分类号:　　学校代码：10389

密　级:　　学　　号：52311050006

福建农林大学

硕士学位论文

（专业学位）

面向 SDN 的 DDoS 多模态感知与资源感知 DRL 协同防御方法研究

学习形式：全日制

学位类别：电子信息硕士专业学位

专业领域：网络与信息安全

研究方向：软件定义网络及其安全机制

学生姓名：徐泽鹏

指导教师：舒兆港 副教授

完成时间：二〇二六年四月

A Study on a Collaborative DRL Defense Method for SDN-Oriented DDoS Attacks with Multimodal and Resource-Aware Capabilities

By

Zepeng Xu

Supervised by Associate Professor Zhaogang Shu

A Thesis Submitted to

Fujian Agriculture and Forestry University

in Partial Fulfillment of the Requirements

for

Professional Master's Degree in Electronic Information

College of Computer and Information Science

Fujian Agriculture and Forestry University

Fujian, P.R. China

Completion Date (April 13，2026)

Commencement Date (December 13，2024)

独创性声明

本人声明，所呈交的学位（毕业）论文，是本人在指导教师的指导下独立完成的研究成果，并且是自己撰写的。尽我所知，除了文中作了标注和致谢中已作了答谢的地方外，论文中不包含其他人发表或撰写过的研究成果。与我一同对本研究做出贡献的同志，都在论文中作了明确的说明并表示了谢意，如被查有侵犯他人知识产权的行为，由本人承担应有的责任。

学位（毕业）论文作者亲笔签名：徐泽鹏　　日期：2026年5月30日

论文使用授权的说明

本人完全了解福建农林大学有关保留、使用学位（毕业）论文的规定，即学校有权送交论文的复印件，允许论文被查阅和借阅；学校可以公布论文的全部或部分内容，可以采用影印、缩印或其他复制手段保存论文。

延期公开，在　　年后可适用本授权书。 □

公开，本论文属于不延期公开论文。 ☑

学位（毕业）论文作者亲笔签名：徐泽鹏　　日期：2026年5月30日

指导教师亲笔签名：　　日期：2026年5月30日

目 录

图 录

表 录

摘 要

随着软件定义网络（Software Defined Networking，SDN）的广泛部署，集中式控制架构在提升网络可编程性与管理灵活性的同时，也使控制平面处理能力与交换机流表资源在分布式拒绝服务（Distributed Denial of Service，DDoS）攻击下更易成为性能瓶颈。针对 SDN 场景中 DDoS 攻击流量来源分散、时空特征高度耦合以及现有方法难以兼顾检测精度与实时性的问题，本文围绕时间、空间、流量特征、控制器资源四类模态的攻击感知与智能防御决策协同优化主线，研究面向 SDN 的 DDoS 检测与防御一体化方法。

面向 SDN 流表与控制平面交互特性，本文构建多模态时空流量张量表示方法，在统一框架下对时间、空间与特征维度进行结构化建模，并引入平行因子分析（Parallel Factor Analysis，PARAFAC）张量分解对高维流量特征进行低秩近似与显式解耦，以提取具有可解释性的时空交互因子，从而增强对多源协同、时序突发及特征隐蔽等攻击结构特性的表达能力。为解决检测结果与防御策略相互割裂的问题，本文将张量分解得到的结构化时空表征作为强化学习的状态输入，基于 Dueling DQN 构建防御决策模型，使智能体能够在不同攻击态势下自适应选择重定向、限速与封禁等防御动作，形成检测表征、决策优化与执行反馈相结合的闭环协同机制。进一步地，面向工程部署中控制器资源受限与网络负载动态变化等约束，本文提出资源感知的防御优化方法：在感知阶段采用增量式 PARAFAC 分解对新增流量数据进行局部更新，避免历史数据重复计算，从而降低在线分解开销；在决策阶段将控制器 CPU 与内存等资源状态纳入状态空间，并在奖励函数中引入资源代价与开销惩罚项，实现防御效果与系统开销之间的自适应权衡。实验结果表明，增量式分解的单次计算耗时可控制在 8ms 以内，且增量更新因子矩阵与全量分解结果的相似度超过 95%，能够满足在线决策的实时性需求。

基于 CIC-DDoS2019 数据集构建 SDN 仿真拓扑环境开展实验评估。结果显示，本文方法在 5 折交叉验证条件下取得稳定的检测性能，并在误封率对比实验中表现出更好的误识别控制能力，最大误封率不超过 0.5%。

关键词：软件定义网络；分布式拒绝服务攻击；深度强化学习；张量分解

ABSTRACT

With the widespread deployment of Software-Defined Networking (SDN), centralized control architectures—while enhancing network programmability and management flexibility—also make control plane processing capacity and switch flow table resources more susceptible to becoming performance bottlenecks during Distributed Denial of Service (DDoS) attacks. Addressing the challenges in SDN scenarios—such as the dispersed origins of DDoS attack traffic, highly coupled spatiotemporal characteristics, and the difficulty of existing methods in balancing detection accuracy with real-time performance—this paper explores an integrated DDoS detection and defense method for SDN. The research focuses on the coordinated optimization of attack detection and intelligent defense decision-making across four modalities: time, space, traffic features, and controller resources.

Given the interaction characteristics between SDN flow tables and the control plane, this paper constructs a multimodal spatiotemporal traffic tensor representation method. Within a unified framework, it performs structured modeling across temporal, spatial, and feature dimensions, and introduces PARAFAC tensor decomposition to perform low-rank approximation and explicit decoupling of high-dimensional traffic features. This approach extracts interpretable spatiotemporal interaction factors, thereby enhancing the ability to capture attack structural characteristics such as multi-source coordination, temporal bursts, and feature obfuscation. To address the disconnect between detection results and defense strategies, this paper uses the structured spatiotemporal representations obtained from tensor decomposition as state inputs for reinforcement learning. Based on Dueling DQN, a defense decision-making model is constructed, enabling the agent to adaptively select defense actions—such as redirection, rate limiting, and blocking—under different attack scenarios, thereby forming a closed-loop collaborative mechanism that integrates detection representation, decision optimization, and execution feedback. Furthermore, addressing constraints such as limited controller resources and dynamic network load changes in engineering deployments, this paper proposes a resource-aware defense optimization method: during the perception phase, an incremental PARAFAC decomposition is used to perform local updates on new traffic data, avoiding redundant calculations of historical data and thereby reducing the overhead of online decomposition; during the decision-making phase, the state space incorporates controller resources such as CPU and memory, and the reward function includes resource cost and overhead penalty terms, achieving an adaptive trade-off between defense effectiveness and system overhead. Experimental results show that the computation time for a single incremental decomposition can be controlled within 8 ms, and the similarity between the incrementally updated factor matrix and the full decomposition results exceeds 95%, meeting the real-time requirements for online decision-making.

Experimental evaluations were conducted using an SDN simulation topology built on the CIC-DDoS2019 dataset. The results show that the proposed method achieves stable detection performance under 5-fold cross-validation and demonstrates superior false positive control capabilities in comparison experiments, with a maximum false positive rate not exceeding 0.5%.

KEY WORDS: Software-Defined Networking; Distributed Denial-of-Service Attack; Deep Reinforcement Learning; Tensor Decomposition

1 绪论

1.1 研究背景和意义

随着互联网规模持续扩张以及云计算、数据中心、物联网与 5G/6G 等应用快速落地，网络业务呈现出高并发、强动态与多样化服务质量（Quality of Service, QoS）需求并存的特征[1]。传统网络依赖防火墙、网络地址转换（Network Address Translation, NAT）、负载均衡（Load Balance, LB）等专用硬件实现功能，网络服务与硬件设备紧耦合，标准不统一导致配置灵活性受限、运维复杂且成本较高，硬件设备需要预留大量峰值性能冗余，资源利用率低下，云清洗服务则按流量计费，大规模攻击时带宽成本呈指数级增长。难以适应快速变化的新业务需求与弹性扩展要求。网络功能虚拟化（Network Functions Virtualization, NFV）通过将网络功能软件化并运行在通用计算平台上，可显著降低资本性支出与运营性支出并提升资源利用率，但同时也带来了网络编排复杂度上升的问题；因此需要借助 SDN 的集中控制与可编程能力，将 NFV 通过服务功能链（Service Function Chain, SFC）动态编排，以实现网络资源的按需调度与服务的快速部署[2]。

然而，SDN 可编程网络技术在带来灵活性的同时，也引入了新的安全挑战。SDN 采用集中式控制架构，控制器负责全局网络视图维护与策略决策，数据平面依赖流表规则完成转发[3]。一旦控制平面遭受异常流量冲击，控制器计算能力、南向交互能力以及交换机流表容量将更易成为性能瓶颈与攻击目标。在大规模异常流量场景下，控制器与交换机侧的流表容量、表项更新频率以及控制平面消息处理能力，都会因负载激增而显著受限，从而影响网络服务质量与稳定性[4]。在众多安全威胁中，DDoS 攻击因成本低、破坏性强、易于规模化而长期处于高发态势。DDoS 攻击通常通过多源协同持续消耗目标网络带宽、计算与存储资源，使合法用户无法获得正常服务。与传统网络相比，SDN 环境下 DDoS 攻击可能进一步利用“新流触发—控制器交互—规则下发”的链路放大影响：一方面，Packet-In 消息洪泛会显著增加控制器的南向消息处理与规则下发开销，导致控制平面排队与策略执行迟滞；另一方面，频繁的新流触发会造成交换机侧表项膨胀与更新，导致端口统计分布与流表熵值发生漂移，从而削弱基于固定阈值或单一统计特征的检测与防御效果[5]。

