面向 SDN 流表多模态感知与 DRL 协同防御 DDoS 方法*

徐泽鹏[1,2]，舒兆港[1,2†]，陈淑武[1,2]，涂 强[1,2]，庄 涛[1,2]
(1. 福建农林大学 计算机与信息学院，福州 350002；2. 福建农林大学 智能传感与农业芯片技术福建省高校工程研究中心，福州 350002)

摘 要：软件定义网络(SDN)的集中化控制架构在提升管理效率的同时，面临分布式拒绝服务(DDoS)攻击风险。针对传统检测方法难以应对大规模动态流量中的隐蔽攻击行为，且易误封短时高并发正常流量的问题，提出一种基于多模态深度强化学习的 DDoS 防御系统。该系统通过融合时空特征解耦与智能决策优化，实现检测精度与资源效率的动态平衡，在资源充足时最大程度规避对非攻击流量的拒绝服务。实验结果显示，其攻击检测准确率平均达 99.61%，误封率最高不超过 0.5%，在保证高准确率的前提下降低了合法流量误封，实现了防御过程对网络服务质量的保障。

关键词：软件定义网络；分布式拒绝服务攻击；对抗深度强化学习网络；张量分解
中图分类号：TP939.08 **文献标志码**：A **文章编号**：1001-3695(2026)02-033-0596-08
doi:10.19734/j.issn.1001-3695.2025.06.0219

SDN flow table multi-modal perception and DRL collaborative defense against DDoS method

Xu Zepeng[1,2], Shu Zhaogang[1,2†], Chen Shuwu[1,2], Tu Qiang[1,2], Zhuang Tao[1,2]
(1. *College of Computer & Information Science, Fujian Agriculture & Forestry University, Fuzhou* 350002, *China*; 2. *Engineering Research Center of Smart Sensing and Agricultural Chip Technology, Fujian Agriculture & Forestry University, Fuzhou* 350002, *China*)

Abstract: The centralized control architecture of SDN enhances management efficiency while posing risks of DDoS attacks. Addressing the challenges of traditional detection methods in handling covert attack behaviors within large-scale dynamic traffic and the tendency to mistakenly block short-term high-concurrency normal traffic, this paper proposed a DDoS defense system based on multi-modal deep reinforcement learning. This system achieved a dynamic balance between detection accuracy and resource efficiency by integrating spatio-temporal feature decoupling and intelligent decision optimization. It maximized the avoidance of denial of service for non-attack traffic when resources are abundant. Experimental results show that the attack detection accuracy rate averages 99.61%, with a false positive rate not exceeding 0.5%. This system reduces false positives for legitimate traffic while maintaining high accuracy, thereby ensuring the quality of network services during the defense process.

Key words: software-defined networking (SDN); distributed denial-of-service (DDoS) attack; adversarial deep reinforcement learning network; tensor decomposition

0 引言

SDN 通过如图 1 所示的控制平面与数据平面的解耦架构，实现了网络流量的全局可编程调度[1]。其核心创新在于构建了垂直分层的三平面体系：应用层(业务逻辑)、控制层(中央决策单元)和数据层(可编程交换机)。这种“集中控制-分布执行”模式有效解决了传统网络静态配置僵化问题，但同时也引入了 DDoS 攻击风险[2,3]。攻击者利用南向接口协议的开放性，通过多协议协同泛洪攻击威胁 SDN 架构安全，导致流表资源耗尽和控制平面过载[4]。当前防御技术主要分为单模态检测方法和多模态融合方法。前者依赖固定阈值，难以适应动态流量，本质上割裂了攻击流量的时空耦合特性，导致异构特征空间语义割裂；后者常常仅进行特征拼接，未显式分离时间、空间、特征模态的交互关联，并且聚焦检测精度，忽视防御动作的资源消耗，缺乏“攻击抑制收益”与“防御成本”的量化权衡，导致动态决策缺失[5,6]。现有技术存在时空特征解耦不足和检测-防御闭环缺失两大关键挑战。传统方法无法显式建模流量数据中时间、空间、特征模态的非线性交互关系，难以捕捉 DDoS 攻击的隐蔽模式；多数研究尚未建立检测到防御的动态决策机制，进而引发合法流量误封或系统资源过载。

针对上述问题，本文提出多模态深度强化学习协同防御机制，核心创新如下：

a)两级防御体系。在数据平面实时计算流量失衡度、Packet-In突发率和流表熵值，结合动态阈值与模糊逻辑实现攻击初筛，解决实时性问题；完成了轻量化异常检测之后进行细粒度时空解耦，构建时间-IP-特征三阶张量模型，通过 PARAFAC 分解显式分离时空交互特征，克服高维特征语义鸿沟。

b)动态决策优化。基于 Dueling DQN 架构解耦状态价值流与动作优势流，通过奖励函数量化攻击抑制收益、成本惩罚及时间衰减因子，引导模型优先选择“高收益低成本”策略，实

收稿日期：2025-06-02；**修回日期**：2025-07-30 **基金项目**：福建省福厦泉协同创新平台项目(2025E3012)；福建省高校产学研合作项目(2024H6007)；福建省高校产学研联合创新项目(2024H6030)

作者简介：徐泽鹏(2001—)，男，福建泉州人，硕士研究生，主要研究方向为网络与信息安全；舒兆港(1981—)，男(通信作者)，江西鄱阳人，副教授，硕导，博士，主要研究方向为软件定义网络、网络功能虚拟化、网络切片(zgshu@fafu.edu.cn)；陈淑武(1976—)，男，福建罗源人，教授，硕导，硕士，主要研究方向为物联网通信技术；涂强(1993—)，男，江西南昌人，讲师，博士，主要研究方向为物联网通信技术、水声通信技术；庄涛(2001—)，男，福建漳州人，硕士研究生，主要研究方向为网络与信息安全.

现防御过程对网络服务质量的精准保障。

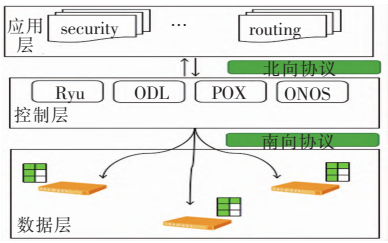

图 1　经典 SDN 体系架构

Fig. 1　Architecture of classic SDN

1　相关工作

随着 SDN 架构中 DDoS 攻击的复杂化,现按照技术演进路径展开分析:单模态检测方法和多模态融合方法。

单模态检测方法基于单一维度的特征分析。统计分析通过数学手段量化时序特征的分布异常,计算开销低但是依赖固定阈值。文献[7]采用熵值检测低速攻击,验证了单一时序特征的有效性,但需在检测率与误报率间权衡;文献[8]设计两级框架,先用快速熵算法定位恶意节点,再用朴素贝叶斯分类器验证,提升了准确性,但未能解决熵值对动态流量的适应性问题;文献[9,10]引入 KL 散度、Rényi 熵等改进统计指标,在物联网和 TCP 攻击场景中提升精度,但仍受限于单一时序维度的语义割裂。机器学习方法通过人工设计多维特征(如包长、速率、协议类型)结合分类模型,缓解了统计方法的"刚性"缺陷,但特征仍隶属于同一模态(如流量统计属性)的浅层组合。文献[11]的 FMDADM 框架提取七维特征,通过混合分类模型实现 99.79% 检测精度,但未区分"时间窗口内的特征波动"与"IP 空间的特征分布";文献[12]将检测模块集成到 SDN 控制器,同步优化资源分配,但特征工程依赖专家经验,难以应对高维数据;文献[13]的 OptMLP-CNN 模型通过 SHAP 技术筛选关键特征,结合 MLP 和 CNN 处理时序与空间特征,但"空间特征"仅指单 IP 的统计属性,未建模多 IP 协同模式;文献[14]针对物联网边缘设备资源受限、实时性要求高的特点,提出了融合深度学习与语义推理的混合架构,通过时空特征协同检测机制和语义层知识图谱增强解决深度学习"黑箱"误判问题,同时结合动态权重融合机制自适应分配计算资源,使模型具有高度计算能力和能源效率。

