法准确性高度依赖于收集到的网络流量数据。当数据受到污染或伪造,会影响模型的训练和检测效果	[76]
条件熵		通过均值、标准差及条件熵值变化来精确识别异常流量。对数据预处理后,随机样本处理即可快速获取熵值,实现高效攻击检测	即使结合了签名型和异常型方法,仍然可能无法覆盖所有类型的网络攻击	[78]
Renyi熵		该方法使用Renyi熵进行信息距离的度量,然后使用丢包技术缓解攻击	Renyi熵在处理大规模网络流量时可扩展性较差	[79]
Renyi熵	CICIDS2017数据集	使用了带有随机森林分类器模型的混合深度自动编码器,提高本地SDN中的入侵检测性能。模型被整合到一个新的自适应框架中缓解SDN中的攻击。该框架基于混合熵和机器学习共同构成防御	尽管框架被设计为自适应的,但在面对快速变化的网络环境和攻击策略时,其自适应速度和准确性可能受到限制	[80]
统计熵	CICIDS2017、CICIDS2018、CICIDS2019	提出了一种将统计方法与机器学习功能相结合的混合方法,该方法的统计阶段采用基于熵的检测机制,而机器学习阶段采用聚类机制来分析活跃用户对系统熵的影响	熵的计算对数据分布非常敏感,如果数据存在噪声或异常值,可能会严重影响熵的准确计算,进而影响后续的分析结果	[81]

与特定局限性。其优势在于适应性强,对异常流量的变化非常敏感,能够快速识别出网络中的潜在威胁。然而,信息熵方法的不足在于阈值的设定较为困难,过高的阈值可能导致漏报,过低的阈值则可能引发误报。此外,对于复杂多变的攻击模式,信息熵的检测能力可能受到一定限制。尽管如此,信息熵在轻量级和实时性要求较高的网络环境中具有广泛的应用前景。在这些场景中,它能够在 SDN 中以较低的计算资源消耗实现高效的入侵检测,确保网络的稳定运行。因此,信息熵为 SDN 中的入侵检测提供了一种高效、实用的解决方案。

4 方法对比和评价指标

4.1 方法对比

入侵检测作为 SDN 安全防护体系中的重要一环,不仅能够在网络和系统受到危害之前进行报警、拦截和响应等操作防止网络入侵事件发生。还可以实时监测和分析网络流量,当入侵检测方法发现违反安全策略的异常行为或攻击迹象,就会立即发出报警,提醒管理员及时采取应对措施。基于机器学习、深度学习、强化学习和信息熵的入侵检测方法都在 SDN 环境中展现了各自不同的优劣势。表 6 是对各类方法进行的总结和对比。

4.2 评价指标

为了展现 SDN 中入侵检测各个方法的显著效果,需要设立一套典型全面的评价指标来评估方法的性能[82]。基于混淆矩阵的综合性分类方法可以系统地评估算法在识别攻击流量与正常流量时的准确性、效率及稳健性等。混淆矩阵根据预测值和真实值测算出真实正例(TP)、真实负例(TN)、错误正例(FP)以及错误负例(FN)等统计量(表 7)。

表 6 各类方法的总结和对比

名称	优势	劣势	主要算法	特点	
				相同点	不同点
机器学习	可以在一定程度上识别未知的攻击模式。并且通过训练数据可以适应不同的网络环境	模型的性能高度依赖于训练数据的数量和质量	DT、NB、SVM、KNN、K-means、PCA	基于数据驱动的方法,通过学习和分析网络流量数据来识别异常行为	在处理数据、特征提取和分类策略上有所不同
深度学习	能够自动从原始数据中提取高级特征,减少人工干预。在处理复杂和高维数据时,能够提供更准确的检测结果	训练深度学习模型需要大量的计算资源和时间。深度学习模型的决策过程相对复杂,难以解释其内部机制	DNN、RNN、CNN、AE、GAN	通过多层次非线性变换从数据中自动学习高级特征表示。能够自动学习数据的深层次特征	在网络架构、应用场景及学习机制上各具特点
强化学习	根据网络环境的变化自动调整检测策略	需要大量的训练样本来确保模型的稳定性和泛化能力	Q-learning、DQN、PPO、MADDPG	通过智能体与环境交互来学习优化策略	策略表示、更新方式以及是否依赖模型等方面存在差异
信息熵	快速计算并响应网络流量的变化	单独使用信息熵方法可能难以准确识别复杂的攻击模式	联合熵、统计熵、条件熵、Renyi熵	基于统计和信息论的方法,用于评估网络数据的复杂性和不确定性	在应用场景、计算公式和所度量的信息特性上有所差异