围绕 SDN 场景的 DDoS 检测与防御，近年来研究的主要方向包括基于熵、统计特征的快速异常感知、机器学习的细粒度分类、以及强化学习驱动的缓解决策等[6]；并进一步出现“跨平面协同、任务卸载、快速数据路径”等工程化思想，以提升防御及时性并降低控制器 CPU 消耗[7]。同时，也有研究通过强化学习实

现更智能的缓解决策，强调在动态环境下提高合法流量留存率与系统自适应性[8]。这些工作为 SDN 环境下的 DDoS 防护奠定了基础，但现有方法仍存在三类关键不足，制约其在复杂动态网络中的适用性与可部署性。第一，攻击流量时空协同结构缺乏显式建模，DDoS 攻击本质上表现为多个源节点在特定时间窗口内以相似或协同流量特征对目标持续请求，但多数检测方法仍将不同时间窗口或不同源 IP 的流量视为独立样本，或采用简单特征拼接，难以在模型层面显式刻画时间演化、空间分布与流量特征之间的协同关系；在隐蔽型或低速率持续演化的攻击场景下，检测稳定性与泛化能力不足。第二，检测结果与防御决策缺乏闭环协同机制。现有研究常将检测与防御作为相对独立阶段，检测输出多以告警或二值标签呈现，难以为后续防御策略提供结构化信息支撑；防御策略依赖预定义规则或静态阈值触发，难以根据攻击强度、网络状态及资源消耗动态调整，易产生误封或响应滞后，影响服务质量与系统稳定性。第三，工程可部署性不足与资源约束未被系统性建模。在真实部署中，控制器资源受限与负载动态变化是决定系统能否在线运行的关键约束，若仅追求检测精度而忽略在线计算成本，将难以在实际网络中稳定落地。

鉴于此，本研究将问题聚焦于“面向防御效能的 DRL 决策优化与资源动态调度”。相较于当前产业界使用的防火墙、流量清洗设备而言，本文方法直接部署于 SDN 控制器，纯软件实现复用现有网络资源，无需额外硬件投入。深度利用控制平面全局信息，基于资源感知 DRL 实现了防御策略的动态优化，能够根据攻击强度和系统负载自适应选择最优防御动作，避免“防御性宕机”。其核心思路是：一方面用结构化建模显式刻画攻击的时空协同特征，另一方面将结构化特征直接服务于防御决策，实现检测—决策闭环，并针对资源约束给出可部署的优化机制。

1.2 研究现状

在过去的几年中，围绕 SDN 场景下 DDoS 攻击的检测与防御问题，国内外研究主要聚焦两条主线：其一是面向控制平面与数据平面的高精度、低开销攻击检测[9]；其二是兼顾 QoS 与资源约束的防御与缓解决策[10]。近年来，研究趋势由“单一特征/静态规则”逐步转向“多模态结构化建模和闭环自适应决策”，张量建模、图神经网络与深度强化学习等方法得到广泛关注[11-13]。

1.2.1 面向 SDN 的 DDoS 攻击检测方法研究现状

基于传统机器学习与特征工程的检测方法。Santos 等人在 SDN 仿真环境 Mininet 中部署多种机器学习算法对 DDoS 攻击进行分类检测，通过 Scapy 工具

结合有效 IP 地址列表模拟生成 DDoS 攻击流量，实验显示随机森林算法的检测准确率表现最优，决策树算法则拥有最快的处理速度[14]。Madoune 等人利用主成分分析和分布式随机邻域嵌入的两阶段降维过程，有效地捕获了网络流量中的线性和非线性模式。通过 K-Means 聚类进一步实现特征增强，从而提高模型性能[15]。Perez-Diaz 等人基于超参数调优增强机器学习模型在识别 DDoS 攻击方面的性能[16]。Chen 等人提出了一种使用自动特征提取和选择来检测 DDoS 攻击的智能代理系统，动态检测 DDoS 攻击流量时选择最佳特征并重构 DDoS 检测代理[17]。该类方法实现简单、易部署，但多采用向量化统计特征，难以显式刻画攻击在时间演化、空间分布与多维特征之间的高阶耦合关系。

面向低速与隐蔽攻击的深度学习检测方法。Abu 等人提出了一种灵活的模块化架构，使用多种机器学习模型在架构中训练入侵检测系统，可以识别和缓解 SDN 设置中的 LR-DDoS 攻击[18]。Prabhu 等人通过过滤恶意流量最大限度地减少控制器的计算和存储开销，能够高效检测 SDN 环境中的 LR-DDoS，并结合了并行混合注意力机制模块进行流分类，通过评估多种特征分析合法流，成功区分合法流和恶意流[19]。Sun 等人通过从流规则中提取字段，构造平均包数和字节数作为混合模型的输入数据，在训练过程中自动优化超参数，分别提取输入数据的更深层次的空间和时间特征[20]。Omer 等人将时间序列学习与特征细化相结合，利用混合长短期记忆前馈神经网络来应对检测低速率[21]。上述方法在复杂模式识别方面具有优势，但在 SDN 在线环境仍需进一步权衡控制器算力/时延约束，并思考如何将检测输出有效服务于后续防御决策。

基于图结构与动态建模方法。Li 等人通过攻击溯源知识库的构建流程，设计域内攻击图和溯源算法推荐图，解决 DDoS 攻击路径溯源和最优溯源方案推荐问题，实现子图采样算法 Tracing-Sample 适应域内 DDoS 攻击溯源，高效利用知识库中的图结构重现 DDoS 攻击路径[22]。Biradar 等人通过对网络事件的顺序分析有效地捕获时间动态。与传统的机器学习方法和独立的深度学习模型相比，所提出的混合模型在多个评估指标上取得了卓越的性能[23]。Lyu 等人使用层次图结构来跟踪主机、子网和自治系统三个级别的 DNS 流量，并结合识别层次结构各个级别的异常行为的机器学习[24]。Wang 等人基于结构平衡图理论，针对代理之间的复杂行为，同时考虑代理之间的合作和对抗交互，引入内部动态变量减少了触发次数并节省资源[25]。该类研究说明显式建模通信关系有助于捕获协同攻击中的结构特征，但图构建与在线更新机制也带来额外的计算与工程复杂度。

基于张量化建模与高维数据降维去噪方法。Fan 等人提出 IDAD 框架，将大规模异构网络数据张量化建模，并给出改进与分布式张量列车分解去噪算法，结合 LightGBM 实现 DDoS 检测，在 CIC-DDoS2019 与 NSL-KDD 上达到极高准确率，同时具备低存储开销与较好的加速比[26]。Li 等人提出 TLanczos-TSVD 降维

去噪算法，将高维网络数据表示为张量并进行截断 Lanczos-TensorSVD，再结合 XGBoost 构建检测框架，在保证实验中的准确率同时，在不同规模数据集上表现出较强鲁棒性与低资源消耗[27]。此外，Ekle 等人面向流式动态图边异常检测提出通过多层张量 sketching、Count-Min Sketch 与时间衰减实现轻量级实时异常评分，展现大规模流式数据下的吞吐能力与内存可控性[28]。Tebbaa 等人基于 PRISMA 对 SDN 场景下 ML/DL/混合方法指出真实部署面临的数据集偏差、在线可扩展性与控制器负载等挑战[29]。总体而言，张量相关方法能够保留多维结构信息并挖掘高阶相关性，但多数仍停留在“张量降维—分类判别”的两阶段范式，缺少与后续防御策略学习共享的统一状态表示。

1.2.2 面向 SDN 的 DDoS 攻击缓解方法研究现状

基于资源管理策略。Kabdjou 等人利用网络欺骗指标，包括请求收集率随时间变化以及不同僵尸网络规模下请求次数的差异处理 QoS 参数，利用均匀分布和随机选择的网络欺骗策略，以转移潜在攻击者的注意力[30]。王涛等人根据用户信任值将流请求分类并将其划分到具有不同优先级的多个缓冲队列，然后使用 SDN 控制器以双轮询机制来调度处理这些流请求，并用多控制器动态调度策略来降低全局响应时间[31]。Kumar 等人提出了一种结合带宽限制和资源保留策略并结合容器化的双线防御系统，根据目标网络服务在特定时刻的连接数量将来电请求分离和限制向目标网络服务传输请求的中间设备带宽[32]。