多模态融合方法整合了异构特征。为弥补单模态缺陷,研究转向融合多类型数据(如流量特征 + 用户日志、数据包特征 + 流统计)。文献[15]在应用层检测中融合数据包特征(如端口、协议)与流统计特征,但未考虑时空维度的复杂关联,对"跨时间窗口的 IP 协同攻击"无效;文献[16]结合张量分解与 XGBoost,通过降噪提升检测准确率至 99%,但仅停留在离线检测阶段,无法应对 SDN 的在线防御需求;文献[17]针对区块链网络混合攻击,采用多分类器集成融合多模态数据,但缺乏动态防御策略,检测与缓解环节割裂;文献[18]处理流量与用户日志两类数据,通过弹性权重算法减少模型更新的"灾难性遗忘",但未深入挖掘流量的时空非线性关系。多模态融合方法虽提升了特征多样性,但未解决"时空耦合特征难以显式建模"的核心问题,且缺乏从检测到防御的闭环决策机制。

现有技术在时空特征解耦和动态决策上存在时空耦合特征建模不足和检测与防御的动态平衡缺失两大挑战。传统方法或依赖单维特征或仅进行多模态特征拼接,无法显式分离时间、空间、特征模态的交互关联,难以捕捉 DDoS 攻击中更底层的隐蔽模式;多数研究聚焦检测精度忽视防御动作的资源消耗,缺乏对"攻击抑制收益"与"防御成本"的量化权衡,易导致合法流量误封或系统资源过载。

2　检测与防御方案

本文提出了一种基于时空多模态感知的 DDoS 攻击协同防御框架,其核心架构包含三级递进式处理流程。第一级是轻量化统计监测,部署于 SDN 数据平面,通过实时监测网络流量动态特征实现攻击初筛。当一级监测触发细粒度检测阈值时,系统将时间、空间和特征三维流量数据组织成三阶张量结构,通过 PARAFAC 张量分解算法,分离并提取流量数据中隐含的时空交互特征[19]。第三级是智能防御决策,使用 Dueling DQN 构建检测精度与防御成本的多目标优化模型。整个系统采用"粗粒度检测(数据平面) + 细粒度决策(控制平面)"的级联式架构,通过动态阈值触发机制,实现检测精度与资源效率的平衡,如图 2 所示。

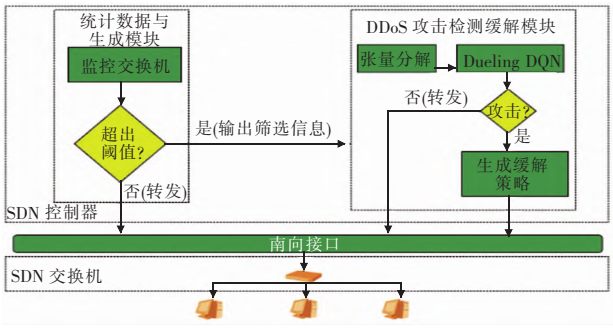

图 2　协同防御框架

Fig. 2　Framework of collaborative defense

2.1　统计与生成模块

为解决传统单模态检测中固定阈值难以适应动态流量的问题,实现攻击的快速初筛以保障实时性,本文设计一级监测采用动态阈值与模糊逻辑协同机制:首先基于滑动窗口,针对 DDoS 攻击中新流泛洪导致控制器过载、非对称性和分布混乱性三种特性,传统固定阈值无法应对正常流量的潮汐效应,因此采用滑动窗口计算,实时更新基线。当流量波动符合正常统计规律时,阈值自适应放宽,减少误触发;当攻击导致指标突变时,阈值快速收紧以提高敏感性。此外,单一指标异常可能是正常波动,而多指标协同异常更具攻击特征。通过高斯型隶属度函数将三指标归一化后,基于规则库(表 1)实现非线性关联推理解决指标间语义割裂问题,降低单指标误判率。以 5 min 为时间窗口计算正常流量的 Packet-In 突发率、流量失衡度、流表熵值的均值与标准差,动态调整基线阈值,然后通过模糊逻辑控制器融合三指标,输出攻击概率。

定义 1　Packet-In 突发率。转发至控制器的 Packet-In 数量与流入交换机的网络流数量的比值,公式为

$$Rate_{\text{Packet-In}} = \frac{Num_{\text{Packet-In}}}{Num_{\text{Inflow}}} \tag{1}$$

定义 2　流量失衡度。流入与流出交换机的网络流数量的失衡度,公式为

$$Imb_t = \frac{|Num_{\text{Inflow}} - Num_{\text{Outflow}}|}{Num_{\text{Inflow}} + Num_{\text{Outflow}}} \tag{2}$$

定义 3　流表熵值。反映流表项的分布混乱程度,公式为

$$H_{\text{flow}} = -\sum_{i=1}^{N} \frac{c_i}{C} \log_2 \frac{c_i}{C} \tag{3}$$

其中:N 为流表项总数;c_i 为第 i 条流表项的匹配计数;$C = \sum_{i=1}^{N} c_i$ 为总匹配次数。阈值的公式如下:

$$\mu_{\text{normal}} + k \times \sigma_{\text{normal}} \tag{4}$$

阈值定义为正常流量的均值和置信系数为 2 的标准差之和,通过实时统计动态更新,对输入变量 Packet-In 突发率R_pin、流量失衡度 I_mb 和流表熵值 H_flow 归一化到[0,1]。模糊集隶属度函数采用高斯型:低、中和高,规则库定义如表 1 所示。R_pin 与 I_mb 同时异常(如高 Packet-In 速率与高 IP 分布失衡并存)时,即便熵值仅为中等,仍判定为中等风险攻击,因两指标协同异常的可信度较高,需执行分级防御(重定向 + 限速)。而 R_pin 或 I_mb 单一指标异常,但熵值 H_flow 显著升高可能为隐

蔽攻击(如单 IP 伪造大量流请求),需启动张量分解检测时空特征(如时间窗口内的 IP 行为模式),避免误判正常突发流量。规则库基于专家经验与历史攻击数据构建,通过离线仿真测试调整隶属度函数参数,确保对正常突发流量和隐蔽攻击的区分能力。通过重心法解模糊,得到 0 ~ 1 的攻击概率值,超过预设阈值 0.7 时触发二级检测,避免单一指标误判。

表 1 规则库定义

Tab. 1 Rule base definition

核心触发条件	攻击概率输出	防御动作(等级)	场景映射与决策逻辑
R_pin 高且 I_mb 高且 H_flow 高	极高(1.0)	直接封禁主攻击 IP(等级 4)	高强度 DDoS 攻击,快速阻断避免控制器崩溃
R_pin 高且 I_mb 高且 H_flow 中	高(0.8)	执行重定向 + 限制端口(等级 3)	中等强度攻击,分级防御平衡效果与资源消耗
R_pin 高或 I_mb 高且 H_flow 高	中(0.6)	启动张量分解检测(等级 2)	单指标高 + 高熵值,精细化检测排除正常流量
R_pin 高或 I_mb 高且 H_flow 中	低(0.3)	触发轻量级日志审计(等级 1)	单指标高 + 熵值中等,日志审计减少误报开销
其他情况	极低(0.1)	继续监测(等级 0)	正常流量或低风险异常

在正常网络运行状态下,交换机依靠流表预存的匹配规则能够处理绝大多数网络流,流入与流出交换机的数据包数量相当,此时的 $Rate_{\text{Packet-In}}$ 和 Imb_t 接近于 0 且流表项匹配分布均匀熵值较低。当 DDoS 攻击发生时,攻击者通过伪造随机源 IP 地址生成海量异常新流,由于交换机流表中缺乏对应匹配条目,导致大量 Packet-In 消息被发送至控制器,交换机缓存溢出导致丢包,此时流表请求导致熵值激增,并且 $Rate_{\text{Packet-In}}$ 和 Imb_t 会急剧增大,当三者都超过预定阈值时,判定可能存在 DDoS 攻击。根据 3.2.3 节所示的实验数据,单交换机平均延迟结果表明流规则安装总时间不超过 0.002 s。系统以 2 s 为周期实时计算上述三项特征值,并与基准阈值进行动态比对,该周期设置可近似认为两者保持同步,从而确保统计数据的时效性,进而实现对网络攻击的实时监测。

