基于深度学习的软件定义网络异常检测方法

车博山　田元元　薛建彬　侯邦旺　王　强
北方自动控制技术研究所　山西　太原　030006

摘　要：在数字化浪潮推动下，软件定义网络（SDN）凭借其灵活性与可编程性，成为现代网络架构的关键支撑。本文聚焦于基于深度学习的软件定义网络异常检测方法。首先阐述软件定义网络与深度学习技术基础，包括软件定义网络的概念及深度学习技术原理。接着详细介绍基于深度学习的软件定义网络异常检测模型构建过程，涵盖数据采集与预处理、特征工程、模型选择与训练以及评估优化。最后探讨多种深度学习在软件定义网络异常检测中的具体方法，如基于流量分析、控制器行为分析、融合多源数据以及基于深度强化学习的自适应异常检测方法，旨在为软件定义网络异常检测提供有效方案。

关键词：基于深度学习；软件定义；网络异常；检测方法

引言：随着网络规模不断扩大和复杂度日益提升，软件定义网络（SDN）凭借其灵活性与可编程性得到广泛应用。然而，SDN也面临着诸多安全威胁，异常检测成为保障其安全稳定运行的关键环节。深度学习作为人工智能领域的核心技术，具有强大的数据特征提取和模式识别能力，为解决SDN异常检测难题提供了新思路。本文旨在研究基于深度学习的软件定义网络异常检测方法，通过构建检测模型和探索多种检测方法，提高异常检测的准确性和效率，以应对不断变化的网络攻击，保障软件定义网络的安全可靠运行。

1 软件定义网络与深度学习技术基础

1.1 软件定义网络概述

软件定义网络（SDN）是一种新型网络架构，它将网络的控制平面与数据平面分离。控制平面负责网络的整体管理和策略制定，由集中的控制器实现，可对网络进行全局视图下的灵活编程与配置；数据平面则专注于数据包的转发，依据控制平面下发的规则处理流量。这种架构打破了传统网络设备功能紧耦合的局限，使网络更具灵活性和可管理性。它支持快速部署新业务、实现流量灵活调度，还能简化网络运维。凭借这些优势，SDN在数据中心、企业网络等众多场景得到广泛应用，成为推动网络创新发展的重要力量。

1.2 深度学习技术原理

深度学习是机器学习的一个分支，基于人工神经网络构建。其核心原理是通过构建多层非线性变换的神经网络模型，自动从海量数据中学习复杂的特征和模式。网络包含输入层、隐藏层和输出层，数据从输入层进入，经隐藏层逐层抽象和转换，最终在输出层得到结果。训练过程中，利用反向传播算法，根据输出结果与真实标签的误差，从输出层向输入层逐层调整网络参数，使模型不断优化。深度学习凭借强大的特征提取和表示能力，在图像识别、语音处理、自然语言处理等众多领域取得了卓越成就[1]。

2 基于深度学习的软件定义网络异常检测模型构建

2.1 数据采集与预处理

数据采集是构建异常检测模型的基础。在软件定义网络环境中，可从控制器、交换机等设备采集多维度数据，如流量统计信息（包括数据包大小、传输速率等）、网络拓扑变化记录、控制器指令日志等。为保证数据的完整性和准确性，需采用高效可靠的采集工具，并合理设置采集频率。采集到的原始数据往往存在噪声、缺失值和重复值等问题，影响模型性能，因此要进行预处理。对于噪声数据，可采用平滑滤波方法去除；缺失值可通过插值法或直接删除缺失样本处理；重复值则予以剔除。此外，还需对数据进行标准化或归一化处理，将不同量纲的数据映射到统一范围，避免因数据尺度差异导致模型训练偏差，为后续特征工程和模型训练提供高质量数据。

2.2 特征工程

特征工程旨在从原始数据中提取有价值的特征，以更好地表示网络行为和异常模式。在软件定义网络异常检测中，可从流量特征、时间特征和拓扑特征等多方面入手。流量特征包括平均流量、流量突发程度等，能反映网络的负载情况；时间特征如流量随时间的变化趋势、周期性等，有助于发现基于时间的异常行为；拓扑特征则关注网络结构的动态变化，如节点连接状态的改变。提取特征后，还需进行特征选择，去除冗余和不相关特征，降低数据维度，提高模型训练效率和泛化能