基于 DRL 的缓解决策。Janakiraman 等人提出了基于深度强化学习 DRL 和长短期记忆的 DDoS 攻击缓解方案，用于处理雾辅助云计算环境中 DDoS 攻击的影响；SDN 用于在控制器中部署防御模块，以识别传输层或网络层 DDoS 攻击的异常特征。它通过执行网络流量分析来帮助过滤和转发合法数据包，同时规避受感染数据包引起的攻击[33]。Ji 等人提出了一种用于连接顺序优化的动态 DDQN 顺序选择方法；该方法首先将连接查询建模为马尔可夫决策过程，然后通过将网络模型 DQN 和 DDQN 权重集成到 DRL 模型在查询连接中的估计误差问题中解决 DRL 模型，最终提高开发查询的质量计划[34]。这些工作为进一步引入价值——优势分解结构提升学习效率提供了理论与工程启发。

主动防御与多智能体趋势。Dong 等人提出 Poseidon 框架，将（Moving Target Defense, MTD）与欺骗防御结合，使得对高速率分布式拒绝服务和低速率分布式拒绝服务攻击都能做出差异化的响应；利用集装箱的轻便特性，实现了资源高效的保护[35]。Aydin 等人提出了一个 IIoT 网络防御系统，该系统将深度强化学习的敏感性与多代理系统的敏捷性相结合，为 DDoS 攻击提供自主防御解决方案 NS-IoT 系统对于检测模块，开发了基于深度 Q 网络的代理来检测 DDoS 攻击，利用反馈来改进马尔可夫决策过程中的决策，并结合奖励以提高性能[36]。该类研

究拓展了防御策略空间，但也使状态表达与代价函数设计更复杂，对结构化状态建模提出更高要求。

多域协作与协同防护。Feng 等人提出了一个两级检测框架，用于多域场景中的协作 DDoS 攻击检测包括基于 Rényi 熵算法的一级粗粒度异常检测方法和基于混合深度学习模型的 DCNN-LSTM 算法作为二级检测方法[37]。Chen 等人提出了一种基于多域协作的实时 DDoS 防御框架，在源端部署有效的防御对策[38]。冯惠粉等人围绕多域协作式 DDoS 防御，从协同检测、溯源与缓解、动态拓扑路径选择等方面构建多层次机制，强调多域环境下攻击来源多样与隐蔽性增强导致防御难度显著提升[39]。朱海婷等人提出异步个性化联邦学习，通过定制 ResNet 结构处理一维流量数据，并引入个性化聚合与异步机制以适应 Non-IID 数据与异构设备条件，同时集成缓解系统应对多样化攻击场景，实验表明该方法在多个数据集上具有更快收敛与更强鲁棒性[40]。

1.2.3 研究现状小结

综合上述研究可以看出，当前 SDN 场景下 DDoS 检测与防御已形成机器学习、信息熵、资源控制、张量分解和其他技术等较为丰富的技术谱系。在防御侧则呈现从 SFC 闭环优化、DRL 保障 QoS 的自适应缓解到主动防御与多智能体协作以及多域与联邦学习协同防护的发展趋势。张量方法多用于离线降维去噪服务分类器，多模态结构化状态表达不足。而 DRL 防御多使用低维统计向量作为状态输入，缺少统一张量化状态空间融合流量、流表与资源信息。与研究目标为隐式学习流量的局部统计特征用于分类的 CNN 流量特征提取方法和隐式学习流量序列的全局长程依赖用于分类的 Transformer 多维度行为建模方法不同，本文通过显式解耦攻击的时空协同结构，提取可解释的基础模式。CNN 方法过卷积核提取局部特征，但无法显式刻画“多个 IP 在同一时间窗口协同攻击”的全局结构；Transformer 方法通过自注意力机制计算任意两个时间步的关联，但时间与空间维度被混合在 token 中，无法分离“哪些 IP 在什么时间发起了攻击”；而本文通过“时间-IP-特征”三阶张量完整保留攻击的多源协同与时序突发特性，避免了扁平化处理导致的高阶关联丢失。此外，检测与缓解多为串联式设计，检测输出难以直接驱动策略学习并进行联合优化，检测—决策闭环协同不足[41-44]。虽然 DQN 已验证其稳定性优势，动态 DQN 等工作对过估计与探索提出改进思路，但与张量化状态表征结合、并进一步引入价值—优势分解结构以提升学习效率的研究仍较少，DQN 体系的稳定性与效率仍需增强。

因此，构建“基于张量建模的多模态状态表示的深度强化学习策略优化”的统一框架，有望在保证检测精度的同时提升策略学习稳定性与在线部署可行性，并实现检测—防御闭环的系统级优化，这也为本文后续章节的研究内容与技术路

线提供了依据。

1.3 研究目标和研究内容

针对现有 SDN 场景下 DDoS 攻击检测与防御方法在时空协同建模不足、检测与防御割裂以及资源感知能力有限等问题，本文围绕“多模态攻击感知—智能防御决策协同优化”主线，构建面向 SDN 的 DDoS 检测与防御一体化方法。总体上形成“轻量化感知—结构化表征—智能决策—执行反馈”的闭环流程，在保证检测精度的同时兼顾在线实时性与控制器资源约束。

1.3.1 研究目标

本文的研究目标是在兼顾检测精度与系统开销的前提下，针对 SDN 场景中 DDoS 攻击流量时空特征复杂、检测与防御过程割裂以及工程部署受限等问题，构建一种多模态感知与智能决策协同的 DDoS 防御方法。具体目标包括：

(1) 显式刻画 DDoS 多源协同与时序突发特性，输出具备可解释性的时空因子表征，为后续检测与决策提供统一状态描述；

(2) 设计低秩分解的细粒度检测机制，在保持检测稳定性与泛化能力的同时降低高维建模开销，能够有效识别洪泛型与低速隐蔽型攻击；

(3) 构建检测—防御协同的深度强化学习决策模型，将结构化时空表征映射为可执行防御动作，实现重定向、限速、封禁等策略在不同攻击强度与业务压力下的自适应选择，降低误封并保障服务质量；

(4) 面向资源受限与负载动态场景，优化机制，缓解端到端检测—决策流程在线防御的时延。

1.3.2 研究内容

围绕上述研究目标，本文主要开展以下研究工作：

(1) SDN 场景下 DDoS 攻击多模态时空特征建模。充分利用 SDN 控制器对网络全局状态的感知能力，从流量统计特征、时间演化特征与空间分布特征三个维度出发，对网络流量进行结构化建模，构建多维时空张量表示攻击流量在不同时间窗口、不同源节点及多维特征空间中的变化规律，为后续攻击检测与防御决策提供统一的数据表达基础。同时设计轻量化统计监测与触发策略，减少高复杂度建模的无效调用。

(2) 基于张量分解的结构化表征提取与攻击检测。针对高维时空张量数据计算复杂度高、直接分析困难的问题，引入 PARAFAC 张量分解思想对多模态时空

张量进行低秩近似表示，挖掘流量数据中的潜在结构特征，实现对正常流量模式与异常攻击行为的有效区分。

(3) 检测—防御闭环协同框架设计。针对现有研究中攻击检测与防御策略相互独立的问题，构建以检测结果驱动防御决策的协同框架，将攻击检测阶段提取的结构化时空特征作为防御决策的重要输入，定义防御动作空间及其 SDN 可执行映射，形成“检测输出—策略学习—流表执行—反馈更新”的闭环协同机制。

(4) 资源感知的深度强化学习防御决策与动态调度。将 DDoS 防御过程建模为马尔可夫决策过程，引入资源感知的深度强化学习方法，在状态空间中综合考虑攻击态势信息与控制器资源状态，建立防御效果与资源代价的权衡模型；进一步研究增量式张量分解降低在线计算开销，以及模型轻量化以提升推理效率。

上述研究工作的展开，旨在方法层面实现多模态时空结构化表征与 DRL 决策的统一建模，在系统层面实现检测与防御协同闭环，并在工程层面面向资源受限条件给出可部署的优化策略。

1.4 论文章节安排

本文围绕 SDN 场景下 DDoS 攻击的检测与防御问题展开研究，遵循“问题分析—方法设计—机制优化—实验验证”的技术路线，对多模态攻击感知与智能防御决策协同机制进行了系统研究。全文共分为五章，其中，第三章侧重方法可行性验证，第四章进一步引入资源约束条件，对工程部署场景下的防御策略进行优化。具体论文结构如图 1-1 所示。

第一章：绪论。本章介绍论文的研究背景与研究意义，分析 SDN 环境下面临的 DDoS 攻击安全挑战，系统梳理国内外在 SDN 场景下 DDoS 攻击检测与防御方面的研究现状，总结现有研究的不足与挑战，明确本文的研究目标、研究内容及主要创新点，并给出全文的章节结构安排。

第二章：相关理论。本章对本文研究中涉及的基础理论与关键技术进行介绍，包括 SDN 体系结构与工作机制、DDoS 攻击的基本原理及流量特征、张量建模与张量分解理论，以及深度强化学习的基本原理与典型模型，为后续章节中攻击检测与防御方法的设计提供理论支撑。

第三章：基于多模态时空表征与 DRL 协同决策的 DDoS 检测与防御方法。本章在默认控制器计算资源相对充足的条件下，重点研究 SDN 场景中 DDoS 攻击的高精度感知与检测问题。首先分析攻击流量在时间演化、空间分布及统计特征维度上的协同特性，构建多模态时空流量表示模型；在此基础上，设计基于 PARAFAC 张量分解的细粒度攻击检测方法，实现对攻击时空特征的显式解耦；进一步引入深度强化学习机制，构建检测与防御协同的决策框架，并通过仿真实