2.2 张量分解驱动的多模态特征解耦模块

在第一阶段检测到网络攻击迹象后,触发第二阶段精细化检测流程。为突破传统多模态特征“简单拼接”导致的语义混淆,显式分离时间、空间、特征模态的交互关系,解决隐蔽攻击模式识别难题。攻击行为的本质是特定时间窗口内,多 IP 协同发送具有异常特征的流量。因此构建时间-IP-特征三阶张量,基于 PARAFAC 算法对流量进行张量分解,解耦出时间因子矩阵 $\boldsymbol{A}$、IP 因子矩阵 $\boldsymbol{B}$ 和特征因子矩阵 $\boldsymbol{C}$,以挖掘潜在的攻击相关因子。通过将流量数据建模为三阶张量,实现时间、IP 地址、特征维度的模态显式分离,同时保留数据内部的非线性关联特性。与 Tucker 分解相比,PARAFAC 分解的优势在于满足“三线性假设”,强制要求各模态因子矩阵共享秩 $\boldsymbol{R}$,从而保证时间、空间、特征模态的物理可解释性,因子矩阵的语义独立性更优,更适合攻击特征的显式解耦。

2.2.1 特征集构建

CIC-DDoS2019 原始数据集包含 87 个特征,全面覆盖了网络流量的各类统计指标。通过以下关键步骤筛选关键特征。首先进行数据清洗,剔除“无意义数据”及低影响力特征(数据 90% 以上为 0)并对剩余特征进行统计增强,按每分钟切割时间窗口计算均值、方差、峰度、熵值等衍生指标。随后采用决策树对特征计算置换重要性:对数据集中的特征进行随机重排后输入到决策树中,计算模型在受污染数据集上的评分并重复 50 次取其平均值。最后通过 Person 相关系数衡量特征之间的线性相关性,计算两两特征之间的协方差和标准差的比值。筛选出对重要性大且相关性低的特征子集如表 2 所示[20~23]。

表 2 最优特征子集

Tab. 2 Feature selection

特征	含义
Flow Packets/s_mean	平均每秒网络流的数据包数
Bwd Packets/s_mean	平均每秒反向流量数据包数
Fwd Packet Length Max_mean	前向数据包最大长度的均值
Fwd Packet Length Max_var	前向数据包最大长度的方差
Fwd Packet Length Max_entropy	前向数据包最大长度的香农熵
Packet Length Std_kurtosis	数据包长度标准差的峰度
Bwd Header Length_entropy	反向包头长度分布的香农熵
Packet Length Variance_entropy	数据包长度方差的分布熵
Avg Fwd Segment Size_entropy	前向分段大小的分布熵
Active Min_mean	活动连接数最小值的均值

2.2.2 张量建模

PARAFAC 分解的三线性假设为时空特征解耦提供了数学基础。通过将流量数据建模为时间-IP-特征三阶张量 $\boldsymbol{\Gamma} \in \mathbb{R}^{T\times I\times F}$,原始数据中隐含的攻击脉冲的时间定位(如夜间 2 点的流量激增)、攻击源的空间分布(如多个随机 IP 协同请求)、异常流量的特征组合(如小包速率异常高)被显式分离为三个二维矩阵($\boldsymbol{A},\boldsymbol{B},\boldsymbol{C}$)。这种解耦不仅规避了单模态特征的片面性,还通过时空交互项 $\boldsymbol{A}_t \circ \boldsymbol{B}_i$ 捕捉特定 IP 在特定时间的协同异常,为后续强化学习决策提供了结构化的状态表示。其中时间模态 T 为时间窗口数,I 为源 IP 数,F 为流量特征维度。张量元素表示时间窗口 t、源 IP 地址 i 下第 f 个流量特征的均值,融合了时间动态、IP 空间分布及流量特征的三维关联信息。对于张量 $\boldsymbol{\Gamma}$ 使用 PARAFAC 分解如式(4)所示。

$$\boldsymbol{\Gamma} = a_1 \circ b_1 \circ c_1 + \cdots + a_R \circ b_R \circ c_R + \boldsymbol{E} \tag{5}$$

其中:“ ∘ ”为外积,将三个向量组合成三阶张量;$\boldsymbol{E}$ 为误差张量,是原始张量与重构张量之间的差值,代表分解过程中未被提取的信息,如图 3 所示。

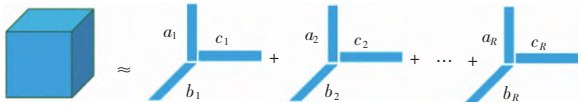

图 3 三维张量的 PARAFAC 分解

Fig. 3 PARAFAC decomposition of three-dimensional tensor

图中展示了三维张量通过 PARAFAC 分解的过程,PARAFAC 分解基于“三线性假设”,即三阶张量可近似为 R 个秩-1 张量的外积之和:

$$\Gamma_{t,i,f} \approx \sum_{r=1}^{R} \lambda_r (\boldsymbol{a}_r \circ \boldsymbol{b}_r \circ \boldsymbol{c}_r) \tag{6}$$

其中:时间向量 $\boldsymbol{a}_r \in \mathbb{R}^T$、空间向量 $\boldsymbol{b}_r \in \mathbb{R}^I$、特征向量 $\boldsymbol{c}_r \in \mathbb{R}^F$ 分别对应第 r 个基础模式的时间、空间、特征分量。该假设允许将原始张量的时空交互特征分解为独立模态的线性组合,从而显式分离“时间-空间-特征”的关联。时间模态刻画流量在时间序列上的动态模式,如秒级脉冲式爆发、分钟级周期性波动。通过时间因子矩阵 $\boldsymbol{A} \in \mathbb{R}^{T\times R}$ 表示,每一行对应一个时间窗口在 R 个“基础时间模式”上的强度分布(如突发模式、平稳模式),每一列表示不同时间窗口下的基础流量模式(如突发流量、周期性波动)。空间模态描述 IP 地址的空间分布特征,如攻击 IP 的分布式伪造、正常 IP 的集中访问,IP 因子矩阵 $\boldsymbol{B} \in \mathbb{R}^{I\times R}$ 的每一行表示一个 IP 在 R 个“基础空间模式”上的活跃程度(如恶意 IP 集群、合法客户端),每一列表示不同 IP 地址的分布模式(如攻击 IP 集群、正常 IP 分布)。特征模态捕捉流量的统计属性,如包长、速率、协议类型的分布,特征因子矩阵 $\boldsymbol{C} \in \mathbb{R}^{F\times R}$ 反映每个流量特征与 R 个“基础特征模式”的关联强度(如异常高的小包速率对应攻击模式)。以及时空交互项 $\boldsymbol{A}_t \odot \boldsymbol{B}_i$ 的解耦特征通过特征拼接进行多模态融合。其中,R 为分解秩、λ 为权重系数。从时间、IP、特征三个维度捕捉流量的相关信息,每个秩-1 张量由时间、IP、特征三个向量外积构成。原始张量中时间、IP、特征的底层关联隐含在三维结构中,分解后通过三个二维矩阵显式分离,每个矩阵聚焦单一维度的“基础模式”。固定其中两个模式的因子更新第三个模式来交替更新因子矩

阵，通过最小二乘法最小化残差平方和，迭代至最终收敛阈值。高维优化问题拆解成了低维子问题，降低计算耦合性[24]。

时间因子矩阵更新：

$$\boldsymbol{A}_{:,r} \leftarrow \boldsymbol{A}_{:,r} \cdot \frac{(\boldsymbol{\Gamma} \times_2 \boldsymbol{B}^T \times_3 \boldsymbol{C}^T)_{:,r}}{\boldsymbol{A} \cdot (\boldsymbol{B} \odot \boldsymbol{C}) \cdot \boldsymbol{A}^T \cdot \boldsymbol{A}_{:,r}} \tag{7}$$

IP 因子矩阵更新：

$$\boldsymbol{B}_{:,r} \leftarrow \boldsymbol{B}_{:,r} \cdot \frac{(\boldsymbol{\Gamma} \times_1 \boldsymbol{A}^T \times_3 \boldsymbol{C}^T)_{:,r}}{\boldsymbol{B} \cdot (\boldsymbol{A} \odot \boldsymbol{C}) \cdot \boldsymbol{B}^T \cdot \boldsymbol{B}_{:,r}} \tag{8}$$

特征因子矩阵更新：

$$\boldsymbol{C}_{:,r} \leftarrow \boldsymbol{C}_{:,r} \cdot \frac{(\boldsymbol{\Gamma} \times_1 \boldsymbol{A}^T \times_2 \boldsymbol{B}^T)_{:,r}}{\boldsymbol{C} \cdot (\boldsymbol{A} \odot \boldsymbol{B}) \cdot \boldsymbol{C}^T \cdot \boldsymbol{C}_{:,r}} \tag{9}$$