表 7 SDN 混淆矩阵

		预测值	
		ATTACK	NORMAL
真实值	ATTACK	TP	FP
	NORMAL	FN	TN

表 7 中,TP 是指正确检测到的攻击流量,TN 表示正确检测到的合法流量,FP 表示合法流量被检测为攻击流量,FN 则是被检测为合法流量的攻击流量。基于混淆矩阵,可以进一步计算出其他重要的评估指标,如 TPR、FPR、DR、Precision、ACC、ROC、AUC 等。

(1) TPR:真阳性率,在所有实际为恶意样本的数据中,被正确地判断为恶意样本的比率,该指标越高越好。(2) FPR:假阳性率,在所有实际为良性样本的数据中,被错误地判断为恶意样本的比率,该指标越低越好。(3) DR:检测率,表示该方法在检测恶意样本的能力方面的性能,该指标越高越好。(4) Precision:原本为恶意样本的数据占预测为恶意样本数据的比率,该指标越高越好。(5) ACC:将实例正确地分为良性样本和恶意样本的比率。(6) AUC:ROC 曲线下的面积即为 AUC 指标的值,ROC 曲线由 TPR 和 FPR 计算得到,该指标越高越好。

评估检测算法的性能时,计算效率与资源利用情况是至关重要的考量因素,它们直接关系到算法的运行效率、资源消耗快慢及响应时间的优化。核心的计算性能指标涵盖了 CPU 占用率、系统响应时间、内存消耗量以及数据处理速率等方面。这些指标为科研人员提供了全面审视算法在实际部署到 SDN 中的效果,进而为算法的精细化调整与优化提供了坚实的依据。

5 总结与展望

探索了 SDN 研究者基于各种方法的入侵检测方法,采用机器学习、深度学习、强化学习和信息熵等方法克服了 SDN 在入侵检测过程当中遇到的检测率较低、系统能耗较高、网络不稳定等挑战。但是,由于该领域处于初期探索阶段,目前仍有许多关键问题尚未被解决。

1) 单控制器易受网络威胁。SDN 引入了一个集中控制层,极大地增强了网络的控制、可编程性和管理能力。然而,这种中心化的架构也带来了安全隐患,因为缺乏足够健壮和安全的控制器平台使单控制器成为攻击者的主要目标[83]。一旦网络发生拥塞,可能导致 OpenFlow 交换机缓冲区溢出,从而引发控制包的丢失。这种丢失会导致底层设备可能无法及时接收到控制器的指令,而且还会产生网络拥塞、数据

包丢失或传输延迟等问题。如何确保单个控制器能有效地维护网络信息,仍是一个亟待解决的问题[84]。

2)缺乏可扩展性。在网络规模日益增大的情况下,SDN 中的控制器与交换机之间的通信常常受到网络拥塞的威胁。由于缺乏足够的可扩展性,SDN 环境中的入侵检测操作可能会付出高昂的代价。因此,未来将 SDN 的安全性与可扩展性紧密结合起来,以构建安全可靠的 SDN 体系结构显得尤为重要。

3)缺乏缓解和预防的方法。目前大多数研究主要集中在入侵检测方法本身,而很少讨论检测后的缓解方法。尽管有少数研究涉及到了这一方面,但明显缺乏对检测和缓解机制的综合性研究[85-88]。在实际应用中,当系统受到攻击时,能够迅速有效地防止攻击并保持 SDN 系统的正常运行,比单纯的检测和缓解攻击更为重要。因此,需要更多的研究来关注 SDN 基础设施中的攻击预防机制,而不仅仅是检测和缓解措施。通过发展预防机制,可以在攻击消耗网络资源之前,就有效地阻止攻击在网络中的扩散,确保连接的主机之间拥有公平的带宽分配、能量消耗和请求处理能力。

