基于AI的SDN网络安全方案浅析

Analysis of AI-based SDN Network Security Solutions

李发财[1]，余思阳[1]，王向华[1]，刘　果[2]，雷鹏飞[1]（1.中国联合网络通信集团有限公司，北京 100033，2.中讯邮电咨询设计院有限公司，北京 100048）

Li Facai[1], Yu Siyang[1], Wang Xianghua[1], Liu Guo[2], Lei Pengfei[1] (1. China United Network Communications Group Co., Ltd., Beijing 100033, China; 2. China Information Technology Designing & Consulting Institute Co., Ltd., Beijing 100048, China)

摘　要：

随着SDN技术的快速发展和网络安全威胁的日益复杂，对SDN网络进行有效的安全防护变得至关重要。然而，传统的网络安全防护手段和方案，无法快速准确检测SDN网络安全隐患并快速做出响应。为了解决这一问题，提出了一种基于AI的SDN网络安全方案。该方案将SDN网络面临的主要网络安全场景进行综合分析，并结合主流AI技术和威胁情报，及时发现SDN网络面临的安全风险，以帮助企业快速有效定位SDN网络安全问题，并做出快速响应。

关键词：

软件定义网络；网络安全；AI技术；威胁情报

doi：10.12045/j.issn.1007-3043.2024.08.006

文章编号：1007-3043（2024）08-0029-05

中图分类号：TP181

文献标识码：A

开放科学（资源服务）标识码（OSID）：

Abstract：

With the rapid development of Software-Defined Networking (SDN) technology and the increasing complexity of network security threats, effective security protection for SDN networks has become crucial. However, traditional network security measures and solutions can not accurately detect SDN network security vulnerabilities and respond quickly. To address this issue, it proposes an AI-based SDN network security solution. This solution comprehensively analyzes the major network security scenarios faced by SDN networks and combines mainstream AI technologies and threat intelligence to timely identify security risks faced by SDN networks. It helps enterprises quickly and effectively pinpoint SDN network security issues and respond rapidly.

Keywords：

SDN; Network security; AI technology; Threat intelligence

引用格式：李发财，余思阳，王向华，等. 基于AI的SDN网络安全方案浅析[J]. 邮电设计技术，2024(8)：29-33.

0 引言

随着信息技术的快速发展，网络安全成为全球焦点。软件定义网络（SDN）架构[1]的广泛应用带来了新的安全问题，SDN的中央化控制提高了网络灵活性和配置效率，但集中控制和可编程性也引入了安全风险。因此，利用现代技术提升SDN安全性是技术发展的必然要求，也是网络安全的关键[2]。

收稿日期：2024-06-26

传统网络安全技术依赖定义和签名检测SDN威胁，但这些技术在应对SDN的动态性和复杂性方面存在局限，缺乏实时应对新兴威胁的敏捷性和适应性。

AI技术通过分析大量网络、配置和安全数据进行预训练，结合反馈学习和加速推理，形成成熟的专有模型。这种模型能够识别SDN中的安全风险和异常，包括未知威胁。AI的自适应学习能力使其成为检测SDN环境中复杂和不断演变威胁的理想解决方案。

总之，AI技术为SDN安全性的提升提供了新的可能性，有助于应对网络安全的挑战，保障网络环境的

稳定和安全。

1 SDN安全挑战

SDN技术通过将网络控制平面与数据转发平面分离，实现了网络管理和控制的集中化和自动化，改变了传统网络的工作方式，通过实时动态灵活的控制，提高了网络的可伸缩性和可扩展性，作为一种革命性的网络架构，其面临的安全挑战更加复杂[3]。