其中：$\times_k$ 表示沿第 k 维度的张量乘法；$\odot$ 为内积。时空交互项 $\boldsymbol{A}_t \odot \boldsymbol{B}_i$ 通过逐元素乘积捕获特定 IP 在特定时间窗口的协同异常行为（如分布式 IP 在短时间内集中发送攻击流量）。最终，将上述四部分特征与攻击持续时间 $D(t)$ 拼接为状态向量 $\boldsymbol{S}_t \in \mathbb{R}^{4R+1}$ 作为 Dueling DQN 的输入。如式(9)所示。

$$\boldsymbol{S}_t = [\boldsymbol{A}_t, \boldsymbol{B}_i, \overline{\boldsymbol{C}}_t, \ln(1 + \boldsymbol{A}_t \odot \boldsymbol{B}_i), D(t)] \tag{10}$$

取时间因子矩阵 $\boldsymbol{A}$ 的第 t 行（维度 $1 \times R$），通过转置得到 R 维列向量，表示当前时间窗口在 R 个“基础时间模式”上的强度分布。时空交互项乘积结果取自然对数压缩数值范围并保留非线性关联特征。最终拼接的状态向量为 $4R+1$ 维。既保留了各模态的独立语义信息，又通过拼接整合全局状态使强化学习模型能够自适应学习不同模态特征的权重关系。

文献[25]采用时空图神经网络和 GCN-GRU 模型，通过图结构建模网络节点的空间关联及时序特征，但本质上仍依赖图拓扑的静态建模，对动态流量中的非线性时空交互特征捕捉能力有限。本文采用的三阶张量分解显式解耦时间-空间-特征模态方式避免了图神经网络隐含建模的语义模糊性，尤其在处理高维动态流量时，能更精准地识别攻击模式与正常流量的差异。在 SDN 环境中，高维流量数据会导致张量分解的计算复杂度呈指数级增长。当网络规模扩大时，三阶张量的元素数量可达 10^9 级别，此时单次分解的迭代计算量也会显著增加。此外，高维数据中的噪声和冗余特征会加剧张量分解的收敛难度，在高维场景下可能导致收敛时间超过防御响应的时间阈值。网络流量（如突发攻击、流量潮汐效应）的动态变化要求张量分解具备在线更新能力，但高维数据的动态更新会进一步放大实时性瓶颈：增量更新时可能因新数据的引入导致因子矩阵重计算，尤其是在攻击突发阶段，流量特征的剧烈变化可能使分解模型频繁重构，消耗大量计算资源。为了解决高维流量下的实时性瓶颈，可在一级检测设置更严格的触发阈值，仅在高风险场景下启动张量分解，避免低风险流量的冗余计算，并且利用强化学习的状态价值流动态筛选关键特征维度，仅对高风险特征子集进行张量分解，减少计算量。

2.3　MDP 模型构建与动态决策

将 SDN 防御场景建模为马尔可夫决策过程，定义五元组 (S, A, P, R, γ)，解决传统方法“重检测轻防御”导致的资源效率低下问题，构建“检测-决策-执行”闭环，实现防御动作的动态优化。状态空间 S 包含当前网络状态的时空特征；动作空间 A 为防御动作集合，对应 SDN 控制器的流表操作；转移概率 $P(s'|s,a)$ 由网络流量动态和防御动作共同决定，隐含于环境模型中；奖励函数 $R(s,a)$ 量化攻击抑制收益与防御成本的动态平衡；折扣因子 γ 权衡即时奖励与未来奖励的重要性。例如当检测到时间窗口 t 的流表熵值激增（时间模态异常），且 IP 因子矩阵 $\boldsymbol{B}$ 显示多个随机 IP 活跃（空间模态异常），状态价值流 $V(s)$ 会评估当前态势为高风险。此时动作优势流 $A(s,a)$ 计算重定向与封禁 IP 成本的相对收益：若攻击强度较低，模型优先选择重定向（避免误封）；若攻击持续超过 60 s，奖励函数的时间衰减因子强制提升封禁 IP 的收益，触发高成本动作。

2.3.1　MDP 模型构建与动态决策

状态向量包含时空特征分量：$\boldsymbol{A}_t$（时间因子，R 维）来自张量分解的时间窗口因子矩阵，捕捉流量突发模式；$\boldsymbol{B}_i$（IP 因子，R 维）来自 IP 地址因子矩阵，刻画异常 IP 分布特征；$\overline{\boldsymbol{C}}_f$（特征均值，$R$ 维）为所有流量特征在基础模式上的均值，反映全局特征趋势；$\boldsymbol{A}_t \odot \boldsymbol{B}_i$（时空交互项，$R$ 维）通过内积捕捉特定 IP 在特定时间的协同异常。分解秩的选择通过如 3.3 节重建率确定。通过这四个分量，状态向量实现了时间动态、空间分布、特征趋势和时空交互的四维特征融合，避免单一模态的片面性。

2.3.2　动作空间显示化

动作空间定义了三类防御动作，对应 SDN 控制器的流表操作如表 3 所示。“封禁 IP”对高威胁源的优势显著高于“重定向”，但成本更高；而重定向机制通过一次性路径计算下发流表，避免传统逐包规则匹配导致的“规则匹配风暴”，实现数据转发阶段近零 CPU 消耗。为了量化防御动作的成本，假设单位等待时间对应单位成本，基于等待时间的成本建模。实验采用分级防御机制设计，疑似攻击先重定向至清洗平台，若未缓解再触发高成本的封禁 IP，通过攻击抑制奖励抵消成本。这种策略避免了“一刀切”，平衡了误判风险与资源消耗。

表 3　动作空间

Tab. 3　Action space

动作	SDN 实现	资源成本	防御效果
a_1 重定向	通过 Flow-Mod 下发目的 IP 改写规则，将疑似攻击流量导向清洗平台	0.2	低风险，保留流量可恢复性
a_2 限制端口	调用交换机 MeterTable 功能，对特定端口设置速率限制	0.4	中等风险，部分阻断异常流量
a_3 封禁 IP	通过 Flow-Mod 删除对应 IP 的流表项，阻断其所有通信	0.8	高风险，可能误封合法流量

2.4　Dueling DQN 架构

双流架构如图 4 所示。状态价值流用于评估网络整体状态，动作优势流量化防御动作相对优势，实现精准检测与资源高效利用的平衡。正常状态下，高状态价值 $V(s)$ 与低动作优势 $A(s,a)$ 会抑制误触发“封禁 IP”的 Q 值。Q 值定义如下：

$$Q(s,a) = V(s) + \left[A(s,a) - \frac{1}{|A|}\sum A(s,a)'\right] \tag{11}$$

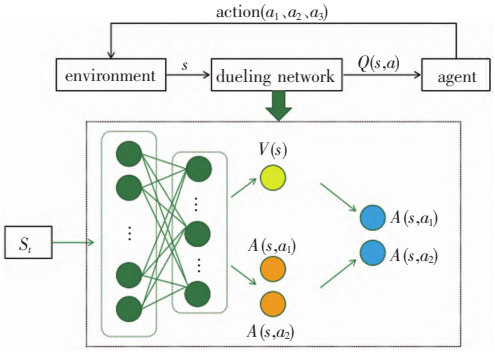

图 4　Dueling DQN 架构

Fig. 4　Architecture of dueling DQN

攻击状态中，大规模流量洪泛时状态价值显著下降触发干预。动作优势 $A(s,a)$ 定义为封禁 IP、限制端口和重定向三个动作相对于平均动作的优势。当攻击强度足够大时，奖励函数允许模型选择封禁 IP，因其攻击抑制收益远超过成本。状态价值流捕捉流量波动、IP 分布等全局趋势；优势流基于动作相对优势学习，避免过拟合。该架构解决 DDoS 时空协同建模难题，为网络安全动态决策提供普适框架，特别是高维动态资源受限的实时防御场景。状态价值流输入完整状态向量，输出网络整体安全等级，如式(12)(13)所示。

$$V(s;q_v) = W_v^T j(W_2^T \mathrm{ReLU}(W_1^T s)) \tag{12}$$

$$A(s,a;\theta_a) = W_a^T \varphi(W_2^T \mathrm{ReLU}(W_1^T s)) \tag{13}$$

其中：θ_v 为价值流参数；φ 为激活函数；W_1 和 W_2 为全连接层权重。当单个特征异常时 $\overline{C}_t$ 变化较小，避免误判；当多个特征在同一基础模式上异常时 $\overline{C}_t$ 显著升高，触发攻击预警。动作优势流输出对每个动作计算相对优势如式(14)所示。

$$A(s,a;\theta_a)=W_a^T\varphi(W_2^T\mathrm{ReLU}(W_1^T s)) \tag{14}$$

其中：θ_a 为优势流参数。通过减去优势均值 $\frac{1}{|A|}\sum A(s,a')$，确保 $V(s)$ 仅表征状态固有价值，而 $A(s,a)$ 聚焦动作间的相对收益差异，从而使优势归一化。实验采用网格优化策略，引入概率 0.2 的 dropout 层防止过拟合，结合余弦退火学习率为

$$\mathrm{lr}(t)=\frac{1}{2}\left[1+\cos\left(\frac{tp}{T}\right)\right]\times lr_0 \tag{15}$$