验验证所提方法可行性。

第四章：面向资源约束的 DDoS 防御决策优化与轻量化动态调度方法。针对实际部署中 SDN 控制器资源受限、网络负载动态变化等工程约束条件，在实际 SDN 网络环境中，控制器计算资源有限且网络负载具有显著动态性。第三章在假设资源相对充足的条件下验证了多模态感知与协同防御机制的可行性，但尚未充分考虑资源受限场景下的计算开销与实时性约束。因此，本章在引入资源约束条件的前提下，围绕防御效能与系统开销之间的权衡关系，研究面向工程部署场景的防御决策优化与资源动态调度方法。通过引入增量式张量分解方法降低在线计算开销，在深度强化学习决策过程中融入资源感知机制，实现防御动作对攻击强度与系统资源状态的动态自适应；同时结合模型轻量化与加速策略，提升防御系统在资源受限环境下的实时性与稳定性，并通过仿真实验对防御效能与系统开销进行验证与分析。

第五章：本章对全文研究工作进行总结，归纳本文在 SDN 场景下 DDoS 攻击检测与防御方面的主要研究成果与创新点，分析研究过程中存在的不足，并对未来可能的研究方向进行展望。

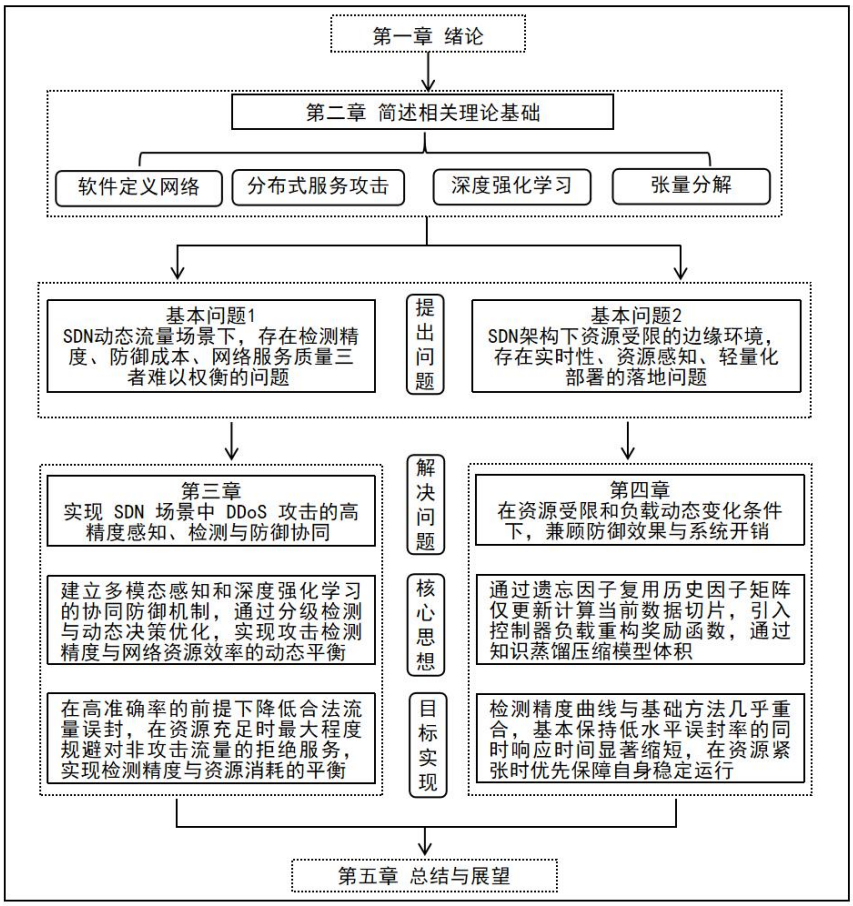


图 1-1 论文的组织结构与章节安排

2 相关理论

本章围绕本文研究中涉及的关键理论与技术基础展开阐述，重点介绍 SDN 体系结构、DDoS 攻击基本原理与特征、张量建模与分解理论以及深度强化学习的基本思想，为后续章节中检测与防御方法的设计与实现奠定理论基础。

2.1 软件定义网络

SDN 以“控制与转发分离”为设计核心，将网络设备中的控制平面从数据平面解耦，形成“控制器集中决策、交换机按规则转发”的运行机制。传统网络的各类设备中内置分布式控制逻辑（如路由选择、策略转发、链路状态维护等），需依赖多种协议在设备间协同，才能完成全网收敛与策略落地[45]；而 SDN 将控制逻辑上移至控制器，使其能以全局视角维护网络拓扑、链路状态、主机可达性及关键性能指标等信息，并据此统一生成转发与管理策略，下发至数据平面执行。得益于策略制定与实施路径的简化清晰，SDN 在网络可编程、自动化运维及策略一致性方面优势显著：一方面，网络行为由可编程接口驱动，便于快速部署新业务与新策略；另一方面，控制器可统一编排全网资源，实现链路利用率优化、业务分流、QoS 保障等精细化管理，同时为网络测量、异常分析及安全机制提供统一的数据与执行入口。

典型 SDN 采用“三层体系结构”如图 2- 1 所示。应用层承载各类网络应用与业务逻辑，涵盖路由优化、负载均衡、访问控制、流量工程及安全检测等功能模块。应用层不直接操作底层设备，而是通过控制层提供的抽象能力编程：应用将业务需求转化为可理解的策略或意图（如“某业务流量低时延优先、某类流量限速、某主机仅可访问特定服务”等），控制层再将这些策略转换为可执行的网络规则。控制层由 SDN 控制器及其核心服务组件构成，可视为“网络操作系统”，负责网络状态维护与资源管理，包括拓扑发现与更新、主机发现、链路状态监测、路径计算、策略编排、冲突检测及规则下发等。数据层由可编程交换机或转发设备组成，依据控制器下发的流表规则，执行报文处理与转发，实现业务流的精细化控制。其核心价值在于将网络从传统的“设备驱动模式”转向“软件与策略驱动模式”。SDN 通过分层设计，将业务逻辑（应用层）、控制逻辑（控制层）与转发逻辑（数据层）彻底分离，使得网络的控制权集中到控制器，应用程序可通过编程灵活定义网络功能，业务部署无需依赖硬件升级，只需修改控制策略即可快速实现，大幅降低了网络部署和运维的成本，提升了网络的灵活性、可扩展性

和可管理性，为云计算、大数据、物联网等新兴技术的发展提供了坚实的网络支撑。

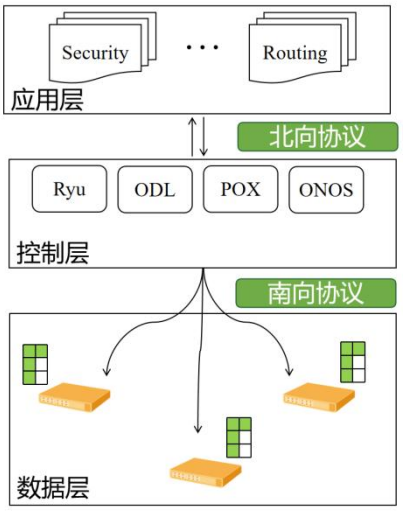


图 2-1 经典 SDN 体系架构

接口机制是 SDN 实现分层解耦与能力开放的关键。北向接口为应用层提供统一编程接口，支持以“意图/策略”描述业务需求，让开发者无需关注底层硬件细节，即可完成网络功能编排，其核心特点是抽象化与可组合性。南向接口连接控制器与数据平面设备，负责规则下发、状态上报及事件通知等交互，其中 OpenFlow 是最具代表性的南向协议。基于 OpenFlow，控制器与交换机通过控制信道交互：当交换机本地流表未命中时，会将匹配信息与首包封装为 Packet-In 消息上报控制器[46]；控制器结合网络状态与应用策略决策，生成转发表项并通过 Flow-Mod 消息下发，定义该类流量的转发行为；此外，控制器可通过 Stats-Request 等统计查询机制，获取端口、队列、流表项计数等信息，结合遥测指标构建细粒度网络画像，为路径优化、拥塞控制及业务质量保障提供数据支撑。多控制器场景下，东西向接口可实现控制器间拓扑、策略、会话状态的同步，保障全局一致性与高可用运行。

流表是 SDN 数据平面执行策略的核心，也是实现“按流精细化控制”的基础。典型 OpenFlow 交换机采用多级流水线结构，每级表包含若干表项，每条表项通常由匹配域、优先级、计数器及动作集合组成。匹配域覆盖二至四层多维字段，可对不同粒度流量分类；动作集合定义报文处理方式，包括转发、丢弃、修改报文头、限速等，实现路径控制与流量管理一体化。控制器规则安装分为主动式与反应式：主动式在业务启动前预先下发规则，降低时延、提升转发确定性；反应式在流量到达且流表未命中时按需下发，适配动态业务与突发流量。工程中常通过规则聚合、分层统计等机制，提升规则管理效率与可维护性。