1.1 网络攻击

SDN的开放性和集中控制特性，虽然带来了管理上的便利，但也使其成为攻击者的重点目标。网络攻击主要分为以下几类。

a）拒绝服务攻击（DoS/DDoS）[4]。通过大量的请求淹没网络，影响SDN控制器的处理能力，从而使正常的网络服务无法进行。

b）中间人攻击。攻击者在通信双方之间截取或篡改信息，利用SDN环境的动态性进行攻击。

c）侧信道攻击。通过分析网络流量模式，攻击者可以推断出网络中的敏感操作或数据。

这些攻击不仅直接影响网络的稳定性和可用性，还可能导致重要数据的泄露，进一步损害企业的信誉和经济利益。

1.2 网络故障

在SDN环境中，及时识别和处理网络故障是保障网络连续性和业务稳定的关键。网络故障可能源于以下几个方面。

a）硬件故障。包括交换机、路由器等网络设备的物理故障。

b）软件缺陷。SDN控制器或其他网络管理软件出现故障或漏洞。

c）操作失当。不当的操作、策略调整可能导致网络拓扑出现问题，影响数据流的正常传输。

对这些故障的及时识别和修复，需要依赖高效的监控系统和自动化的故障响应机制。

1.3 配置错误

配置错误是SDN中常见的安全风险之一，错误的配置可能导致如下问题。

a）数据泄露。不正确的访问控制列表（ACLs）设置可能导致未授权访问。

b）服务中断。错误的流表项配置可能阻断合法流量，影响业务的连续性。

c）性能下降。不恰当的网络资源分配可能导致关键应用性能不佳。

在SDN中，配置管理的自动化和智能化显得尤为重要，以减少人为错误，提高网络的整体安全性。

2 AI在SDN网络安全中的应用场景

AI技术的应用，不仅能够有效进行网络攻击检测和防护，还能在网络故障检测与响应、配置优化与提升中发挥关键作用。

2.1 网络攻击检测和防护

AI技术为网络防御提供了动态智能的新方法。借助行为分析与推理，AI能在SDN环境中实时监控流量，迅速识别基础攻击。对于APT等高级攻击，AI通过宏观和纵深视角的联合分析，从广度和深度发现潜在威胁。AI的知识积累为攻击防护提供策略，如检测DDoS攻击的非常规访问或流量突增[5]。AI还能通过分析攻击者行为预测新攻击方式，使用决策树、SVM、随机森林等算法有效识别包括DDoS、SQL注入和XSS在内的多种攻击（见图1）。

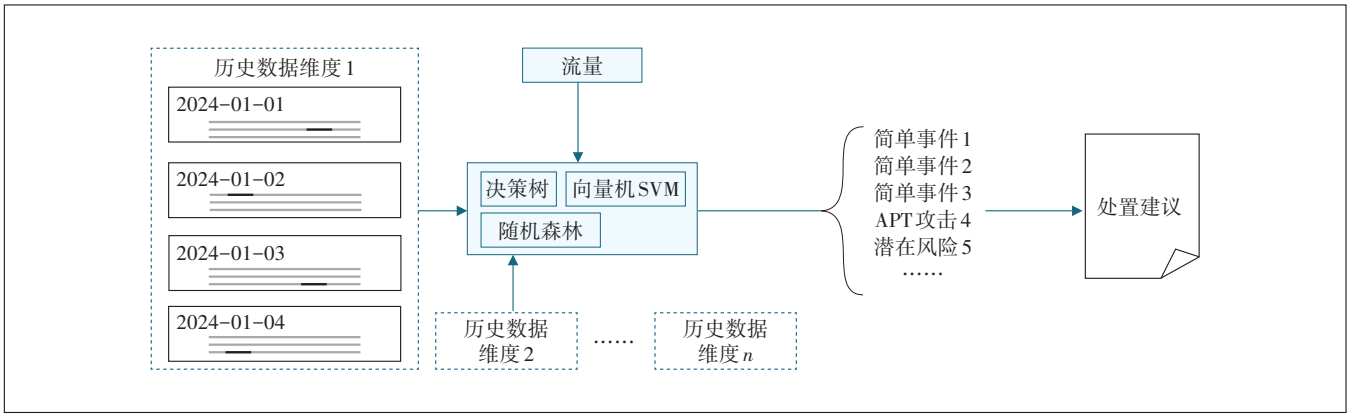

图1　AI网络安全风险识别

2.2 故障检测和响应

AI技术，特别是机器学习和深度学习，通过分析历史数据和实时流量，可以有效地识别网络中的异常行为实现对故障的早期检测。例如，深度学习用于识别复杂的网络异常模式和未知的攻击行为，一些研究通过使用卷积神经网络（CNN）分析网络流量数据，能够准确地确定异常流量的类型和来源。