初期高学习率快速收敛，后期精细调整，避免局部最优。通过分离主网络与目标网络参数更新，目标值计算如式(16)所示。

$$y_j=r_j+\kappa\times max_a\times Q_{\mathrm{target}}(s_j',a')(1-d_j) \tag{16}$$

其中：y_j 表示第 j 个样本的目标值，用于训练网络逼近真实 Q 值；r_j 为即时奖励；κ 为折扣因子；d_j 表示终止状态，当后续无状态转移则忽略未来奖励。通过分离主网络与目标网络的参数更新，降低 Q 值计算的方差，避免因参数频繁变动导致的训练波动，使训练过程更稳定。

$$Loss=E[(y_j-Q_{\mathrm{main}}(s_j,a_j;q))^2] \tag{17}$$

通过均方误差优化 Q 值，使模型学会在高流表熵值时优先选择重定向，在历史匹配度高时果断封禁 IP。$Q_{\mathrm{main}}(s_j,a_j;\theta)$ 逼近上述目标值 y_j。目标网络参数定期从主网络同步，减少训练过程中 Q 值的方差，使损失函数优化更稳定，其中 $Q_{\mathrm{main}}(s_j,a_j;\theta)$ 表示主网络对状态 s_j 和动作 a_j 的 Q 值预测，E 为对样本集的期望，通过批量梯度下降优化。具体架构如图 5 所示。融合时空特征的状态向量输入到主网络中，主网络分别计算状态价值 $V(s)$ 和动作优势 $A(s,a)$，进而得到 Q 值向量 $\boldsymbol{Q}(s,a)$。同时，通过分离主网络与目标网络参数更新，目标网络根据主网络同步的参数计算目标值 y_j。在训练过程中，以 MSE 作为优化目标，使主网络的 Q 值输出逼近目标值，从而优化模型决策，确保决策的准确性和高效性。

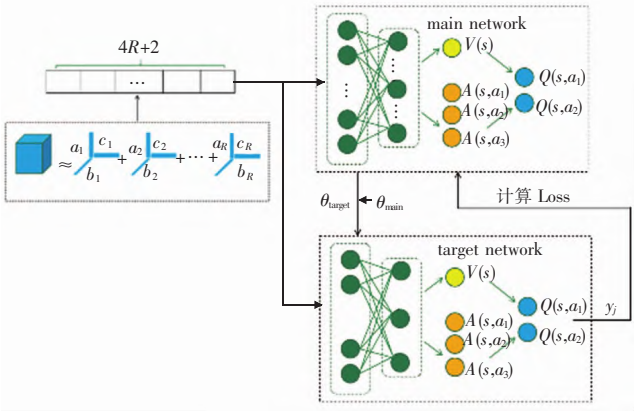

图 5 基于 Dueling DQN 的动态决策

Fig. 5 Dynamic decision making based on Dueling DQN

2.5 动态奖励机制设计

为引导模型选择高收益低成本策略，量化攻击抑制收益与防御成本，解决传统方法缺乏闭环决策的问题，设计时空感知动态奖励函数，由三部分构成：

$$R(s,a)=R_{\mathrm{attack}}+R_{\mathrm{cost}}+R_{\mathrm{temporal}} \tag{18}$$

攻击抑制奖励是基于 Packet-In 速率变化率设计奖励机制的核心项，结合时空特征解耦结果如式(19)所示。

$$R_{\mathrm{attack}}=\mu\times\Delta I(t)-\nu\times Intensity \tag{19}$$

其中：$\Delta I(t)$ 表示当前时间窗口与前一时间窗口的 Packet-In 速率变化量，降低为正、升高为负，鼓励模型快速降低异常流量。μ、ν 为权重系数；$Intensity$ 表示当前攻击强度，定义为前向流量包数，平衡短期变化与长期影响。防御成本惩罚量化动作的资源消耗与潜在误伤风险如式(20)所示。

$$R_{\mathrm{cost}}=-\omega\times[C_a\times(1+\delta(t))+\lambda_{\mathrm{risk}}\times H_{\mathrm{false}}] \tag{20}$$

其中：H_{false} 为当前动作导致合法流量误封的概率，与状态中的 H_{flow} 负相关(若熵低但实施封禁，惩罚加重)。如果流表熵值 H_{flow} 达到预定阈值过长，$\delta(t)$ 增大到 0.5 强制增加高成本动作的惩罚，避免控制器资源过载。

$$\delta(t)=\begin{cases}0.5\\0\end{cases} \tag{21}$$

引入攻击持续时间衰减因子 R_{temporal}，鼓励模型快速响应：

$$R_{\mathrm{temporal}}=\frac{R_{\mathrm{attack}}+R_{\mathrm{cost}}}{1+\delta\times D(t)} \tag{22}$$

其中：$D(t)$ 为当前持续时间；δ 为衰减系数，当攻击持续时间大于 60 s 时，奖励减半，强制模型快速响应短时爆发攻击。权重系数 μ、ν、ω 通过网格搜索确定。预设参数范围为

$$\begin{cases}\mu\in\{0.1,0.5,1.0\}\\\nu\in\{0.01,0.1,1.0\}\\\omega\in\{0.2,0.4,0.8\}\end{cases} \tag{23}$$

对于每组参数组合，在 CIC-DDoS2019 数据集上进行五折交叉验证，选择使检测准确率与误封率加权和最优的组合(权重设为 0.8∶0.2)。最终确定参数分别为 0.5、0.1 和 0.4。此时平均准确率达到 99.61%，误封率小于 0.5%，在保证检测精度的同时兼顾了防御成本，实现“检测-决策-资源”的高效协同，显著提升了 SDN 控制器的资源利用率。本文提出的如式(3)所示的 PARAFAC 张量分解通过三线性假设将流量数据分解为时间、IP、特征三维模态的线性组合，其核心优势在于基模式的可扩展性和异常模式的显式表征。当新型攻击引入新的时空模式(如未知端口的脉冲式流量)，分解秩 $\boldsymbol{R}$ 可动态调整以捕获新的基模式。若攻击特征与现有基模式的余弦相似度低于阈值，新增基模式将被激活，从而避免“特征空间固化”问题。并且新型攻击的时空交互项会呈现独特的矩阵分布(如突发时间窗口与随机 IP 的高相关性)，通过动态更新特征因子矩阵 $\boldsymbol{C}$，可实时识别异常特征组合。如式(18)所示的 Dueling DQN 奖励函数设计具备动态权重自适应和成本惩罚的动态校准能力。当新型攻击导致 Packet-In 速率变化率的梯度异常时，攻击抑制奖励项会通过反向传播调整权重强化对新型攻击模式的敏感性；若新型攻击利用低熵特征规避检测，防御成本惩罚项中的与流表熵值的负相关性会触发惩罚系数的自适应增大。

3 实验与分析

3.1 实验环境设置

实验基于 Ubuntu 16.04 LTS 系统，采用 Mininet 模拟器构建 SDN 网络拓扑，包含 4 台交换机(各连接 9 台主机)与 POX 控制器，网络带宽配置为 100 Mbps，延迟控制在 2 ms 以内。控制器及主机 IP 地址分配如表 4 所示。

表 4 控制器及主机 IP 地址分配

Tab. 4 Controller and host IP address assignment

名称	IP 地址	定位
控制器	10.0.0.1	流量控制
主机 1/10/19	10.0.0.41/50/59	攻击主机
主机 2 ~ 9	10.0.0.42-10.0.0.49	正常主机
主机 11 ~ 18	10.0.0.51-10.0.0.58	正常主机
主机 20 ~ 27	10.0.0.60-10.0.0.67	正常主机
主机 28 ~ 36	10.0.0.68-10.0.0.76	正常主机