总体而言，SDN 通过控制与转发解耦、全局集中控制及开放接口体系，实

现了网络从“硬件设备驱动”向“软件与策略驱动”的转型。其三层架构与南北向接口使网络能力可抽象、可编程、可自动化编排，流表与流水线转发模型则提供了精细化管控基础，为网络高效管理、业务创新及安全保障奠定了技术底座。

2.2 DDoS 攻击

DDoS 攻击是指攻击者控制大量受感染主机或滥用开放服务节点，在短时间内向目标持续发送异常请求，使目标的带宽、连接状态、CPU 与内存等关键资源被快速消耗，进而导致合法用户请求超时、丢弃或服务不可用[47]。相较于单点 DoS，DDoS 的本质在于“多源协同+规模化放大”：攻击流量由大量分散源同时发起，既提升攻击强度，也使过滤与溯源更复杂。典型攻击链路通常由“攻击者—C2 控制基础设施—僵尸网络—受害目标”构成，攻击者通过恶意程序感染终端形成僵尸网络，并经由 C2 下发攻击指令；僵尸主机按统一节奏或分批策略产生攻击流量，形成持续压制。

按协议层与利用方式不同，DDoS 一般可分为三类。第一类为容量型洪泛攻击，目标是占满链路带宽或上游转发能力，常见形式包括 UDP Flood、ICMP Flood 以及反射、放大型攻击。反射/放大攻击利用无连接或弱认证协议的“请求—响应”不对称性：攻击者伪造源地址为受害者并向开放服务器发送小请求，诱使其向受害者返回更大的响应，从而以较小代价获得流量放大，典型协议包括 DNS、NTP、CLDAP、SSDP 等。第二类为协议型资源耗尽攻击，主要消耗协议栈状态或中间设备的会话资源，例如 TCP SYN Flood 通过大量半连接占用 SYN 队列与连接跟踪表，导致正常连接建立受阻。第三类为应用层攻击，攻击请求在语义上更接近正常业务（如 HTTP GET/POST、HTTPS 握手、DNS 高频查询等），但通过高并发、慢速传输或热点资源访问使后端线程池、数据库连接与缓存系统长期高负载，从而在较低总流量下仍造成明显服务退化。

从流量与统计角度，DDoS 攻击通常具有以下特征：

（1）突发性与非平稳：攻击启动或强度切换时，单位时间包速率、字节速率与新流速率出现阶跃式上升，时间序列的均值、方差与峰度显著偏离基线。

（2）连接/新流异常增长：针对 TCP 或需状态维护的服务，连接建立请求数与短生命周期流占比上升，表现为 Flow Packets/s、Fwd/Bwd Packets/s 增大，而平均流持续时间、IAT（Inter-Arrival Time）均值与方差收缩。

（3）分布特征变化：多源攻击会使源 IP、源端口组合更离散，源地址熵、端口熵等指标在窗口内出现明显漂移；反射型攻击则呈现“源集中于反射器集合、目的高度集中”的结构性分布。

（4）报文与字段模式：UDP/ICMP 洪泛常见“小包高频”，包长均值下降

且包长方差/方差熵变化；SYN Flood 在标志位统计上表现为 SYN 占比异常升高；应用层攻击可能体现为请求间隔异常、请求路径/主机字段热点集中等。

（5）方向性特征：在攻击流量主要向目标汇聚时，入口与出口统计量的差异扩大，端口级入出方向包数与字节数呈现明显不对称。

在 SDN 环境中，上述特征可通过“控制平面交互+数据平面统计”被更直观地观测：异常新流会增加 table-miss 事件并触发更多 Packet-In 消息，控制器侧的消息到达速率与规则下发频次可用于刻画攻击强度；交换机端口、队列、流表计数器等统计信息则可反映速率、方向性与分布变化，并可按时间窗口汇聚形成稳定的时序特征。此外，真实攻击常呈现“多向量”特征，即在同一时间段内同时叠加多种攻击手段（例如 UDP 洪泛与应用层请求并行），或以脉冲式方式周期性调节强度以绕过基于固定阈值的告警机制。对于低速率或隐蔽型攻击，整体 bps/pps 未必极端，但在微观统计上仍会表现为活动连接区间增多、空闲区间缩短，以及包长标准差、反向包头长度熵、分段大小熵等分布类特征的系统性偏移。

2.3 张量建模

张量是对向量与矩阵的高阶推广，可表示三阶及以上的多维数组，用于刻画多模态数据在多个维度上的耦合关系[48]。与将多维信息简单拼接为长向量不同，张量建模能够在统一框架下保留各模态的结构与相互作用，因此更适合描述网络流量在时间演化、空间分布与统计特征之间的高阶相关性。设 N 阶张量记为$\Gamma \in \mathbb{R}^{I_1\times\cdots\times I_N}$，其中$\Gamma$的元素（即张量中某一位置处的具体数值）记为$x_{i_1,\cdots,i_N}$，这里的$\mathrm{i}_1,\cdots,\mathrm{i}_\mathrm{N}$为各维度的索引下标，用于指示该元素在第 1 维到第N维上的位置。张量的“模”对应张量的每一个维度，其物理含义随应用场景而定。为便于计算，常将张量沿第n模展开为矩阵$\Gamma_{(\mathrm{n})}$。其含义是：将第n维作为矩阵行索引，其余维度按一定顺序组合为列索引，从而把高阶张量转换为二维矩阵形式，便于线性代数运算。并以 Frobenius 范数$||\Gamma||_\mathrm{F}$衡量张量能量或重构误差。

Tucker 分解是典型的张量分解方法，其形式可写为式（2-1）：

$$\Gamma \approx G\times_1 A \times_2 B \times_3 C \tag{2-1}$$

其中G为核心张量，$\times_n$表示第n模乘。Tucker 分解允许各模采用不同秩，表达能力更灵活，但核心张量会引入额外参数并增加计算开销。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。PARAFAC 分解将张量表示为若干个秩一张量外积之和，其核心思想是用低秩结构近似原始张量[49]，如图 2-2 所示：

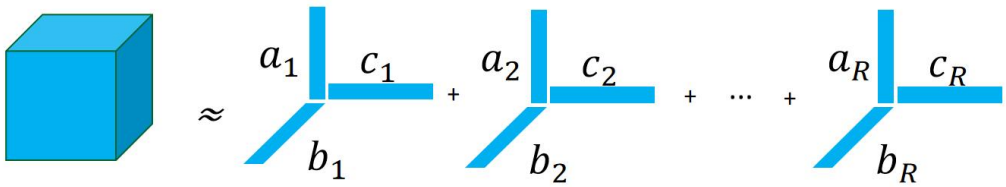


图 2-2 三维张量的 PARAFAC 分解

对于三阶张量$\mathcal{T}$，可表示为式（2-2）：

$$\mathcal{T} \approx \hat{\mathcal{T}} = \sum_{r=1}^{R} \lambda_r (a_r \circ b_r \circ c_r) \tag{2-2}$$

其中，“$\circ$”表示向量外积；a_r、b_r、c_r分别为三个模上第r个潜在因子向量；λ_r为对应分量的权重系数；R为分解秩。残差张量式（2-3）：

$$E = \mathcal{T} - \hat{\mathcal{T}} \tag{2-3}$$

表示未被低秩结构解释的部分。将因子向量按列堆叠可得到因子矩阵$A \in \mathbb{R}^{I_1 \times R}$、$B \in \mathbb{R}^{I_2 \times R}$、$C \in \mathbb{R}^{I_3 \times R}$。PARAFAC 分解基于“三线性”假设，对各模潜在因子进行显式解耦，具有因子含义直观、参数规模低（约为$O(R(I_1 + I_2 + I_3))$等优点，便于在在线/增量场景中提取可解释的多模态交互模式。

PARAFAC 分解常用交替最小二乘进行求解。其基本流程为：固定两组因子矩阵，更新剩余一组因子矩阵，使目标函数式（2-4）：

$$min||\mathcal{T} - \hat{\mathcal{T}}||_F^2 \tag{2-4}$$

逐步下降，循环迭代直至满足收敛条件。实现过程中通常结合张量展开与 Khatri–Rao 积对更新步骤进行加速，并可在统计窗口构建后对张量进行稀疏化或采样处理，以降低非零元素规模带来的计算与存储压力。此外，为抑制噪声对分解稳定性的影响，常在 ALS 更新中引入正则化项提升鲁棒性。分解秩R的设置会直接影响重构质量与模型复杂度：当R过小，低秩近似可能无法充分表达攻击流量的结构特征；当R过大，则计算成本上升且可能引入冗余分量。

在网络环境中流量数据具有持续到达与动态演化的特点，若每次都对全量历史数据重新分解，将产生较高的时间与空间开销。增量式 PARAFAC 的基本思路是在保留历史因子矩阵的基础上，仅对新增时间切片进行局部更新，并结合滑动窗口与遗忘机制控制历史影响，从而实现近实时的张量分解过程。该思想为本文后续在线检测与资源受限条件下的模型更新提供了理论支撑。