4)缺乏低速率 DDoS 的攻击检测。目前多数研究聚焦于高速率 DDoS 攻击的检测,而对于低速率 DDoS 攻击的研究相对较少。低速率 DDoS 攻击者通过短时间内发送大量突发攻击报文或持续以低速率发送攻击报文导致 SDN 的网络产生 TCP 拥塞漏洞[89]。由于低速率 DDoS 攻击发送的数据包种类较少,因此那些用于识别高速率 DDoS 攻击的特征可能并不适用于低速率 DDoS 攻击[90]。因此,检测低速率 DDoS 攻击仍然充满挑战,需要引起更多的关注和研究。虽然文献[86, 91-92]尝试使用基于机器学习的方法检测 SDN 中的低速率 DDoS 攻击,但这一领域仍需进一步深入探索。

5)缺乏用于训练的 SDN 特定数据集。在利用非 SDN 特定数据集训练机器学习与深度学习驱动的入侵检测方法时,通常面临着一个显著的兼容性问题。这主要是因为 SDN 架构的独特性和新颖性要求攻击向量需量身定制,而现有的公开数据集(如 KDD99、NSL-KDD、UNSW-NB15 等)虽广泛应用,但其包含的攻击模式并不完全贴合 SDN 环境,导致 SDN 在实际应用中出现了高误报率。因此,GAN 作为一种创新的数据生成技术,可以用作改善数据集质量与多样性的潜在途径[37]。然而,当前基于 GAN 自收集的合成网络流量数据在实时性和真实性方面仍存在不足的情况,无法完全模拟真实网络环境下的复杂多变情况。所以,为了推动入侵检测方法在 SDN 环境中的高效、准确应用,我们迫切需要研发一套针对 SDN 特性定制的公共数据集。这套数据集应确保数据的一致性与精确性,覆盖多样化的攻击场景与最新威胁模式,有效支撑 SDN 的持续优化与升级,来应对不断演变的网络安全挑战。

6)应用层的防御方法较少。强化 SDN 应用层的安全防护体系是当前亟须关注的领域。目前,网络攻击检测策略主要聚焦于 SDN 的控制层与数据层,而应用层的安全防护往往被忽视,这构成了一个显著的安全漏洞。尤其考虑到 SDN 架构的开放性与高度可配置性,其应用层缺乏严密的访问权限管理、身份认证机制以及实时异常监测能力,这使得它成为潜在的安全威胁目标。恶意用户或软件能够利用 SDN 应用层提供的丰富 API 接口,进行高频次、大规模的非法调用,不仅可能引发控制器的资源耗尽与崩溃,还可能对整个 SDN 网络架构造成连锁反应,导致服务中断或网络瘫痪[9]。因此,在未来应该重视对 SDN 应用层防御机制的研究。

综上所述,SDN 通过网络架构的解耦与抽象,简化了网络管理和配置,提高了网络灵活性和可编程性;同时也促进了网络资源的优化利用,提升了整体网络性能。但是,由于 SDN 是新型的网络架构,仍然有许多不足有待深度研究和发展。本文旨在为相关研究者探索 SDN 中的入侵检测方法做总结和阐述。确保 SDN 在面对复杂多变的网络威胁时能够稳健运行。希望研究者未来可以提出更多的方法来解决目前 SDN 的问题,为网络用户提供更加安全、可靠的网络环境。

参考文献(References)

[1] Liao H J, Lin C H R, Lin Y C, et al. Intrusion detection system: A comprehensive review[J]. Journal of Network and Computer Applications, 2013, 36(1): 16-24.

[2] Software defined networking market size, share and global market forecast to 2025[EB/OL]. (2021-02-14)[2024-01-04].

https://www.marketsandmarkets.com/.