其中主机 1、10、19 作为攻击主机，其余为正常主机，如图 6 所示。通过 GNS3 集成 Virtual Box 虚拟机与 Docker 容器，利用 TCP Replay 工具注入 CIC-DDoS2019 数据集以模拟真实世界中

的网络环境,用于评估和测试分布式拒绝服务攻击检测算法。

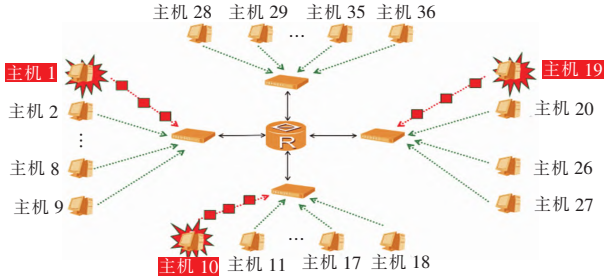

图 6　拓扑示意图
Fig. 6　Topological schematic

3.2　实验结果分析

设置主机 1 为攻击源,以 90% 的最大流量强度 f_{max} 持续发送包含随机伪造目标 IP 的 SYN 脉冲流(单次脉冲 0.2 s,周期 2 s),其余主机以[0,f_{max}]随机速率发送正常流量。以 0.2 s 为周期统计交换机的流入数据包数 $Inflow_t$ 流出数据包数 $Outflow_t$ 的流量失衡度 Imb_t、Packet-In 的消息速率 $Rate_{packet\_in}$,以及反映流表项的分布混乱程度流表熵值。当三者同时超过阈值(基于训练阶段 20 000 组样本均值确定)时触发攻击判定。部署主机 1、5、9 为协同攻击源,初始速率 10 Kf/s 持续 40 s,之后再在 10 s 之内达到最高值 38 Kf/s,最后逐渐减少在 80 s 后恢复初始速率。通过对比静态阈值限速、动态协同防御、全量阻断对照三种策略,验证防御机制对流量突发和资源消耗的平衡能力,结果如图 7 所示。

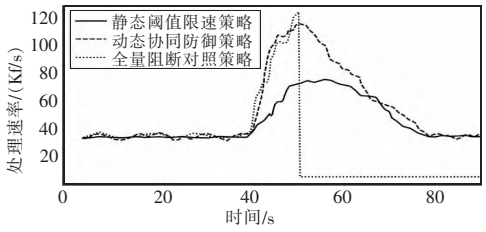

图 7　模型效果
Fig. 7　Model effect

在正常的网络活动中,三种策略都能正常处理流量数据。但随着攻击主机群发动攻击,控制器的资源被迅速消耗。依赖控制器自然处理能力机制在攻击发起后因过载直接中断;为每台主机预设固定发送速率上限机制虽避免了中断问题,但是实际处理速率显著低于上限导致控制器的队列容量始终存在冗余;本文的曲线光滑且贴近容量上限表明策略实时抑制恶意主机的新流请求同时保障了合法流量,使控制器处理速率贴近可用的资源容量,既无超载也无闲置。结果证明该方法在抗攻击能力(无中断)和资源利用率(无闲置)之间实现了更好的平衡。

为了验证在不同负载场景下的实时性,设置 6 组实验,自变量是控制器的剩余资源和攻击速率,因变量是攻击响应时间。让攻击主机使用 Hping3 发送随机目标 IP 的 SYN 脉冲流,模拟分布式 DDoS 攻击,每组实验重复 50 次确保数据稳定性。具体结果如表 5 所示。由实验结果可知,在剩余资源较为不足时候(20% 的剩余资源和 45 Kf/s 攻击)因为资源容易耗尽触发缓解机制更加迅速,控制器响应更快,证明了对高速攻击的快速反应能力;在剩余资源充足的情况下(90% 的剩余资源和 30 Kf/s)控制器响应稍慢但是资源缓冲更加充足避免误封,表明了高容量下仍能在合理时间内缓解攻击。

表 5　不同负载下的实时性
Tab. 5　Real-time under different loads

控制器剩余资源/%	攻击速率/(Kf/s)	平均响应时间/s	控制器剩余资源/%	攻击速率/(Kf/s)	平均响应时间/s
90	30	10.98	20	30	4.82
90	38	10.12	20	38	4.21
90	45	9.09	20	45	3.99

3.3　动作的成本量化

防御动作的成本量化是平衡检测精度与资源消耗的核心环节,其本质是对控制器与交换机处理开销、流表规则复杂度及潜在服务中断风险的综合评估。不同防御动作在消息交互频次、规则部署范围及硬件资源占用上存在显著差异,现结合 SDN 设备的实际处理效率进行建模。

3.3.1　基于消息处理效率的成本建模

SDN 控制器与交换机的协同过程中,防御动作的执行依赖以下三类关键消息交互:a) Packet-In 消息:交换机向控制器请求未知流的转发策略,攻击时大量新流触发高频 Packet-In 消息,导致控制器过载;b) Flow-Mod 消息:控制器向交换机下发流表规则,在双向通信场景中,需通过 Flow-Mod 下发入方向和出方向的过滤规则,并通过 Barrier 消息确认多交换机规则同步;限制端口通过 Flow-Mod 下发带速率限制的流表规则,调用交换机内置的 Meter Table 功能实现流量控制;重定向在传统场景下通过 Flow-Mod 下发改写目的 IP、端口的转发规则;c) 状态维护消息:处理防御动作引发的状态维护,其服务率随动作复杂度升高而下降。

通过 Mininet 仿真环境实测获取交换机和控制器在正常处理流程中的服务速率和等待时间,得到相关数据如图 8 所示。

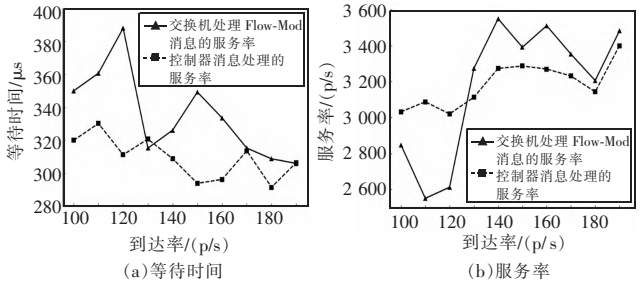

图 8　交换机和控制器在不同到达率下的服务率和等待时间
Fig. 8　Service rates and waiting times at different arrival rates

不同的防御动作在消息交互频次、规则部署范围及硬件资源占用上有所不同,这些差异会影响交换机和控制器的服务率和等待时间。通过 Mininet 仿真环境实测获取相关数据,为后续基于消息处理效率的成本建模量化不同防御动作的资源消耗。

3.3.2　资源消耗量化

基于平均等待时间和平均服务率,结合动作对系统资源的占用特性,通过平均等待时间、服务率的资源消耗与风险评估构建综合模型确定动作成本,引导防御决策优先选择高性价比动作。

表 6 列出了交换机与控制器在相关操作中的平均等待时间等关键参数,为后续基于等待时间和服务率计算动作成本提供数据支持。量化御动作的综合成本 C_{action} 如下所示。

$$C_{action}=\lambda_{res}\times\frac{W_{wait}}{S_{service}}+\lambda_{risk}\times\left(1-\frac{R_{clean}}{R_{total}}\right) \tag{24}$$

调整系数 λ_{res} 对基础资源消耗值进行区间适配,基于平均等待时间 W_{wait} 和平均服务率 $S_{service}$ 计算资源消耗量化结果,映射到与实验预设成本值相匹配的量级区间。系数的设定遵循防御动作对系统资源的影响维度(范围、强度、持续时间)。平均等待时间与平均服务率的实测数据见表 6,构成基础资源消耗的量化依据。流量清洗率 R_{clean} 和总流量 R_{total} 的比值表示流量清洗的有效性,未清洗比例($1-R_{clean}/R_{total}$)越高,说明误封合法流量的风险越大,惩罚项通过权重系数放大该风险对总成本的影响。反映防御动作对合法流量的误伤风险,通过实时监测每秒采样获取。业务损失权重 λ_{risk} 表征误封对业务连续性的影响程度,依据防御动作的阻断特性差异化设定。结合业务影响评估与误封风险分析,综合资源消耗成本归一化到[0,1],最终确定封禁 IP 的成本为 0.8,限制端口为 0.4,重定向为 0.2。动作成本-攻击收益-时间衰减的三维量化框架是模型的核心价值,该框架可兼容多样化的网络环境与策略目标,为智