2.4 深度强化学习

强化学习（Reinforcement Learning, RL）是一类通过“智能体—环境”交互学习最优决策策略的方法，其目标是在长期交互过程中最大化累积回报[50]。深度强化学习（Deep Reinforcement Learning, DRL）将深度神经网络引入强化学习框架，用于逼近高维状态或动作空间下的价值函数或策略函数，从而显著提升复杂决策问题中的表示与泛化能力[51]。

DRL 通常将决策问题抽象为马尔可夫决策过程（Markov Decision Process, MDP），记为$(\mathrm{S},\mathrm{A},\mathrm{P},\mathrm{R},\gamma)$[52]。其中，S 为状态空间，A 为动作空间；$P(s^{'}|s,a)$表示在状态$s$下执行动作$a$转移到下一状态$s^{'}$的概率；$R(s,a)$为即时奖励；$\gamma \in (0,1]$为折扣因子，用于平衡短期收益与长期收益。智能体在时刻t观测到状态s_t，根据策略$\pi(a|s)$选择动作a_t，环境反馈奖励r_t并转移到 s_{t+1}。长期回报通常定义为折扣累积和式（2-5）：

$$G_t = \sum_{k=0}^{\infty} \gamma^{\mathrm{k}} \mathrm{r}_{\mathrm{t+k}} \tag{2-5}$$

RL 的目标是学习使期望回报 $\mathbb{E}[G_t]$最大的策略 π^*。为评价策略优劣，引入状态价值函数式（2-6）与动作价值函数式（2-7）：

$$V^{\pi}(s) = \mathbb{E}_{\pi}[G_t|s_t = s] \tag{2-6}$$

$$Q^{\pi}(s,a) = \mathbb{E}_{\pi}[G_t|s_t = s, a_t = a] \tag{2-7}$$

最优价值函数满足贝尔曼最优方程式（2-8）：

$$Q^*(s,a) = \mathbb{E}[r + \gamma max_{a^{'}} Q^*(s^{'},a^{'})] \tag{2-8}$$

基于该递推关系，经典 Q-learning 通过迭代更新式（2-9）

$$Q(s,a) \leftarrow Q^*(s,a) + \alpha(r + \gamma max_{a^{'}} Q(s^{'},a^{'}) - Q(s,a)) \tag{2-9}$$

逼近Q^*。在离散动作空间中，若能获得准确Q值，则可用贪心策略在“探索—利用”之间折中选择动作，从而逐步收敛到更优策略。

当状态维度较高或连续时，基于表格的 Q 函数难以存储与泛化。深度 Q 网络（Deep Q-Network, DQN）用神经网络$Q(s,a,\theta)$近似动作价值函数，并通过最小化时序差分误差训练网络参数。为缓解“相关样本导致震荡/发散”等不稳定问题，DQN 引入两项关键机制：其一是经验回放（Experience Replay），将交互样本$(s,a,r,s^{'})$存入回放池并随机小批量采样训练，打破样本相关性并提高数据利用率；其二是目标网络（Target Network），用延迟更新的参数θ^{-}计算目标值式（2-10）：

$$y = r + \gamma max_{a^{'}} Q(s^{'},a^{'};\theta^{-}) \tag{2-10}$$

并周期性将主网络参数同步到目标网络，从而降低目标漂移带来的训练不稳定。上述思想与“DQN 通过引入经验回放与目标网络机制缓解训练不稳定”的描述一致。

标准 DQN 在使用 max 运算时易出现动作价值过估计，从而影响策略稳定性。Double DQN 将“动作选择”和“动作评估”解耦：由主网络选择式（2-11）：

$$a^* = \sqrt{max_{a'} Q(s', a'; \theta)} \tag{2-11}$$

由目标网络评估$Q(s', a^*; \theta^-)$，以降低过估计偏差并提升训练稳定性。进一步地，Dueling DQN 采用双流结构，将$Q(s,a)$分解为状态价值$V(s)$与动作优势$A(s,a)$，通过式（2-12）：

$$Q(s,a) = V(s) + [A(s,a) - \frac{1}{|A|}\sum_{a'} A(s,a')] \tag{2-12}$$

实现优势归一化，使$V(s)$更专注于“状态本身的好坏”，$A(s,a)$则刻画“某动作相对平均动作的优势”。这种结构有助于在某些状态下动作差异不明显时仍能稳定学习状态价值，提高样本效率与决策精度。架构核心逻辑如图 2-3 所示。

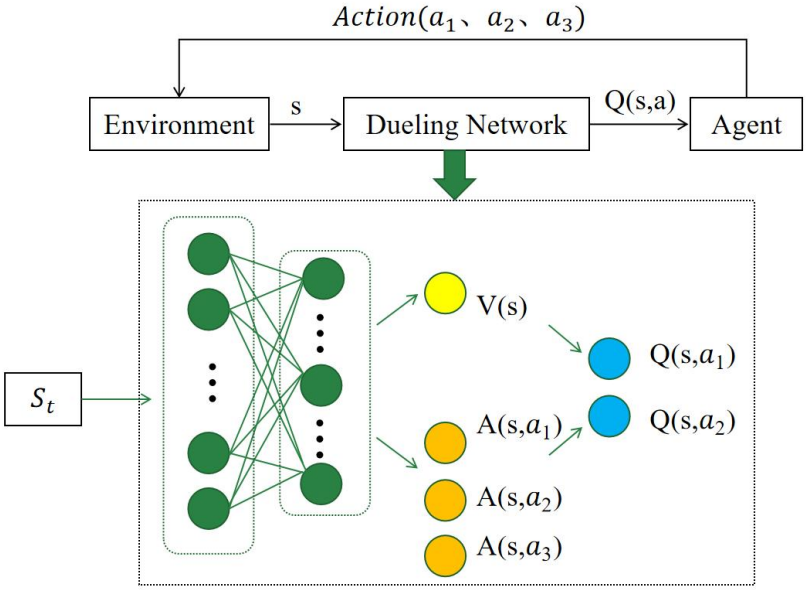


图 2-3 Dueling DQN 架构

在网络安全防御场景中，环境具有强动态与不确定性，DRL 可根据网络状态变化自适应调整防御策略，将“检测—防御”过程形式化为 MDP：状态s由张量分解得到的时空结构化特征及控制器/交换机关键指标构成；动作a对应可执行的防御操作；奖励r综合刻画攻击抑制收益、误封风险与执行代价，引导智能体在攻击强度与系统开销之间进行权衡。特别地，Dueling 结构能够分别学习“网络整体安全态势价值”与“不同防御动作的相对优势”，从而在攻击态势变化时输出更稳定的动作选择。

2.5 知识蒸馏

知识蒸馏（Knowledge Distillation, KD）是一类典型的模型压缩与知识迁移技术，其核心思想是在不显著牺牲性能的前提下，让轻量学生模型（Student）模仿高容量教师模型（Teacher）的输出行为与隐含知识，从而获得接近教师的决策能力[53]。经典 KD 通常通过“软目标（soft targets）+ 硬目标（hard targets）”的联合监督实现：软目标来自教师网络的输出分布（包含类间相似性与暗知识），硬目标来自真实标签或任务本身的监督信号。该思想最早由 Geoffrey Hinton 等提出并系统化阐述，其中温度参数用于软化分布以暴露更多非最大类信息。

与分类任务输出类别概率不同，本文的防御决策模型属于值函数型 DRL：教师模型采用 Dueling DQN 输出动作价值$Q_T(s,a)$，学生模型采用更轻量 Double DQN 输出$Q_S(s,a)$。蒸馏的目标是：在相同状态s下，使学生对各动作的相对偏好尽可能逼近教师，从而在推理速度、参数规模与部署成本显著降低的同时，维持较高的决策质量。通过策略蒸馏，从已训练的 DQN 教师中抽取策略，并训练更小网络达到接近专家的表现。

为将值函数输出转化为“动作偏好分布”，对教师式（2-13）与学生式（2-14）的Q值采用带温度的 softmax（温度记为τ）：

$$p_T(a|s)=\frac{e^{\frac{Q_T(s,a)}{\tau}}}{\sum_{a'}e^{\frac{Q_T(s,a')}{\tau}}} \tag{2-13}$$

$$p_S(a|s)=\frac{e^{\frac{Q_S(s,a)}{\tau}}}{\sum_{a'}e^{\frac{Q_S(s,a')}{\tau}}} \tag{2-14}$$

当$\tau>1$时，分布更“软”，可显式暴露教师对非最优动作的相对偏好，从而提升学生的可学习性。软蒸馏损失式（2-15）可定义为 KL 散度或交叉熵形式（两者等价到常数项）：

$$L_{soft}=KL(p_T(\cdot|s)||p_S(\cdot|s))=\sum_a p_T(a|s)log\frac{p_T(a|s)}{p_S(a|s)} \tag{2-15}$$

