 DOI: https://doi.org/10.12349/iser.v6i11.8108

Design of DDoS Attack Detection and Defense Mechanism in Software-Defined Networks

Qi Sun Hongyu Zhang

Beijing Institute of Space Electromechanical Research, Beijing, 100094, China

Abstract

With the continuous expansion and increasing complexity of networks, distributed denial-of-service (DDoS) attacks have emerged as a primary threat in cybersecurity. Traditional defense mechanisms, constrained by rigid architectures and passive responses, struggle to detect and mitigate attacks in real-time. Software-defined networking (SDN), leveraging centralized control, programmability, and global visibility, offers innovative approaches for DDoS detection and defense. This study analyzes the characteristics and vulnerabilities of DDoS attacks in SDN environments, proposing a collaborative detection and defense mechanism at both the control and data layers. The framework integrates traffic feature extraction, intelligent pattern recognition, and dynamic policy scheduling. Simulation results on Mininet demonstrate that this mechanism effectively reduces false positive and false negative rates while enhancing controller processing efficiency and network recovery capabilities, providing technical support for building intelligent and adaptive cybersecurity protection systems.

Keywords

software-defined network; DDoS attack; traffic detection; controller security; defense mechanism

软件定义网络中 DDoS 攻击检测与防御机制设计

孙麒 张宏宇

北京空间机电研究所，中国 · 北京 100094

摘 要

随着网络规模与复杂度不断提升，分布式拒绝服务（DDoS）攻击已成为网络安全领域的主要威胁。传统防御机制受限于结构僵化与被动响应，难以及时识别与处置攻击。软件定义网络（SDN）凭借集中控制、可编程和全局可视化优势，为DDoS检测与防御提供新思路。本文分析SDN环境下DDoS攻击的特征与脆弱性，提出基于控制层与数据层协同的检测与防御机制，融合流量特征提取、智能判别与动态策略调度。在Mininet仿真中验证结果表明，该机制能有效降低误报率与漏报率，提升控制器处理效率与网络恢复能力，为构建智能化、自适应的网络安全防护体系提供技术支撑。

关键词

软件定义网络；DDoS攻击；流量检测；控制器安全；防御机制

1 引言

DDoS 攻击通过大量分布式节点对目标服务器或网络带宽发起并发请求，使受害者无法正常提供服务，是网络空间安全治理中的顽疾。传统防御体系主要部署于固定边界或单点节点，如防火墙、入侵检测系统（IDS）与黑名单过滤等，往往面临响应滞后、难以全局感知的问题。随着云计算、物联网及 5G 网络的兴起，流量类型呈多样化趋势，DDoS 攻击的隐蔽性与复杂度进一步增强。软件定义网络以“控制与转发分离、集中控制、开放接口”为特征，使网络具备可编程性和动态调度能力，为实时检测与快速防御提供技术基础。当前研究在 DDoS 攻击识别算法、控制器防护机制以及动态防御体系构建等方面取得了一定成果，但仍存在模型泛化能力不足、控制层负载集中、策略下发延迟等问题。本文旨在系统分析 SDN 架构下 DDoS 攻击的特征传播规律，提出融合流量特征学习与策略自适应的检测与防御机制，并通过仿真验证其有效性，为 SDN 环境中的主动安全防护提供可行路径。

【作者简介】孙麒（1987–），男，中国北京人，本科，工程师，从事信息安全、计算机网络研究。

2 软件定义网络的安全架构特征与 DDoS 攻击风险分析

2.1 SDN 体系结构及其安全特征

SDN 架构由应用层、控制层与数据层组成，控制层通过南向接口（如 OpenFlow）下发策略，实现对交换机的统一管理与流量调度。集中式控制器使网络具备全局视角与灵活策略分发能力，但这种集中性同时也带来潜在安全风险。控制器一旦遭受攻击，可能导致全局策略失效、流表更新受

阻，严重影响业务连续性。与传统网络相比，SDN 的可编程特性虽然增强了可控性，却扩大了攻击面，使 DDoS 攻击从主机层面延伸至控制平面、应用接口及数据转发路径。研究表明，控制层的集中结构是攻击者重点目标，其可通过流表泛洪、控制消息淹没等手段造成资源耗尽。

2.2 SDN 环境下 DDoS 攻击的演化特征

DDoS 攻击在 SDN 环境中的表现呈现出多样化与智能化趋势。攻击者可利用控制器与交换机之间的通信机制制造虚假流量请求，通过频繁建立短生命周期流表项引发“流表耗尽”现象，导致合法流量被延迟处理。部分攻击利用南向接口协议漏洞伪造 Packet-In 消息，从而造成控制器异常负载。此外，云计算和 IoT 设备的大规模互联为僵尸网络扩散提供了便利，使攻击源更加分散、流量模式更加随机，增加了检测的复杂性。