如图2所示，使用的CNN模型是一系列3层结构，每个3层结构通过一个可区分的函数（激活函数）将一个激活量转换为另一个激活量。在该模型中，设计了一个具有2个卷积层和3个全连接层的CNN架构。在该CNN架构中不使用池化层。

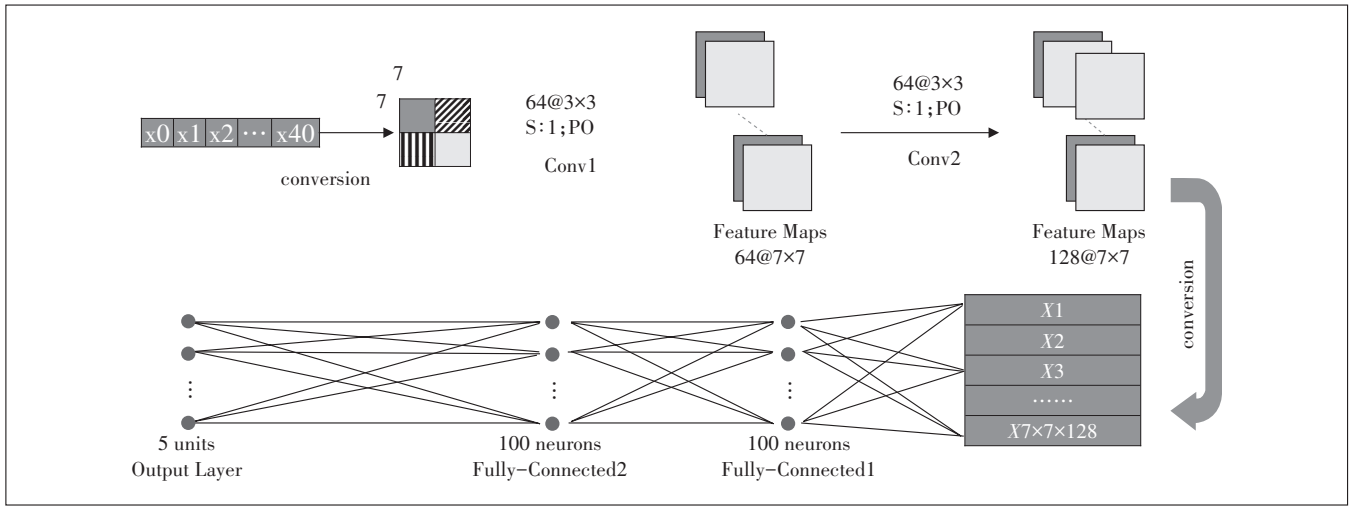

图2　CNN模型结构

如图3所示，利用上述模型能够对流量类型和来源进行识别，同时对流量特征进行采集和监控，快速发现异常流量，使得在应用场景中能够快速定位发现故障，并迅速告警启动随后的应急预案。

此外，利用循环神经网络（RNN）对时间序列进行分析，可以预测网络行为的长期趋势，从而实现自动化响应措施，比如动态调整防火墙规则或隔离受影响的网络段。这些AI模型能在数秒内确定问题的源头，并自动执行修复程序或通知网络管理员进行干预。这种快速的响应减少了网络停机时间，保障了业务连续性和数据安全。

2.3 SDN配置优化与提升

AI技术在网络配置管理中通过实时流量分析自动调整资源分配和路由策略，形成行为基线，快速识别配置错误，提升网络效率。AI集成推动业务流程自动化和智能化，支持数据驱动决策，提高运营效率。