具体实现中加入 τ^2缩放以稳定梯度尺度式（2-16）：

$$L_{soft}\leftarrow\tau^2\cdot L_{soft} \tag{2-16}$$

仅用软蒸馏会使学生过度模仿教师而忽略环境回报信号，尤其在教师存在偏差或环境发生漂移时会降低鲁棒性。因此需要用硬损失L_{hard}，用于约束学生在交互数据上的 TD 一致性。设经验样本为(s,a,r,s')，动作式（2-17）为主网选、价值式（2-18）由目标网评估,采用 DQN 的 TD 目标：

$$a^*=arg\ \max_{a'}Q_S(s',a';\theta) \tag{2-17}$$

$$y=r+\gamma Q_S(s',a^*;\theta^-) \tag{2-18}$$

硬损失式（2-19）定义为：

$$L_{hard} = (y - Q_S(s, a; \theta))^2 \tag{2-19}$$

使学生从教师迁移“策略偏好”，同时保持对环境回报的自洽逼近，避免简单模仿导致的性能退化。蒸馏总损失由软、硬损失加权融合如式（2-20）所示，但固定α、β往往需要大量实验调参，利用梯度下降原理自适应变化权重参数，由惯性指数z与 Sigmoid 约束更新幅度[54]。

$$L_{KD} = \alpha L_{soft} + \beta L_{hard} \tag{2-20}$$

其中$\alpha, \beta \in [0,1]$，$\alpha + \beta = 1$，L_{soft}强调“模仿教师策略分布”，L_{hard}强调“对环境回报的 TD 拟合”。为保证α、β的边界与和约束，使用 Sigmoid 映射：

$$\alpha = \sigma(\lambda) \tag{2-21}$$

$$\beta = 1 - \sigma(\lambda) \tag{2-22}$$

其中 $\sigma(\cdot)$为 Sigmoid 函数，天然保证权重落在$[0,1]$且互补。在第t次更新时，计算蒸馏损失对λ的梯度式（2-23）：

$$g_t = \frac{\partial L_{KD}}{\partial \lambda} \tag{2-23}$$

为降低随机采样导致的梯度抖动，在梯度指数前设置惯性指数z，稳定权重更新，式（2-24）为平滑后的梯度方向：

$$m_t = z \cdot m_{t-1} + (1 - z) \cdot g_t \tag{2-24}$$

为避免权重发生过大跳变，将更新步长通过 Sigmoid 压缩到 $(0, \mu)$（$\mu > 0$为最大步长上限）式（2-25）：

$$\Delta t = \mu \cdot \sigma(m_t) \tag{2-25}$$

最终更新λ：

$$\lambda_{t+1} = \lambda_t - \Delta t \cdot sign(m_t) \tag{2-26}$$

更新后由$\alpha = \sigma(\lambda)$、$\beta = 1 - \sigma(\lambda)$得到新的软、硬权重，实现蒸馏过程中监督强度的自适应分配。若当前趋势表明“增大α”有助于降低L_{KD}，则更新会推动λ增大，使α增大；反之则增大β。

2.6 本章小结

本章从 SDN 网络架构、DDoS 攻击原理和流量特征、张量建模与分解理论以及深度强化学习等方面，对本文研究所涉及的相关理论与技术基础进行了系统介绍。这些理论为后续章节中检测与防御方法的设计提供了必要支撑，也为理解本文提出的多模态时空感知与资源自适应防御机制奠定了理论基础。

在上述理论基础的支撑下，第三章将重点解决“在默认控制器资源条件下能否实现高精度 DDoS 攻击检测与防御协同”的方法可行性问题，具体围绕多模态时空特征建模与基于 PARAFAC 的张量分解检测模型展开；在此基础上，第四章进一步引入工程部署中的资源受限与动态负载约束，结合增量式张量分解与资

源感知深度强化学习机制，对检测与防御过程的实时性、稳定性与可持续运行能力进行系统优化。

3 基于多模态时空表征与 DRL 协同决策的 DDoS 检测与防御方法

3.1 引言

SDN 通过集中式控制机制实现了对网络流量的全局感知与灵活调度，为网络安全防御策略的统一部署提供了技术基础。然而，在 DDoS 攻击场景下，攻击流量通常呈现多源协同、时序突发与特征隐蔽等特点，使得控制平面与流表资源在短时间内承受巨大压力[55]。如何在保证检测精度的同时，实现防御策略对攻击态势变化的快速响应，仍是 SDN 场景下面临的重要挑战。

现有针对 SDN 场景的 DDoS 检测方法，多依赖流量统计特征或机器学习模型进行异常识别，但在建模过程中往往通过特征拼接或隐式学习的方式处理时间、空间与特征信息，难以显式刻画攻击流量在多维度上的协同行为特征。这种建模方式在面对低速率、隐蔽型或动态变化的攻击模式时，检测稳定性与泛化能力仍存在不足。此外，多数研究将攻击检测与防御执行视为相对独立的两个阶段，防御策略往往基于预定义规则或静态阈值触发，缺乏对攻击强度、资源消耗及服务质量影响的综合考量，容易在提升检测灵敏度的同时引入较高的误封风险。

基于上述问题，本章在假设 SDN 控制器计算资源相对充足的前提下，重点研究多模态时空建模与检测—防御协同机制的理论可行性。通过构建“时间–空间–特征”三阶流量张量模型，引入 PARAFAC 张量分解方法对攻击流量的时空结构特征进行显式解耦，并将解耦后的结构化特征引入深度强化学习决策框架，实现检测结果对防御策略选择的有效驱动。本章旨在验证所提出方法在理想条件下对 DDoS 攻击感知与防御协同优化的有效性，为后续在资源受限场景下的决策优化研究奠定基础。

3.2 问题描述

在 SDN 场景下，DDoS 攻击通过多源协同方式在短时间内触发大量新流请求，其攻击流量在时间演化、空间分布以及统计特征等多个维度上呈现出显著的耦合特性。这种耦合特性使得攻击行为难以通过单一维度特征进行准确刻画，也对检测结果向防御决策的有效转化提出了更高要求。综合现有研究，可以将 SDN 场景下 DDoS 攻击检测与防御面临的问题归纳为以下两个方面。

3.2.1 时空特征解耦不足

DDoS 攻击的本质可表述为：在特定时间窗口内，多个源节点以相似或协同的流量特征对目标发起持续请求。然而，现有多数检测方法在建模过程中往往将不同时间窗口或不同源 IP 的流量视为相互独立的样本，或通过简单特征拼接的方式进行处理，未能在模型层面显式刻画时间演化、空间分布与流量特征之间的协同关系。

统计分析方法虽然计算开销较低，但其依赖的固定或弱自适应阈值难以适应复杂动态流量环境；机器学习与深度学习方法虽能够利用多维特征提升检测精度，但多采用隐式特征学习方式，难以解释攻击流量在不同模态之间的结构关联。当攻击流量刻意模仿正常业务模式或以低速率方式持续演化时，上述方法的检测稳定性与泛化能力仍存在不足。

因此，如何构建一种能够在模型层面显式表示攻击流量时空协同行为的建模方法，是提升 SDN 场景下 DDoS 攻击检测能力的关键问题之一。

3.2.2 检测结果与防御决策缺乏协同机制

在攻击检测的基础上，防御策略的合理选择直接影响网络服务质量与系统稳定性。然而，现有研究中攻击检测与防御执行往往被视为相对独立的两个阶段，检测结果多以告警或二值标签的形式输出，未能为防御决策提供足够的结构化信息支持。

在缺乏协同机制的情况下，防御策略通常依赖预定义规则或静态阈值触发，难以根据攻击强度、网络状态及资源消耗情况进行动态调整。当误将短时高并发正常流量判定为攻击流量时，可能导致合法业务被错误阻断；而在攻击强度快速变化或资源受限场景下，防御响应滞后又可能放大攻击影响。

因此，有必要在检测模型与防御决策之间建立有效的协同机制，使检测阶段提取的攻击态势信息能够以结构化形式参与防御策略优化，从而实现攻击抑制效果与系统开销之间的动态平衡。

3.3 问题求解

针对前述 SDN 场景下 DDoS 攻击检测中存在的“时空特征解耦不足”与“检测-防御闭环缺失”两类核心问题，本文从方法建模与求解角度出发，通过动态阈值触发机制实现检测精度与系统效率的平衡。将攻击感知与防御决策过程统一抽象为一个递进式求解问题。在此基础上，提出一种由轻量化筛选、时空特征解耦与智能决策协同构成的分级求解思路。首先通过轻量级统计监测快速过滤正常

流量，仅对疑似攻击流量触发二级检测；然后构建“时间-IP-特征”三阶张量，通过 PARAFAC 分解显式解耦时空特征，提取结构化表征用于攻击判定；最后将结构化特征输入 DuelingDQN 模型，智能体根据攻击态势自适应选择防御动作，形成“检测-决策-执行-反馈”的闭环协同机制。其中各阶段并非独立运行的功能模块，而是围绕计算开销控制与决策精度提升所构建的不同求解层级。该求解框架旨在验证检测结果对防御决策驱动的可行性，并为后续资源受限场景下的优化研究奠定基础。

3.3.1 整体框架设计

为统一刻画 DDoS 攻击感知与防御决策之间的求解关系，本文从方法建模角度构建攻击检测与防御协同的总体求解框架。该框架以攻击流量的多模态表示、时空结构特征提取以及防御动作选择为核心求解环节，通过分级建模与递进求解的方式，将复杂防御问题拆解为若干可控的子问题，从而在保证检测精度的同时降低整体计算开销。