能防御决策提供通用化解决方案。

表 6 交换机与控制器的平均等待时间

Tab. 6 Average wait time between switch and controller

统计量	值	统计量	值
Arrival rate	100 ~ 190 p/s	Flow-Mod waiting time	335 μs
Flow-Mod service rate	3 077 p/s	Controller waiting time	309 μs
Controller service rate	3 198 p/s		

3.4 评估指标

如表 7 所示,本文提出的多模态感知与深度强化学习协同防御机制在 CIC-DDoS2019 数据集上实现了高准确率(99.61%)、强泛化能力(0.998 5)、优平衡性能(0.997 3),验证了该方法在 SDN 环境中应对动态复杂攻击的有效性。其核心支撑源于多模态特征解耦与动态决策的协同优化:通过 PARAFAC 张量分解将流量数据建模为时间-空间-特征三阶张量,强制满足“三线性假设”,使隐藏的攻击模式被分解为独立的因子矩阵。这种解耦避免了单模态特征的语义割裂,从而提升对隐蔽攻击的识别能力。Dueling DQN 架构将状态价值流 $V(s)$ 与动作优势流 $A(s,a)$ 解耦,通过式(11)实现“全局状态评估 + 动作相对优势”的联合优化。

表 7 五折交叉验证的性能

Tab. 7 Performance of 50% discount cross validation

交叉验证	accuracy	AUC	F_1	交叉验证	accuracy	AUC	F_1
1	0.994 6	0.999 2	0.996 9	4	0.997 1	0.999 1	0.998 4
2	0.995 1	0.998 9	0.997 2	5	0.996 5	0.996 6	0.995 6
3	0.997 2	0.998 9	0.998 3				

图 9 展示了在数据集 CIC-DDoS2019 上本文方法与使用 Q-Learning、目标网络和经验回放的文献[26]、使用 DQN 和迁移学习的文献[27]、使用 Dueling DDQN 和优先经验回放的文献[28]、使用 DQN 和 BiLSTM 时序分析的文献[29]的误封率对比。

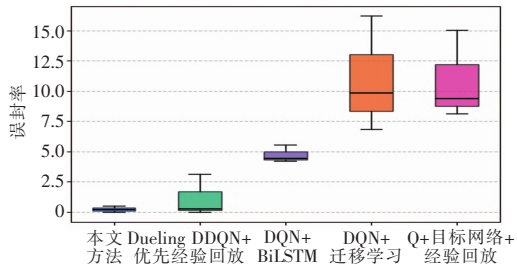

图 9 不同方法的误封率

Fig. 9 False seal rate of different methods

本文方法箱线高度极低,误封率趋近于 0,表现最优,说明该方法在减少误封方面效果显著,主要得益于模糊逻辑与动态阈值的抗干扰性设计。一级监测采用模糊逻辑融合 Packet-In 突发率、流量失衡度、流表熵值三指标,通过高斯型隶属度函数处理指标间的非线性关联。动态奖励函数和防御成本惩罚项量化了动作风险。当流表熵值 H_flow 较低时表明流量特征分布均匀,合法流量概率高,实施封禁 IP 会触发更高惩罚,从而抑制误封行为。Dueling DDQN 的误封率仅稍高于本文方法,但整体仍处于较低水平,表明对策略改进的高价值经验在一定程度上优化了误报情况。相较于文献[26 ~ 29],本文方法误封率显著更低,现有方法仅拼接多模态特征,未显式分离时空交互关系;而本文方法通过 PARAFAC 分解将“时间-空间-特征”模态解耦为独立矩阵,再通过特征拼接状态向量实现语义增强,使模型能精准识别攻击特征与正常流量的边界。Dueling DQN 的优势流设计允许模型学习动作间的相对收益差异而非绝对价值,但传统 Q-Learning 等方法缺乏这种相对价值评估机制。本实验最高不超过 0.5% 的误报率表明所提方法可有效解决误识别问题,实现了防御过程中网络服务质量的精准保障。

经过实验,丢弃率、批量大小和学习率的最佳取值分别为 0.2、64 和 0.001,结果如图 10 所示。当丢弃率为 0.2 时,损失值随训练轮数增加逐渐下降并稳定在 6.5% 左右,且收敛速度最快、稳定性最佳;对比批量大小 32、64、128 的训练效果,发现 64 是平衡收敛速度与稳定性的最佳值,损失值下降速度快于 128,且稳定性优于 32;学习率 0.001 时,损失值迅速降低并稳定至 6% 左右,损失率为 0.000 1 时虽也可以迅速降低但是波动较大,更低的损失率会导致损失率更高。图 11 展示了不同训练轮数下平均累积回报和 Q 值的变化情况。

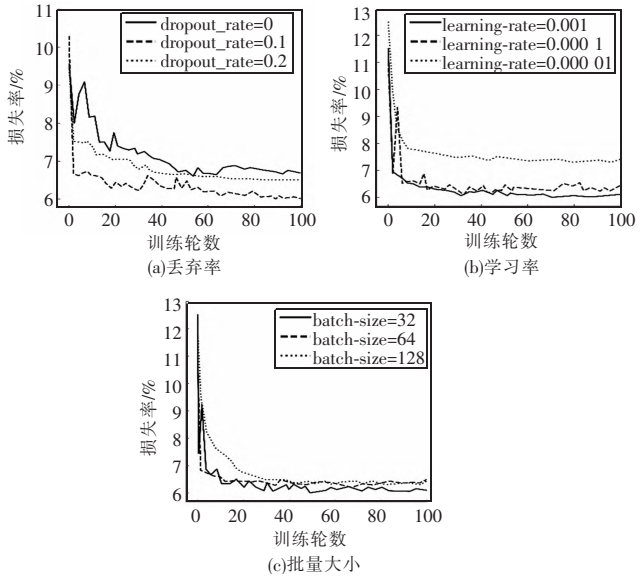

图 10 不同参数对模型的影响

Fig. 10 Effect of different parameters on the model

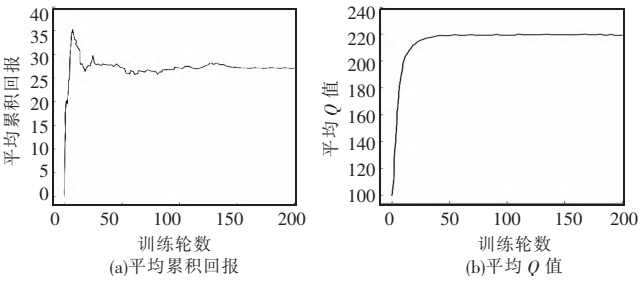

图 11 平均累积回报和 Q 值

Fig. 11 Average cumulative return and Q

在训练初期,平均累积回报波动较大,Q 值变化不稳定,表明模型处于探索阶段;随着训练进行,在大概 150 轮的时候 Q 值波动幅度减小,表明模型逐渐掌握最优防御策略,并且平均累积回报和 Q 值均进入平稳期,模型具备稳定的决策能力。该图验证了改进的 Dueling DQN 架构在动态防御任务中的收敛性和策略优化能力,为实际部署中的实时性与可靠性提供了保障。

为了量化分解后的近似张量对原始张量的还原能力,实验了不同分解秩下的重建比率:

$$1-\frac{\|\boldsymbol{\Gamma}-\hat{\boldsymbol{\Gamma}}\|_F^2}{\|\boldsymbol{\Gamma}\|_F^2}\times 100\% \tag{25}$$

式(25)表示分解后的近似张量 $\hat{\boldsymbol{\Gamma}}$ 对原始张量 $\boldsymbol{\Gamma}$ 的还原程度。如图 12 所示,重建率随 R 增加稳步上升,当 $R=10$ 时重建比率大于 80%,表明此时模型已经能够有效捕捉原始数据中的关键信息。同时为了避免过拟合,本文的秩选择了最小值 10。实验显示单次分解耗时约 50 ms(基于 Ubuntu 系统测试)。当攻击流量触发二级检测时,控制器需处理张量分解任务,导致 Packet-In 消息处理延迟增加,限制了控制器的实时性。此外,状态向量维度在分解秩为 10 时维度为 41,需通过全连接层计算状态价值 $V(s)$ 和动作优势 $A(s,a)$,单次决策耗时约 8 ms,主要消耗在神经网络前向传播。在训练阶段若采用实时更新策略网络,可能因经验回放缓存操作占用内存,导致控制器可用内存减少。研究当中通过级联触发机制显著降低了计