[3] Kreutz D, Ramos F M V, Veríssimo P E, et al. Software−defined networking: A comprehensive survey[J]. Proceedings of the IEEE, 2015, 103(1): 14−76.

[4] Aburomman A A, Bin Ibne Reaz M. Survey of learning methods in intrusion detection systems[C]//Proceedings of International Conference on Advances in Electrical, Electronic and Systems Engineering (ICAEES). Piscataway, NJ: IEEE, 2016: 362−365.

[5] 陈晓帆, 黎志勇, 李宁. 基于软件定义网络的恶意网站防护系统[J]. 科技导报, 2015, 33(5): 93−99.

[6] 翟亚红, 崔峻玮. 软件定义网络安全研究进展[J]. 科技导报, 2023, 41(13): 76−88.

[7] Scott−Hayward S, Natarajan S, Sezer S. A survey of security in software defined networks[J]. IEEE Communications Surveys & Tutorials, 2016, 18(1): 623−654.

[8] Braun W, Menth M. Software−defined networking using OpenFlow: Protocols, applications and architectural design choices[J]. Future Internet, 2014, 6(2): 302−336.

[9] Hamarsheh A. An adaptive security framework for Internet of Things networks leveraging SDN and machine learning[J]. Applied Sciences, 2024, 14(11): 4530.

[10] Yungaicela−Naula N M, Vargas−Rosales C, Perez−Diaz J A. SDN−based architecture for transport and application layer DDoS attack detection by using machine and deep learning[J]. IEEE Access, 2021, 9: 108495−108512.

[11] Sheibani M, Konur S, Awan I, et al. A multi−layered defence strategy against DDoS attacks in SDN/NFV−based 5G mobile networks[J]. Electronics, 2024, 13(8): 1515.

[12] Abdi A H, Audah L, Salh A, et al. Security control and data planes of SDN: A comprehensive review of traditional, AI, and MTD approaches to security solutions[J]. IEEE Access, 2024, 12: 69941−69980.

[13] Hauser F, Schmidt M, Häberle M, et al. P4−MACsec: Dynamic topology monitoring and data layer protection with MACsec in P4−based SDN[J]. IEEE Access, 2020, 8: 58845−58858.

[14] Abdulkarem H S, Dawod A. DDoS attack detection and mitigation at SDN data plane layer[C]//Proceedings of 2nd Global Power, Energy and Communication Conference (GPECOM). Piscataway, NJ: IEEE, 2020: 322−326.

[15] 李道全, 杨乾乾, 鲁晓夫. 基于决策树的SDN网络入侵分类检测模型[J]. 计算机工程与设计, 2022, 43(8): 2146−2152.

[16] Jeba Praba J, Sridaran R. An SDN−based decision tree detection (DTD) model for detecting DDoS attacks in cloud environment[J]. International Journal of Advanced Computer Science and Applications, 2022, 13(7): 23−40.

[17] Janabi A H, Kanakis T, Johnson M. Overhead reduction technique for software−defined network based intrusion detection systems[J]. IEEE Access, 1851, 10: 66481−66491.

[18] 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.

[19] Madathi M, Harini R, Monikaa R, et al. Detection of DDoS attack in SDN environment using KNN algorithm[J]. International Journal of Research and Analytical Reviews, 2022, 9(2): 252−257.

[20] Qian H Z, Cai L L. Improved K−means−based solution for detecting DDoS attacks in SDN[J]. Physical Communication, 2024, 64: 102318.

[21] Xu Y H, Sun H T, Xiang F, et al. Efficient DDoS detection based on K−FKNN in software defined networks[J]. IEEE Access, 2019, 7: 160536−160545.

[22] Sahoo K S, Tripathy B K, Naik K, et al. An evolutionary SVM model for DDOS attack detection in software defined networks[J]. IEEE Access, 2020, 8: 132502−132513.

[23] Sudar K M, Beulah M, Deepalakshmi P, et al. Detection of Distributed Denial of Service Attacks in SDN using Machine learning techniques[C]//Proceedings of International Conference on Computer Communication and Informatics (ICCCI). Piscataway, NJ: IEEE, 2021: 1−5.