力。常用特征选择方法有过滤法、包裹法和嵌入法等，可根据数据特点和模型需求选择合适的方法，构建出能够有效区分正常和异常行为的特征集合。

2.3 深度学习模型选择与训练

选择合适的深度学习模型对于异常检测效果至关重要。常见的可用于软件定义网络异常检测的模型有自编码器（AE）、卷积神经网络（CNN）和循环神经网络（RNN）及其变体（如LSTM、GRU）。自编码器通过无监督学习学习数据的正常表示，将重构误差作为异常得分；CNN擅长处理具有局部相关性的数据，可用于分析网络流量的空间特征；RNN及其变体适合处理序列数据，能有效捕捉网络行为的时间依赖性。确定模型后，使用预处理好的数据集进行训练。将数据划分为训练集、验证集和测试集，采用合适的优化算法（如随机梯度下降、Adam等）调整模型参数，使模型在训练集上不断学习数据的内在规律，同时利用验证集监控模型性能，防止过拟合，确保模型具有良好的泛化能力。

2.4 模型评估与优化

模型评估是检验异常检测模型性能的关键环节。常用的评估指标有准确率、召回率、F1值、误报率和漏报率等。准确率反映模型正确分类的比例；召回率衡量模型检测出真实异常的能力；F1值是准确率和召回率的综合指标；误报率指将正常行为误判为异常的比例；漏报率则是未检测出真实异常的比例。根据评估结果对模型进行优化。若模型存在过拟合问题，可采用正则化方法、增加训练数据或早停法等；若性能不佳，可调整模型结构，如增加或减少网络层数、神经元数量；也可尝试不同的超参数组合，通过网格搜索或随机搜索等方法寻找最优参数，提升模型的异常检测性能，使其在实际软件定义网络环境中能够有效准确地识别异常行为[2]。

3 深度学习的软件定义网络异常检测的方法

3.1 基于流量分析的异常检测方法

（1）流量特征提取。在软件定义网络中，流量蕴含着丰富的网络行为信息，首先从采集到的原始流量数据里，提取基础特征，如数据包的大小、数量、传输速率，能直观反映流量的规模与活跃程度。进一步挖掘高级特征，像流量的时间分布特征，包括不同时间段流量的波动情况，可捕捉基于时间的异常模式；还有流量的空间分布特征，如不同节点间流量的流向和流量占比，能发现异常的流量路径。通过综合多维度特征，构建全面且能精准刻画网络流量状态的特征集合，为后续深度学习模型提供有效的输入数据。（2）深度学习模型应用。选用合适的深度学习模型对提取的流量特征进行分析是关键，卷积神经网络（CNN）可有效处理具有局部相关性的流量特征，通过卷积层自动提取流量中的局部模式，池化层降低数据维度，最后全连接层进行分类判断，识别正常与异常流量。循环神经网络（RNN）及其变体（如LSTM、GRU）适合处理流量序列数据，能捕捉流量随时间的变化趋势和长期依赖关系，准确检测出基于时间序列的异常行为。根据流量数据特点和检测需求，灵活选择或组合这些模型，提高异常检测的准确性。（3）实验验证与优化。为验证基于流量分析的异常检测方法的有效性，需搭建实验环境，使用真实的软件定义网络流量数据进行测试。将数据集划分为训练集、验证集和测试集，用训练集训练深度学习模型，验证集调整模型参数，测试集评估模型性能。根据评估指标，如准确率、召回率、F1值等，分析模型的检测效果。若模型性能不理想，针对问题优化模型，如调整网络结构、增加训练数据、优化超参数等。同时，对比不同模型和算法的检测结果，选择最优方案，不断提升基于流量分析的异常检测能力。

3.2 基于控制器行为分析的异常检测方法

（1）控制器行为数据收集。在软件定义网络里，控制器是核心控制枢纽，其行为数据蕴含着网络运行的关键信息。可通过在控制器内部植入日志记录模块，详细记录其发出的各类指令，如流表下发、拓扑更新等指令的时间、类型、目标设备等。同时，利用网络监控工具，从外部收集控制器与交换机之间的交互消息，包括请求-响应消息的频率、内容等。此外，还能采集控制器的系统资源使用情况，如CPU占用率、内存使用量等。（2）行为特征建模。收集到控制器行为数据后，需构建合适的行为特征模型。先对数据进行预处理，去除噪声和异常值，统一数据格式。接着，运用统计分析方法，提取行为的基本特征，如指令的平均发出频率、资源使用的平均水平等。进一步采用机器学习中的聚类算法，对相似的行为模式进行分类，找出正常行为的典型簇。还可以利用时间序列分析方法，建立控制器行为随时间变化的动态模型，捕捉行为的周期性和趋势性特征。（3）实时监测与预警。基于构建好的行为特征模型，对控制器行为进行实时监测。设置专门的监测模块，持续收集控制器的实时行为数据，并按照预定义的特征提取方法，快速计算出当前行为的特征参数。将这些参数与行为特征模型中的正常范围进行实时比对，若发现某些参数超出正常阈值或行为模式与典型簇不匹配，则判定为异常行为。一旦检测到异常，立即触发预警机制，通过短信、邮件等方式及时通知网络管理员。