2.3 传统防御机制的局限性

传统网络防御通常基于静态规则匹配或流量阈值检测，对动态变化的攻击流量难以及时响应。防火墙与 IDS 虽可拦截部分已知攻击，但面对复杂的多向流量和突发性攻击，其性能瓶颈明显。另一方面，传统防御部署点固定，缺乏全局协调，无法对跨域攻击进行联动防护。SDN 环境要求防御系统具备可编程、动态调度和实时感知能力，实现跨层协同与资源优化。因而，在 SDN 体系下重新设计面向控制与转发层联动的 DDoS 防御框架，是实现主动防御的重要方向。

3 SDN 中 DDoS 攻击检测模型设计与特征提取

3.1 流量特征采集与行为建模

SDN 控制器能够实时收集网络中各交换机的流量信息，为攻击检测提供丰富的数据基础。本文设计的检测模型基于流量统计特征，包括流速变化率、源 IP 分布熵、包间隔均值、控制消息频度等指标。通过分析流量在时间序列中的波动模式，构建流量行为模型，以刻画正常与异常状态之间的差异。

3.2 基于机器学习的智能检测机制

考虑到 DDoS 攻击流量呈现高维度、非线性特征，本文采用随机森林与长短期记忆网络（LSTM）组合模型。随机森林负责静态特征筛选与分类，LSTM 用于捕捉时序相关性，实现流量动态识别。模型通过训练阶段学习正常与攻击样本间的模式差异，并在在线检测阶段对实时流量进行分类判断。为了降低误报率，引入置信阈值动态调整机制，根据网络整体负载自动校正分类边界。实验表明，该混合模型在数据集上可实现 97% 以上的检测精度，并对突发攻击保持较高鲁棒性。

3.3 检测模型的系统集成与控制层部署

检测模块部署于 SDN 控制器的安全子系统中，通过北向接口与监控应用通信，实现检测结果的实时上报与策略联动。系统分为流量采集模块、特征分析模块、模型推理模块和策略反馈模块四个部分。控制器利用 REST API 接口将检测结果传递给防御模块，以实现动态流表更新。为防止控制器负载过重，系统支持多控制器协作部署，通过负载均衡机制分配检测任务，从而确保检测系统在大规模网络中的可扩展性。

4 DDoS 防御机制的动态响应与策略优化

4.1 控制层与数据层协同防御框架

本研究提出的协同防御框架以“控制层检测、数据层隔离、全局策略协同”为核心思路，旨在实现分层联动与高效响应。控制层承担全网流量的实时监测与智能分析任务，当检测模块识别到潜在 DDoS 攻击行为后，通过南向接口向受影响的交换机下发流表规则，对攻击源进行精准标识与隔离。数据层负责执行具体防御策略，包括黑洞转发、带宽限速与包丢弃等操作，从而在网络边缘层即实现恶意流量拦截，减轻控制器负载。系统在关键路径中引入优先级调度机制，动态识别业务重要性并对核心应用流量进行重路由与资源优先分配，确保服务不中断。此外，控制层还建立防御闭环反馈机制，定期回溯检测日志与防御效果，通过参数自校准优化策略配置，实现检测、隔离与评估的持续循环。该架构在保持防御精度的同时提升了系统的整体韧性，为 SDN 环境下的多层联动防御提供了可行技术路径。

4.2 策略自适应与资源调度机制

为应对 DDoS 攻击的多样化与动态性，防御体系需具备自适应策略调节与资源智能调度能力。本文基于强化学习框架设计了自适应策略优化模型，将系统防御效果转化为奖励函数，包括误报率、检测延迟、资源开销及恢复时间等维度指标。通过 Q-learning 或 Deep Reinforcement Learning 算法，系统能在持续运行过程中动态调整流表下发频率、黑名单生存周期及流量限速阈值，实现实时自校正。控制器根据反馈状态选择最优防御动作，以平衡安全性与性能之间的矛盾。实验表明，该机制有效减少 30% 以上冗余策略更新次数，使响应速度提升约 20%，同时显著降低控制层的计算与通信负载。强化学习模型的引入打破了传统阈值判定的静态约束，使系统具备持续学习与环境适应能力，在长期运行中实现“边检测边优化”的动态演化，确保防御策略的前瞻性与资源调度的高效性。

4.3 跨域协同与多控制器防御实现

在大规模或多租户 SDN 部署场景中，单一控制器难以应对跨域攻击与集中负载问题，需通过多控制器协同机制实现全网防护。本文构建的协同防御体系以分布式控制结构为基础，控制器间通过东向接口实现检测结果、黑名单及策略信息的同步共享，利用轻量级消息队列协议（如 gRPC 或 ZeroMQ）降低通信延迟与带宽占用。各控制器根据区域状态进行局部决策，同时在中央协调模块指导下保持全局一致性，形成“局部自治、全局协同”的防御格局。系统引入基于信任度的协作评估模型，对控制器间信息的可信度进行量

化，防止被入侵节点传播虚假警报。仿真结果表明，该机制能在跨域 DDoS 攻击场景下将平均响应时间压缩至 1.2 秒以内，全网攻击流量抑制率超过 90%。多控制器协同模式显著提升了系统的容灾与扩展能力，实现了安全防御的分布式自治与全局最优平衡，为构建新型 SDN 网络安全生态提供了实践依据。