[24] Vetriselvi V, Shruti P S, Abraham S. Two−level intrusion detection system in SDN using machine learning[M]// Lecture Notes in Electrical Engineering. Singapore: Springer Singapore, 2018: 449−461.

[25] 胡睿, 徐芹宝, 王昌达. SDN中一种基于机器学习的DDoS入侵检测与防御方法[J]. 计算机与数字工程, 2023, 51(7): 1590−1596.

[26] Singh A, Kaur H, Kaur N. A novel DDoS detection and mitigation technique using hybrid machine learning model and redirect illegitimate traffic in SDN network[J]. Cluster Computing, 2024, 27(3): 3537−3557.

[27] Arthi R, Krishnaveni S, Zeadally S. An intelligent SDN−IoT enabled intrusion detection system for healthcare systems using a hybrid deep learning and machine learning approach[J]. China Communications, 2024, 21(10): 1−21.

[28] Satheesh N, Rathnamma M V, Rajeshkumar G, et al. Flow−based anomaly intrusion detection using machine

learning model with software defined networking for OpenFlow network[J]. Microprocessors and Microsystems, 2020, 79: 103285.

[29] Santos−Neto M J, Bordim J L, Alchieri E A P, et al. DDoS attack detection in SDN: Enhancing entropy−based detection with machine learning[J]. Concurrency and Computation: Practice and Experience, 2024, 36(11): e8021.

[30] Makuvaza A, Jat D S, Gamundani A M. Deep neural network (DNN) solution for real−time detection of distributed denial of service (DDoS) attacks in software defined networks (SDNs)[J]. SN Computer Science, 2021, 2(2): 107.

[31] Al Razib M, Javeed D, Khan M T, et al. Cyber threats detection in smart environments using SDN−enabled DNN−LSTM hybrid framework[J]. IEEE Access, 2022, 10: 53015−53026.

[32] Albahar M. Recurrent neural network model based on a new regularization technique for real−time intrusion detection in SDN environments[J]. Security and Communication Networks, 2019, 2019: 8939041.

[33] Ravi V, Chaganti R, Alazab M. Deep learning feature fusion approach for an intrusion detection system in SDN−based IoT networks[J]. IEEE Internet of Things Magazine, 2022, 5(2): 24−29.

[34] ElSayed M S, Le−Khac N A, Ali Albahar M, et al. A novel hybrid model for intrusion detection systems in SDNs based on CNN and a new regularization technique[J]. Journal of Network and Computer Applications, 2021, 191: 103160.

[35] Lee S. AE−NIDS: Automated evolving SDN−based network intrusion detection system[EB/OL]. [2023−02−02]. https://2020.eurosys.org/wp−content/uploads/2020/04/eurosys20posters−final35−abstract.pdf.

[36] Yao R Z, Wang N, Liu Z H, et al. Intrusion detection system in the smart distribution network: A feature engineering based AE−LightGBM approach[J]. Energy Reports, 2021, 7: 353−361.

[37] Ezeh D A, de Oliveira J. An SDN controller−based framework for anomaly detection using a GAN ensemble algorithm[J]. Infocommunications Journal, 2023, 15(2): 29−36.

[38] Khekare G, Kumar K P, Prasanthi K N, et al. Optimizing network security and performance through the integration of hybrid GAN−RNN models in SDN−based access control and traffic engineering[J]. International Journal of Advanced Computer Science and Applications, 2023, 14(12): 117−128.

[39] 吕星璇, 韩俐. SDN环境下基于PCA−DNN的扫描攻击检测模型研究[J]. 天津理工大学学报, 2022, 38(1): 43−48.

[40] Alhilo A M J, Koyuncu H. Enhancing SDN anomaly detection: A hybrid deep learning model with SCA−TSO optimization[J]. International Journal of Advanced Computer Science and Applications, 2024, 15(5): 98−107.