3.3 融合多源数据的异常检测方法

（1）多源数据融合策略。在软件定义网络中，多源数据涵盖流量数据、控制器行为数据、拓扑结构数据等。为有效融合这些数据，可采用分层融合策略。在数据层，先对不同来源的数据进行清洗和预处理，统一数据格式与时间戳，确保数据质量与一致性。特征层融合时，从各类数据中提取关键特征，如从流量数据提取流量大小、方向特征，从控制器行为数据提取指令频率特征，再将这些特征进行组合与筛选，去除冗余信息。（2）深度学习模型设计。设计融合多源数据的深度学习模型是关键。可构建一个多输入的神经网络模型，不同输入分支分别处理不同类型的数据。例如，一个分支采用卷积神经网络（CNN）处理具有空间特征的拓扑结构数据，提取拓扑中的局部模式；另一个分支使用循环神经网络（RNN）及其变体处理时间序列性质的流量数据和控制器行为数据，捕捉数据的时间依赖关系。然后，将各分支提取的特征进行拼接，通过全连接层进行综合分析与分类，判断是否存在异常。（3）数据关联与挖掘。融合多源数据后，需深入挖掘数据间的关联关系。利用关联规则挖掘算法，找出不同数据特征之间的频繁模式与关联规则。例如，发现当控制器发出特定指令时，某些网络节点的流量会出现规律性变化，这种关联规则有助于理解网络正常运行时的行为模式。同时，采用聚类分析方法，将相似的数据样本聚集在一起，识别出正常行为簇与异常行为簇。通过分析异常行为簇中数据的特点，找出导致异常的潜在因素。

3.4 基于深度强化学习的自适应异常检测方法

（1）强化学习框架构建。在软件定义网络异常检测场景中构建强化学习框架，将检测系统视为智能体，网络环境作为外部世界。定义状态空间，涵盖流量特征、控制器行为指标、拓扑变化等网络实时状态信息。动作空间设定为检测策略调整动作，如改变检测阈值、切换检测模型等。奖励函数根据检测效果设计，正确检测异常给予正奖励，误报或漏报给予负奖励，引导智能体学习最优检测策略，以适应动态变化的网络环境。（2）深度强化学习算法应用。选用合适的深度强化学习算法，如深度Q网络（DQN），利用神经网络逼近Q函数，处理高维状态输入。通过经验回放机制，打破数据相关性，提高学习效率。还有近端策略优化（PPO）算法，能稳定地优化策略，避免策略更新幅度过大。将网络状态输入算法模型，模型输出动作决策，智能体执行动作与环境交互，根据反馈的奖励不断调整策略参数，提升异常检测的准确性和适应性。（3）在线学习与更新。深度强化学习模型需具备在线学习能力，实时接收网络新数据。当新流量到达或网络拓扑变化时，将当前状态输入模型，获取检测动作并执行。根据执行结果获得奖励，利用新数据对模型参数进行在线更新，采用随机梯度下降等方法优化神经网络权重。通过持续在线学习，模型能及时适应网络的新特征和新攻击模式，不断调整检测策略，始终保持较高的异常检测性能，保障软件定义网络的安全稳定运行[3]。

结束语

基于深度学习的软件定义网络异常检测方法，为保障网络的安全稳定运行开辟了新路径。通过融合流量分析、控制器行为分析、多源数据融合以及深度强化学习等多种技术手段，从不同维度深入挖掘网络中的异常模式，有效提升了异常检测的准确性与适应性。尽管目前该方法在模型复杂度、实时性处理等方面仍面临挑战，但随着深度学习算法的不断优化和计算能力的持续提升，其发展前景十分广阔。

参考文献

[1]李浩.基于深度学习的网络流量入侵检测方法研究[J].电脑知识与技术,2024,20(23):96-99+110.

[2]孟玉飞.基于深度度量学习的匿名网络流量关联技术研究[D].南京信息工程大学,2024.

[3]常志华,许国辉.网络攻击检测中基于深度学习的恶意流量识别[J].网络安全技术与应用,2024,(06):43-45.