5 实验验证与性能评估

5.1 实验环境与数据集构建

本研究在 Mininet 仿真平台上构建了虚拟 SDN 环境，以验证 DDoS 检测与防御机制的有效性与可扩展性。控制层选用 Ryu 框架，具备良好的可编程性与开放性，便于实现自定义安全策略。网络拓扑由 20 个 Open vSwitch 交换机节点与 200 个终端主机构成，采用分层星型结构以模拟真实互联网的多域分布特性。攻击流量由 hping3 和 BoNeSi 工具生成，分别构建 SYN Flood、UDP Flood 以及复合攻击三种类型，以测试系统在不同攻击模式下的检测敏感度。正常流量采用 HTTP、DNS 与 FTP 业务混合生成，确保数据分布多样性。最终收集正常与攻击流量各 10 万条样本，涵盖包速率、源 IP 熵值、流持续时间、控制消息频率、包间时间间隔等 12 个关键特征维度。模型训练与验证在 Python 环境下完成，结合 TensorFlow 与 Scikit-learn 框架实现特征提取与模型推理，采用 70% 训练集与 30% 测试集划分策略。通过这一设计，实验环境能够有效复现真实网络负载变化，保障检测模型在多场景下的泛化性与稳定性，为后续防御机制评估提供坚实基础。

5.2 检测性能与对比分析

为验证检测算法的性能，本文选取随机森林（RF）、长短期记忆网络（LSTM）以及二者融合的混合模型进行对比实验。评估指标包括检测准确率（Accuracy）、召回率（Recall）、F1 值、误报率（FPR）以及平均响应延迟。实验结果表明，混合模型在综合性能上显著优于单一算法，其中准确率达到 97.4%，召回率为 96.8%，F1 值提升至 0.972，误报率维持在 2.3%。在高强度攻击场景下，控制器平均处理延迟降低 18%，说明模型在应对突发流量时仍具实时响应能力。分析发现，随机森林能有效识别静态特征差异，但对时序变化敏感性不足；LSTM 能够捕捉流量波动趋势，但在特征选择阶段存在过拟合风险。混合模型通过集成学习与时间依赖建模相结合，兼顾静态特征与动态行为，实现更全面的攻击识别。此外，对比传统基于阈值的检测方法，智能流量分析模型在低速率、隐蔽型攻击识别中精度提升约 20%，表现出更强的适应性与泛化能力，为后续动态防御策略提供可靠决策依据。

5.3 防御机制性能与资源消耗评估

防御机制的验证实验聚焦于响应速度、带宽恢复率及系统资源消耗三项核心指标。通过模拟持续 60 秒的高密度攻击流量，监测控制器与交换机的状态变化。结果显示，检测模块在 3 秒内完成异常识别与策略生成，防御模块在 5 秒内将恶意流量削减至基线水平，网络带宽恢复率达到 92%，表明系统具备高效的自愈能力。与传统静态过滤机制相比，本系统的控制器 CPU 占用率降低约 35%，内存消耗稳定在 650MB 以内，体现了优化的资源调度策略。多控制器协同防御机制进一步验证了系统的容灾性能，当单控制器遭受攻击或失效时，备用控制器能在 2 秒内完成接管，保障防御服务不中断。测试还发现，动态策略更新频率与流表生存时间的自适应调整能有效平衡检测准确率与系统负载，使防御机制在大规模网络中保持稳定可扩展性。综合分析可知，本文提出的检测与防御体系在精度、时效性及资源利用效率上均表现优异，为 SDN 环境下的 DDoS 综合防护提供了可推广的技术路径。

6 结语

软件定义网络以其集中控制与可编程特性为 DDoS 攻击防御提供了全新的技术支撑。本文在分析 SDN 架构安全脆弱性的基础上，提出了融合流量特征学习与动态策略优化的检测与防御机制，通过机器学习与强化学习结合，实现从被动响应到主动适应的安全转型。实验结果表明，该机制在检测准确率、响应速度与资源利用率方面均表现优异，能够有效抵御多类型 DDoS 攻击。未来研究可进一步拓展在大规模异构网络中的部署模式，结合区块链技术构建可信数据交换体系，以实现防御策略的可信协同与追溯。同时，应持续优化模型轻量化设计，降低控制器计算负担，提升系统在高并发环境下的稳定性与实时性。通过智能化、分布式的安全体系建设，SDN 将在新一代网络防护架构中发挥更为关键的作用。

参考文献

[1] 李阳阳.基于软件定义网络的DDoS攻击检测与缓解技术研究[D].杭州电子科技大学,2025.

[2] 陈佳伟.基于软件定义网络的DDoS攻击检测与防御系统研究[D].湘潭大学,2024.

[3] 刘尚昆.软件定义网络交换机DDoS攻击检测方法[J].信息记录材料,2023,24(01):210-213.

[4] 刘振鹏,王仕磊,郭超,等.软件定义网络中基于深度神经网络的DDoS攻击检测[J].云南大学学报(自然科学版),2022,44(04):729-735.

[5] 王明君.软件定义网络中DDoS攻击检测与防御方法的研究[D].安徽大学,2020.