[41] Chen J, Cui M. Multi−class intrusion detection system in SDN based on hybrid LSTM model[M]//Communications in Computer and Information Science. Singapore: Springer Nature Singapore, 2024: 99−111.

[42] Sri vidhya G, Nagarajan R. A novel bidirectional LSTM model for network intrusion detection in SDN−IoT network[J]. Computing, 2024, 106(8): 2613−2642.

[43] Javeed D, Gao T H, Khan M T. SDN−enabled hybrid DL−driven framework for the detection of emerging cyber threats in IoT[J]. Electronics, 2021, 10(8): 918.

[44] Malik J, Akhunzada A, Bibi I, et al. Hybrid deep learning: An efficient reconnaissance and surveillance detection mechanism in SDN[J]. IEEE Access, 2020, 8: 134695−134706.

[45] Wang H M, Li W. DDosTC: A transformer−based network attack detection hybrid mechanism in SDN[J]. Sensors, 2021, 21(15): 5047.

[46] Goud K S, Rao G S. Towards an efficient DDoS attack detection in SDN: An approach with CNN−GRU fusion[C]// Proceedings of Fourth International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT). Piscataway, NJ: IEEE, 2024: 1−10.

[47] Lee T H, Chang L H, Syu C W. Deep learning enabled intrusion detection and prevention system over SDN networks [C]//Proceedings of IEEE International Conference on Communications Workshops (ICC Workshops). Piscataway, NJ: IEEE, 2020: 1−6.

[48] Chen L, Wang Z H, Huo R, et al. An adversarial DBN−LSTM method for detecting and defending against DDoS attacks in SDN environments[J]. Algorithms, 2023, 16(4): 197.

[49] Zhang Y L, Wu X M, Dong H M. TIBS: A deep−learning model for network intrusion detection for SDN environments[C]//Proceedings of 9th International Conference on Computer and Communication Systems (ICCCS). Piscataway, NJ: IEEE, 2024: 419−426.

[50] Clifton J, Laber E. Q−learning: Theory and applications[J]. Annual Review of Statistics and Its Application, 2020, 7:

279−301.

[51] Nguyen H H, Nguyen T G, Hoang D T, et al. CARS: Dynamic cyber−attack reaction in SDN−based networks with Q−learning[C]//Proceedings of International Conference on Advanced Technologies for Communications (ATC). Piscataway, NJ: IEEE, 2021: 156−161.

[52] Phan T V, Bauschert T. DeepAir: Deep reinforcement learning for adaptive intrusion response in software−defined networks[J]. IEEE Transactions on Network and Service Management, 2022, 19(3): 2207−2218.

[53] Arif F, Khan N A, et al. DQQS: Deep reinforcement learning−based technique for enhancing security and performance in SDN−IoT environments[J]. IEEE Access, 2024, 12: 60568−60587.

[54] Mnih V, Kavukcuoglu K, Silver D, et al. Human−level control through deep reinforcement learning[J]. Nature, 2015, 518(7540): 529−533.

[55] Phan T V, Nguyen T G, Dao N N, et al. DeepGuard: Efficient anomaly detection in SDN with fine−grained traffic flow monitoring[J]. IEEE Transactions on Network and Service Management, 2020, 17(3): 1349−1362.

[56] Schulman J, Wolski F, Dhariwal P, et al. Proximal policy optimization algorithms[EB/OL]. [2024−01−05]. https://arxiv.org/abs/1707.06347v2.

[57] Shen J H, Zhang T, Zhang B C, et al. PPO−RM: Proximal policy optimization based route mutation for multimedia services[C]//Proceedings of International Wireless Communications and Mobile Computing (IWCMC). Piscataway, NJ: IEEE, 2021: 35−40.

[58] Zolotukhin M, Kumar S, Hämäläinen T. Reinforcement learning for attack mitigation in SDN−enabled networks [C]//Proceedings of 6th IEEE Conference on Network Softwarization (NetSoft). Piscataway, NJ: IEEE, 2020: 282−286.

[59] Li M, Deng S X, Zhou H C, et al. A path selection scheme for detecting malicious behavior based on deep reinforcement learning in SDN/NFV−Enabled network[J]. Computer Networks, 2023, 236: 110034.