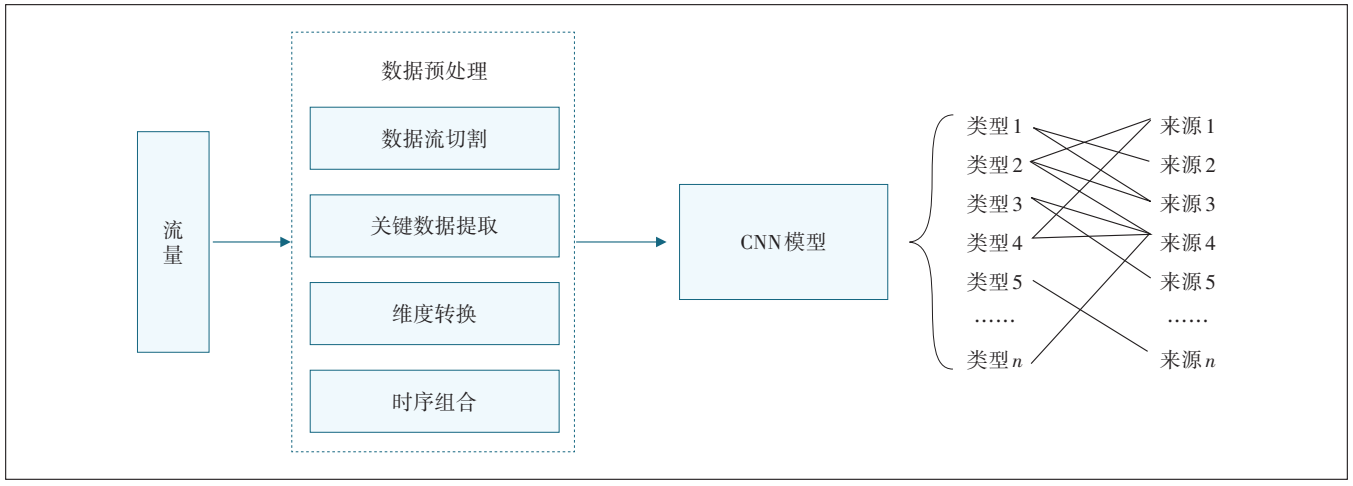

图3　CNN网络流量数据分析

它还能自动化调整网络配置，如负载均衡和故障转移，优化资源利用率和业务稳定性。强化学习技术甚至可用于动态优化数据中心配置，最小化响应时间和成本，确保关键应用连续运行。AI展现了在网络管理和业务流程优化中的强大潜力，能助力企业在技术变革中保持竞争力。

3 AI赋能SDN安全架构

AI技术在海量数据分析、动态异常检测、辅助决策等方面有着先天的优势，通过AI技术打造的安全数据基座和SDN网络及安全分析系统[6]，与SDN控制器共同形成了SDN安全架构[7]，该架构为SDN网络提供了动态灵活、响应及时、防护全面的安全能力（见图4）。

3.1 防护机制

安全数据基座利用AI实时分析网络数据，识别DDoS、中间人攻击等异常行为，并转化为威胁情报。网络流量监测设备收集流量信息，为SDN系统提供数据支持[8]。SDN系统结合AI技术，分析威胁情报和流量信息，快速发现并响应网络攻击和配置错误，驱动控制器生成控制信息。

SDN控制器的网络控制单元迅速解决网络故障和配置错误，与安全控制单元协作，动态调度网络流量。安全控制单元下发策略至安全资源池，指导各类安全设备检测和防护。安全资源池对流量进行安全检测，及时识别异常并执行防护策略。

通过这一系列流程，AI技术在SDN安全领域的应用不仅提高了网络的监测和响应能力，还加强了网络的动态调度和安全防护，确保了网络环境的稳定性和安全性。

3.2 架构优势

首先，实时采集网络流量信息，并通过AI技术进行动态分析，能够及时发现网络攻击及流量异常问题，从而及时应对，避免网络攻击对SDN的影响，提高了SDN网络安全性及业务稳定性[9]。

其次，在传统SDN控制器中，增加安全控制单元，避免安全视野盲区，全面掌握SDN安全现状，以无死角防护应对不断提高的网络攻击水平和自身安全防护需要[10]。

此外，通过安全资源池，可实现多种安全能力的按需调度与协同防护，全面提升SDN网络安全防护水平，为SDN网络安全稳定运行提供根本保障[11]。

3.3 改进方向

尽管本方案具有许多优势，但也存在一些待改进方向。首先，需进一步提升数据治理水平，通过高质量的数据输入，提高AI建模效率和效果，从而提升AI模型的分析能力。其次，研究和探索更精确和可靠的特征提取和选择方法，以捕捉影响SDN网络安全的关键因素。此外，进一步优化安全检测和防护模型，以提高SDN网络攻击、网络故障和配置错误发现的效率