算负载。在数据平面仅计算 Packet-In 突发率、流量失衡度、流表熵值(式(1)~(3)),单次检测耗时小于 1 ms。动态决策中的成本惩罚强制模型优先选择低成本动作,实验显示:在控制器剩余资源 20% 时,系统降低分解频次,平均响应时间仍控制在 3.99 s。虽然智能算法引入额外开销,但通过轻量级触发 + 资源感知决策,在攻击检测率 99.61% 的前提下,保障了控制器核心功能的实时性。

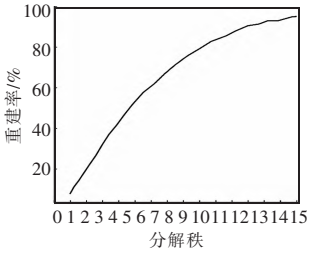

图 12　分解秩与重建率

Fig. 12　Decomposition rank and reconstruction rate

4　结束语

针对 SDN 中 DDoS 攻击检测存在的精度与资源效率失衡问题,本文提出基于多模态感知与深度强化学习的协同防御机制。有效解决传统方法对高并发合法流量的误判问题,实现了检测精度与防御成本的平衡。研究局限性在于实验主要依托仿真环境与公开数据集,真实网络中动态拓扑变化、设备异构性及复杂流量场景可能对张量分解稳定性和模型泛化能力提出更高要求。交换机流量数据需通过 OpenFlow 协议实时抓取,但不同交换机的硬件时钟偏差可能导致时间戳不一致。此外,数据包从物理层至应用层的处理延迟 20~50 μs,然而 SDN 控制器通过南向接口获取数据时,受限于 OpenFlow 协议的 Barrier 消息同步等交互机制,实际延迟可达 1~2 ms。当网络规模超过 100 台交换机时,NTP 同步误差可能导致跨节点数据时间戳偏差超过 10 ms,破坏张量分解的时空关联性。未来研究将聚焦于真实网络环境适配,验证系统在动态拓扑及混合攻击场景下的鲁棒性;同时探索与区块链、联邦学习等技术融合,进一步完善多模态特征体系。本文希望为构建智能、弹性的 SDN 动态防御体系研究能够起到一定的参考作用。

参考文献:

[1] 艾广锋. SDN 中基于无监督机器学习的 DDoS 检测系统研究[D]. 广州:华南理工大学,2021. (Ai Guangfeng. Research on DDoS detection system based on unsupervised machine learning in SDN[D]. Guangzhou:South China University of Technology,2021.)

[2] 王淑玲,李济汉,张云勇,等. SDN 架构及安全性研究[J]. 电信科学,2013,29(3):117-122. (Wang Shuling,Li Jihan,Zhang Yunyong,*et al*. Research on SDN architecture and security[J]. Telecommunications Science,2013,29(3):117-122.)

[3] Yuan Bin,Zhang Fan,Wan Jun,*et al*. Resource investment for DDoS attack resistant SDN:a practical assessment[J]. Science China Information Sciences,2023,66(7):172103.

[4] 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 Yuhua,Sun Zhixin. Research development of abnormal traffic detection in software defined networking[J]. Journal of Software,2020,31(1):183-207.)

[5] Zhao Kaixin,Lu Bo,Shi Hongyu,*et al*. A DDoS attack detection and defense mechanism based on the self-organizing mapping in SDN[J]. Internet Technology Letters,2024,7(1):e305.

[6] Jiménez-Lázaro M,Berrocal J,Galán-Jiménez J. Flow-based service time optimization in software-defined networks using deep reinforcement learning[J]. Computer Communications,2024,216:54-67.

[7] Aladaileh M A,Anbar M,Hintaw A J,*et al*. Effectiveness of an entropy-based approach for detecting low- and high-rate DDoS attacks against the SDN controller:experimental analysis[J]. Applied Sciences,2023,13(2):775.

[8] Puranik K,Patil K,Ghaligi G,*et al*. A two-level DDoS attack detection using entropy and machine learning in SDN[C]//Proc of the 3rd International Conference on Intelligent Technologies. Piscataway,NJ:IEEE Press,2023:1-7.

[9] Saiyed M,Al Anbagi I. Entropy and divergence-based DDoS attack detection system in IoT networks[C]//Proc of the 19th International Conference on Wireless and Mobile Computing,Networking and Communications. Piscataway,NJ:IEEE Press,2023:224-230.

[10] Shirsath V A,Chandane M M,Lal C,*et al*. Syntropy:TCP SYN DDoS attack detection for software defined network based on Rényi entropy[J]. Computer Networks,2024,244:110327.

[11] Khedr W I,Gouda A E,Mohamed E R. FMDADM:a multi-layer DDoS attack detection and mitigation framework using machine learning for stateful SDN-based IoT networks[J]. IEEE Access,2023,11:28934-28954.

[12] 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.

[13] Ali Setitra M,Fan Mingyu,Agbley B L Y,*et al*. Optimized MLP-CNN model to enhance detecting DDoS attacks in SDN environment[J]. Network,2023,3(4):538-562.

[14] Ranpara R,Patel S K,Kumar O P,*et al*. A computational framework for IoT security integrating deep learning-based semantic algorithms for real-time threat response[J]. Scientific Reports,2025,15:16794.

[15] 王小宇,贺鸿鹏,马成龙,等. 基于多模态神经网络流量特征的网络应用层 DDoS 攻击检测方法[J]. 沈阳农业大学学报,2024,55(3):354-362. (Wang Xiaoyu,He Hongpeng,Ma Chenglong,*et al*. Application layer DDoS attack detection method based on multimodal neural network traffic characteristics[J]. Journal of Shenyang Agricultural University,2024,55(3):354-362.)

[16] 许静. 基于张量模型的大规模 DDoS 攻击检测方法研究[D]. 昆明:云南大学,2023. (Xu Jing. Research on large-scale DDoS attack detection method based on tensor model[D]. Kunming:Yunnan University,2023.)

[17] Hill W,Acquaah Y T,Mason J,*et al*. DDoS in SDN:a review of open datasets,attack vectors and mitigation strategies[J]. Discover Applied Sciences,2024,6(9):472.

[18] 周奕涛,张斌,刘自豪. 基于多模态深度神经网络的应用层 DDoS 攻击检测模型[J]. 电子学报,2022,50(2):508-512. (Zhou Yitao,Zhang Bin,Liu Zihao. Application layer DDoS attack detection model based on multimodal deep learning neural network[J]. Acta Electronica Sinica,2022,50(2):508-512.)

[19] Lenhardt L,Zeković I,Dramićanin T,*et al*. Characterization of cereal flours by fluorescence spectroscopy coupled with PARAFAC[J]. Food Chemistry,2017,229:165-171.

[20] Maranhão J P A,da Costa J P C L,Javidi E,*et al*. Tensor based framework for distributed denial of service attack detection[J]. Journal of Network and Computer Applications,2021,174:102894.

[21] Gupta B B,Misra M,Joshi C R. An ISP level solution to combat DDoS attacks using combined statistical based approach[EB/OL]. (2012-03-12). https://arxiv.org/abs/1203.2400.

[22] Bhushan K,Gupta B B. Hypothesis test for low-rate DDoS attack detection in cloud computing environment[J]. Procedia Computer Science,2018,132:947-955.

[23] Wang Meng,Lu Yiqin,Qin Jiancheng. A dynamic MLP-based DDoS attack detection method using feature selection and feedback[J]. Computers & Security,2020,88:101645.

[24] Hou Liangshao,Chu Delin,Liao Lizhi. Convergence of a fast hierarchical alternating least squares algorithm for nonnegative matrix factorization[J]. IEEE Trans on Knowledge and Data Engineering,2024,36(1):77-89.

[25] Wang Jin,Wang Liping. LR-STGCN:detecting and mitigating low-rate DDoS attacks in SDN based on spatial-temporal graph neural network[J]. Computers & Security,2025,154:104460.

[26] 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.

[27] Xia Shiming,Zhang Lei,Bai Wei,*et al*. DDoS traffic control using transfer learning DQN with structure information[J]. IEEE Access,2019,7:81481-81493.

[28] Yao Yuan,He Junjiang,Li Tao,*et al*. An automatic XSS attack vector generation method based on the improved dueling DDQN algorithm[J]. IEEE Trans on Dependable and Secure Computing,2024,21(4):2852-2868.

[29] Wu Yali,Hu Yanghu,Wang Junhu,*et al*. An active learning framework using deep Q-network for zero-day attack detection[J]. Computers & Security,2024,139:103713.