[60] Allakany A, Yadav G, Paul K, et al. Detection and mitigation of LFA attack in SDN−iot network[C]//Web, artificial intelligence and network applications: Proceedings of the workshops of the 34th international conference on advanced information networking and applications(WAINA−2020). Cham: Springer International Publishing, 2020: 1087−1096.

[61] Wang J S, Liu Y, Zhang W T, et al. ReLFA: Resist link flooding attacks *via* renyi entropy and deep reinforcement learning in SDN−IoT[J]. China Communications, 2022, 19(7): 157−171.

[62] Sampaio L S R, Faustini P H A, Silva A S, et al. Using NFV and reinforcement learning for anomalies detection and mitigation in SDN[C]//Proceedings of IEEE Symposium on Computers and Communications (ISCC). Piscataway, NJ: IEEE, 2018: 432−437.

[63] Kim S, Yoon S, Lim H. Deep reinforcement learning−based traffic sampling for multiple traffic analyzers on software−defined networks[J]. IEEE Access, 2021, 9: 47815−47827.

[64] Dake D K, Gadze J D, Klogo G S, et al. Multi−agent reinforcement learning framework in SDN−IoT for transient load detection and prevention[J]. Technologies, 2021, 9(3): 44.

[65] Mohanad M, et al. Intrusion detection in software−defined networks: Leveraging deep reinforcement learning with graph convolutional networks for resilient infrastructure[J]. Fusion: Practice and Applications, 2024, 15(1): 78−87.

[66] Paidipati K K, Kurangi C, Uthayakumar J, et al. Ensemble of deep reinforcement learning with optimization model for DDoS attack detection and classification in cloud based software defined networks[J]. Multimedia Tools and Applications, 2024, 83(11): 32367−32385.

[67] Dey S K, Uddin M R, Rahman M M. Performance analysis of SDN−based intrusion detection model with feature selection approach[M]//Uddin M S, Bansal J C, eds. Algorithms for Intelligent Systems. Singapore: Springer Nature Singapore, 2019: 483−494.

[68] Yadav A, Kori A S, G N D, et al. A hybrid approach for detection of DDoS attacks using entropy and machine learning in software defined networks[C]//Proceedings of 12th International Conference on Computing Communication and Networking Technologies (ICCCNT). Piscataway, NJ: IEEE, 2021: 1−7.

[69] Mohammad H M, Abdullah A A. DDoS attack mitigation using entropy in SDN−IoT environment[C]//Proceedings of AIP Conference Proceedings", "AL−Kadhum 2ND International Conference on Modern Applications of Information and Communication Technology. Baghdad: AIP Publishing, 2023: 56−67.

[70] 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.

[71] Shohani R B, Mostafavi S, Hakami V. A statistical model for early detection of DDoS attacks on random targets in SDN[J]. Wireless Personal Communications, 2021, 120(1): 379−400.

[72] Fan C, Kaliyamurthy N M, Chen S, et al. Detection of DDoS attacks in software defined networking using entropy[J]. Applied Sciences, 2021, 12(1): 370.

[73] Niknami N, Wu J. Entropy−KL−ML: Enhancing the entropy−KL−based anomaly detection on software−defined networks [J]. IEEE Transactions on Network Science and Engineering, 2022, 9(6): 4458−4467.

[74] Liu Y, Zhi T, Shen M, et al. Software−defined DDoS detection with information entropy analysis and optimized deep learning[J]. Future Generation Computer Systems, 2022, 129: 99−114.

[75] Aladaileh M, Anbar M, Hasbullah I H, et al. Entropy−based approach to detect DDoS attacks on software defined networking controller[J]. Computers, Materials & Continua, 2021, 69(1): 373−391.

[76] Ujjan R M, Pervez Z, Dahal K, et al. Entropy based features distribution for anti−DDoS model in SDN[J]. Sustainability, 2021, 13(3): 1522.