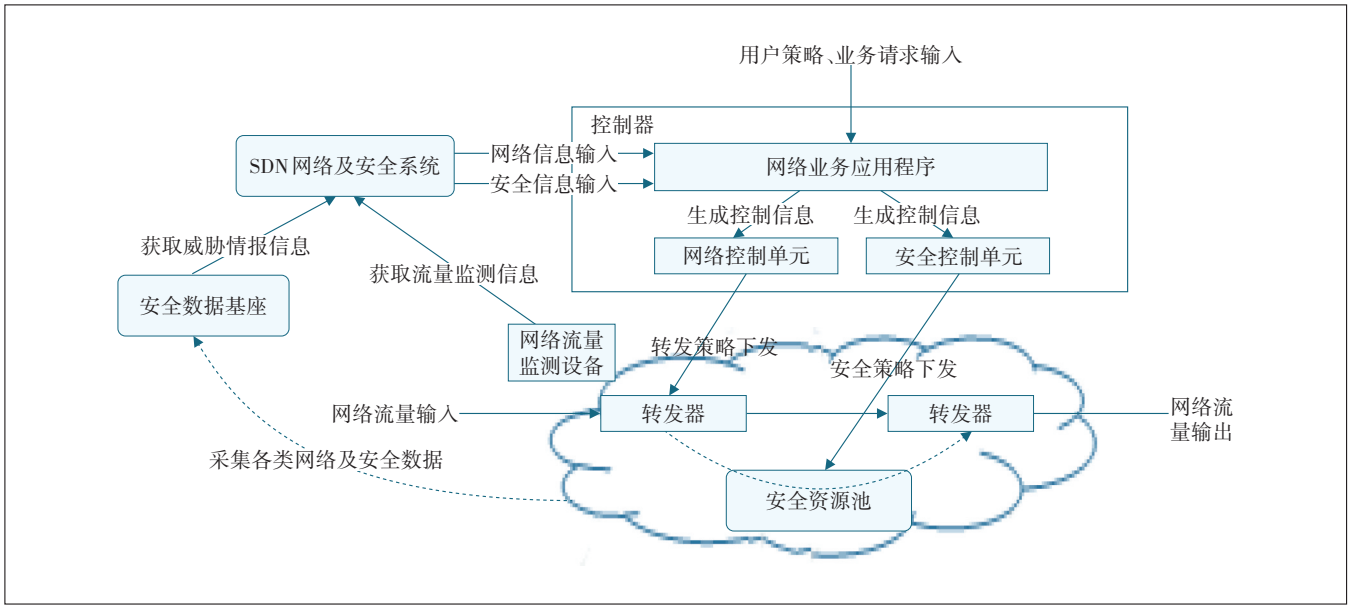

图4　AI赋能的SDN安全架构

和准确性[12]。最后，以SDN网络内生安全为目标，逐步实现SDN架构与安全的深度融合，更好地实现SDN网络安全防护体系，全面保障SDN控制器、SDN网络基础设施及相关业务系统的安全。

4 未来趋势及展望

AI技术已证明其在增强SDN网络安全和业务安全方面的独特价值[13]。通过机器学习和深度学习，AI能够实现对网络攻击的预测性防御，及时识别和响应网络故障，优化网络配置。这些应用不仅提高了网络的自动化水平，还显著提升了网络的响应速度和准确性[14]，特别是在故障检测和攻击防御方面，效果显著。

此外，AI的集成应用通过跨学科技术的整合，能够进一步增强SDN的安全性能，为业务流程的安全性和效率提供强有力的保障。

4.1 技术发展趋势

AI技术与SDN的演进将推动网络安全策略的智能化[15]。关键趋势包括：深度学习驱动的自适应学习系统，能自动调整策略以应对未知威胁；量子计算与AI结合，提升算法速度和安全性；联邦学习在SDN中应用，兼顾数据隐私和攻击检测；AI与区块链整合，通过智能合约自动化安全策略更新，增强网络交易透明度和安全性；物联网技术与AI结合，提升设备自防护能力，强化网络边缘安全。这些技术融合预示着网络环境的安全性和效率将大幅提升。

4.2 网络安全新机遇

研究将集中于AI在网络和业务安全领域的创新，旨在提高SDN的安全性和业务连续性。AI的发展为网络安全带来新机遇，推动技术革新，拓宽其在安全领域的应用。开发中的AI驱动风险评估工具将全面分析网络威胁，提供预防策略。AI技术将智能化分析和保护业务流程，在自动化企业环境中确保业务安全和效率。同时，结合AI算法的新型攻击预防工具将实时防御复杂攻击，增强网络防御。这些研究将为网络安全和业务连续性提供技术支撑，促进信息通信技术发展，确保数字化时代的稳定与安全。

4.3 未来展望

未来，AI在SDN安全领域的应用将不断深化，特别是在自适应学习、联邦学习、AI大模型等关键技术领域。随着AI技术的持续进步，它将更有效地应对日益复杂的安全威胁和业务需求。

AI的融合应用，如量子计算，将为网络带来新的速度和安全性。智能化的风险评估和攻击预防机制将加固网络和业务流的安全架构。这些进步不仅提升了SDN系统的安全性和业务连续性，也为信息通信技术的发展提供了坚实的支撑，促进了数字化时代的稳定发展。

综上所述，AI在SDN安全领域展现出巨大潜力，其影响力和创新能力预计将持续增长，引领网络安全行业迈向更高效、安全的未来。

参考文献：

[1] 孙鹏. SDN安全技术研究[J]. 中国电子科学研究院学报，2015(4)：416-420.
[2] 唐博. 略谈SDN安全需求和安全实现[J]. 信息通信，2020(1)：97-98.
[3] 牧军，李虎. 探究SDN安全防护技术[J]. 中国高新区，2017(21)：198.
[4] 何亨，黄伟，李涛，等. 基于SDS架构的多级DDoS防护机制[J]. 计算机工程与应用，2016，52(1)：81-88.
[5] 廖小群，黄华东. SDN网络DDoS泛洪攻击的被动防御措施研究[J]. 现代信息科技，2022(6)：97-99+103.
[6] 钟志琛，尚方，刘生. 基于SDN的新一代电网数据中心安全防护架构研究[J]. 电力信息与通信技术，2017，15(8)：21-25.
[7] 余竟航，陈欣，陈石，等. 基于SDN的云计算网络平台安全技术分析[J]. 无线互联科技，2022，19(24)：109-111.
[8] 王亮，马海龙，江逸茗，等. 一种基于SDP组件的SDN安全架构模型[J]. 信息工程大学学报，2022，23(4)：478-484.
[9] K. 霍夫曼. 用于在网络元件中使用的方法和装置：CN201680046998.6[P]. 2016-06-10.
[10] 刘文懋，裘晓峰，陈鹏程，等. 面向SDN环境的软件定义安全架构[J]. 计算机科学与探索，2015，9(1)：63-70.
[11] 薛乐梅. SDN网络安全策略研究[J]. 数字技术与应用，2018，36(10)：201-202.
[12] 齐宇. SDN安全研究[J]. 信息网络安全，2016(9)：69-72.
[13] 陈斌，袁莎莎，陈越. 基于SDN安全服务链的数据中心运维体系建设与实践[J]. 网络安全和信息化，2023(7)：75-78.
[14] 杨艺，蔡顺婉. SDN安全研究综述[J]. 中文科技期刊数据库(全文版)工程技术，2021(1)：105-107.
[15] 曹鑫，范国瑨，王昊辰. 基于SDN和NFV技术的网络安全架构[J]. 微型电脑应用，2022，38(1)：114-116.

作者简介：
李发财，高级工程师，硕士，主要从事网络安全产品研究、架构设计、应用实践等工作；余思阳，高级工程师，硕士，主要从事网络安全体系规划及产品应用工作；王向华，工程师，学士，主要从事网络安全产品研究、交互设计等工作；刘果，工程师，学士，主要从事网络安全技术的研究工作；雷鹏飞，工程师，硕士，主要从事网络安全技术研究、研发管理等工作。