[77] Ladigatti A, Merawade V, Jain S, et al. Mitigation of DDoS attacks in SDN using access control list, entropy and puzzle−based mechanisms[C]//Proceedings of International Conference on Applied Intelligence and Sustainable Computing (ICAISC). Piscataway, NJ: IEEE, 2023: 1−8.

[78] Tian Q W, Miyata S. A DDoS attack detection method using conditional entropy based on SDN traffic[J]. IoT, 2023, 4(2): 95−111.

[79] Ahalawat A, Babu K S, Turuk A K, et al. A low−rate DDoS detection and mitigation for SDN using Renyi Entropy with Packet Drop[J]. Journal of Information Security and Applications, 2022, 68: 103212.

[80] Mhamdi L, Isa M M. Securing SDN: Hybrid autoencoder−random forest for intrusion detection and attack mitigation [J]. Journal of Network and Computer Applications, 2024, 225: 103868.

[81] Hassan A I, El Reheem E A, Guirguis S K. An entropy and machine learning based approach for DDoS attacks detection in software defined networks[J]. Scientific Reports, 2024, 14(1): 18159.

[82] 肖建平, 龙春, 赵静, 等. 基于深度学习的网络入侵检测研究综述[J]. 数据与计算发展前沿, 2021, 3(3): 59−74.

[83] Bawany N Z, Shamsi J A, Salah K. DDoS attack detection and mitigation using SDN: Methods, practices, and solutions[J]. Arabian Journal for Science and Engineering, 2017, 42(2): 425−441.

[84] Akyildiz I F, Lee A, Wang P, et al. Research challenges for traffic engineering in software defined networks[J]. IEEE Network, 2016, 30(3): 52−58.

[85] Santos da Silva A, Wickboldt J A, Granville L Z, et al. ATLANTIC: A framework for anomaly traffic detection, classification, and mitigation in SDN[C]//Proceedings of NOMS 2016 − 2016 IEEE/IFIP Network Operations and Management Symposium. Piscataway, NJ: IEEE, 2016: 27−35.

[86] Tuan N N, Hung P H, Nghia N D, et al. A DDoS attack mitigation scheme in ISP networks using machine learning based on SDN[J]. Electronics, 2020, 9(3): 413.

[87] Pérez−Díaz J A, Valdovinos I A, Choo K K R, et al. A flexible SDN−based architecture for identifying and mitigating low−rate DDoS attacks using machine learning[J]. IEEE Access, 2020, 8: 155859−155872.

[88] 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.

[89] Zhou L, Liao M C, Yuan C, et al. Low−rate DDoS attack detection using expectation of packet size[J]. Security and Communication Networks, 2017, 2017: 3691629.

[90] Cui Y H, Qian Q, Guo C, et al. Towards DDoS detection mechanisms in software−defined networking[J]. Journal of Network and Computer Applications, 2021, 190: 103156.

[91] Phan T V, Park M. Efficient distributed denial−of−service attack defense in SDN−based cloud[J]. IEEE Access, 2019, 7: 18701−18714.

[92] Wu Z J, Xu Q, Wang J J, et al. Low−rate DDoS attack detection based on factorization machine in software defined network[J]. IEEE Access, 2020, 8: 17404−17418.

Research progress of intrusion detection methods in SDN

LIU Rui[1], WANG Haifeng[1*], ZHENG Chengwei[1], WU Wenhong[1], NIU Hengmao[2]

1. College of Information Engineering, Inner Mongolia University of Technology, Hohhot 010080, China
2. Inner Mongolia Vocational and Technical College of Architecture, School of Architectural Engineering and Surveying and Mapping, Hohhot 010020, China

Abstract Intrusion detection, as a key security protection method of software defined networks (SDN) architecture, can effectively ensure the secure and stable operation of SDN. By summarizing intrusion detection methods based on machine learning, deep learning, reinforcement learning and information entropy, this paper summarizes and analyzes the existing problems in SDN environment and points out future research directions, providing reference ideas for relevant researchers.

Keywords software−defined network; intrusion detection; machine learning; deep learning; reinforcement learning; information entropy

（责任编辑 王微）