首先，在攻击感知层面，通过对网络流量进行轻量化统计分析，实现对异常流量的初步筛选，以减少后续高复杂度建模对系统资源的占用。该阶段的主要作用在于区分正常波动与潜在攻击迹象，为精细化建模提供触发条件。其次，在特征建模层面，将触发检测的流量数据组织为“时间–空间–特征”三阶张量表示形式，并引入 PARAFAC 张量分解方法对高维流量数据进行低秩近似建模。通过张量分解，将原始流量数据中隐含的时空交互关系显式解耦为多个模态因子，从而获得具有可解释性的结构化特征表示。这一建模过程为后续防御决策提供了统一且可扩展的状态描述基础。最后，在防御决策层面，将张量分解得到的结构化特征作为状态输入，引入深度强化学习方法对防御策略进行建模。通过将防御过程抽象为马尔可夫决策过程，使智能体能够在不同攻击态势与资源状态下自适应选择防御动作，实现检测结果对防御策略的有效驱动。

需要强调的是，本章在默认控制器资源相对充足的条件下，重点验证上述多模态建模与协同决策机制的理论可行性与性能上限。针对实际部署中可能存在的资源受限与实时性约束问题，将在第四章中进一步展开分析与优化。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，实现精度与效率的平衡，如图 3-1 所示。

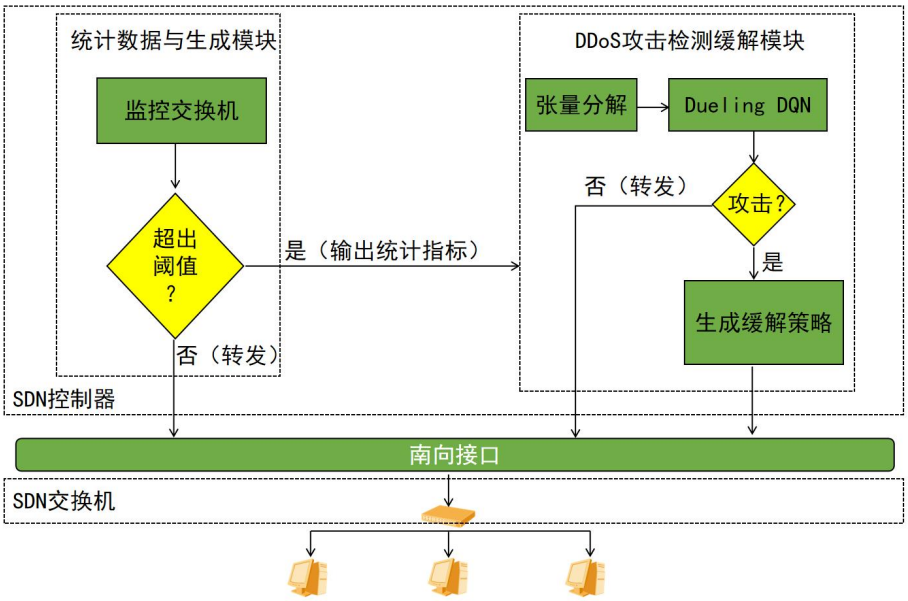


图 3-1 协同防御框架

3.3.2 统计监测模块

本节从轻量化求解的角度，对用于攻击初筛的统计特征构建与触发机制进行形式化描述，其目的在于在保证攻击敏感性的同时，避免高复杂度建模对控制平面造成不必要的计算压力。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，我们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 分钟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，可见算法 1：

算法 1 一级统计监测

输入：交换机流表统计 flow_stats、Packet−In 消息列表 packet_in_msgs、

输出：攻击风险评分 risk_score、是否触发二级检测 trigger

1. while 网络持续运行
2. 计算核心检测指标
3. 更新滑动窗口，溢出则移除旧数据

4. if 滑动窗口已满 then
5. 计算指标基线并归一化
6. 模糊化处理，执行规则推理
7. 解模糊得到 risk, trigger←(risk > θ (触发阈值))
8. else risk
9. end if ← 0 , trigger ← false
10. 输出 risk, trigger；等待进入下一个采样周期
11. end while

(1) 核心监测指标：选取 3 类 DDoS 攻击典型特征，兼顾实时性与区分度

定义 1（Packet-In 突发率）：单位时间窗口内转发至控制器的 Packet-In 消息数与该窗口内交换机观测到的新流请求数（即 table-miss 触发次数）的比值，用于刻画未知流请求对控制器造成的过载风险；在伪造大量新流的 DDoS 场景下该指标会显著上升。式子为（3-1）：

$$Rate_{packet\_in} = \frac{Num_{packet\_in}}{Num_{flow}} \tag{3-1}$$

定义 2（流量失衡度）：单位时间窗口内交换机端口的入方向与出方向数据包数的差值占比，用于刻画攻击造成的流量非对称性；在正常状态下入、出方向统计量通常接近，从而该指标接近 0。式子为（3-2）：

$$Imb_t = \frac{|Num_{inflow} - Num_{outflow}|}{Num_{inflow} + Num_{outflow}} \tag{3-2}$$

定义 3（流表熵值）：反映流表项匹配计数分布的离散程度；在不同攻击形态下，伪造新流可能导致匹配分布显著变化（上升或下降），从而使熵值相对正常基线发生明显偏移。本文将熵值的异常偏移作为辅助判别指标之一。式子为（3-3）：

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

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。攻击时伪造大量随机新流会导致流表项分布混乱，熵值激增。

(2) 动态阈值机制：

基于滑动窗口（5 分钟）实时计算正常流量的 Packet-In 突发率、流量失衡度、流表熵值的均值（μ_{normal}）与标准差（σ_{normal}），阈值设为式（3-4）：

$$\mu_{normal} + k \times \sigma_{normal} \tag{3-4}$$

基于 5 分钟滑动窗口对正常流量指标的均值μ与标准差σ进行在线估计，阈值设置为$\theta = \mu + 2\sigma$并随窗口统计量滚动更新。当正常波动增大导致σ上升时，阈值随之抬升以降低误触发；当攻击引起指标突变而使估计基线发生偏移时，阈值更新后可更敏感地反映异常变化，从而提高告警及时性。

(3) 模糊逻辑推理：

通过高斯型隶属度函数将输入变量 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]，基于专家规则库对多指标进行模糊融合推理，以降低单一指标异常导致的误触发，并输出 0-1 的攻击风险评分作为触发二级检测的依据。为保证模糊推理的可复现性，本文对三项输入指标先进行归一化处理，将其映射到[0,1]。设归一化后的输入变量为$x \in [0,1]$，采用高斯型隶属度函数式（3-5）：

$$\mu(x;c,\sigma) = e^{-\frac{(x-c)^2}{2\sigma^2}} \tag{3-5}$$

并分别定义 Low/Medium/High 三个语言变量。结合离线仿真数据对正常流量与攻击流量的分布统计结果，本文取三项输入指标共用一组参数：

$$\begin{cases} Low: C_L = 0.2, \sigma_L = 0.12 \\ Medium: C_M = 0.5, \sigma_M = 0.12 \\ Low: C_H = 0.8, \sigma_L = 0.12 \end{cases} \tag{3-6}$$

上述参数通过离线仿真对误触发率与漏检率进行联合调节得到：当正常业务短时突发导致单指标升高时，Medium/High 隶属度仍保持可分性；当攻击导致多指标协同异常时，High 隶属度显著增加，从而提高模糊推理输出的攻击概率稳定性。规则库如表 3-1 所示：

表 3-1 规则库定义

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）	对贡献最高的可疑源执行封禁（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

本文将“可疑源”定义为在当前统计窗口内对控制平面压力贡献最大的源 IP 集合。对每个源 IP i，统计其在窗口ΔT内触发的 table-miss 次数m_i，等价于新流请求次数，以及产生的 Packet-In 消息数p_i。同时为增强对“分布异常但总量不极端”的隐蔽攻击识别，计算源 IP 对流表匹配分布的熵贡献：令该源的匹配计数占比为q_i。，则其熵贡献可记为$h_i = -\,q_i log\, q_i$。将三类贡献归一化后得到综合可疑度分数式（3-7）：

$$s_i = \alpha \cdot \frac{m_i}{\sum_j m_j} + \beta \cdot \frac{p_i}{\sum_j p_j} + \gamma \cdot \frac{h_i}{\sum_j h_j} \ , \alpha + \beta + \gamma = 1 \tag{3-7}$$

在本文实验中默认取$\alpha = 0.5$，$\beta = 0.4$，$\gamma = 0.1$ 以强化对控制器过载风险的敏感性，同时保留熵贡献用于刻画分布异常。按s_i从大到小排序，取 Top-k（本文默认$k = 5$）作为“贡献最高可疑源集合”。当模糊推理输出为极高风险（等级 4）时，对 Top-k 中的源 IP 执行封禁；当为高风险（等级 3）时，对 Top-k 执行重定向或限速。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 之间的攻击概率值，超过预设阈值 0.7 时触发二级检测，避免单一指标误判。

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$\mathrm{Rate}_{\mathrm{packet_in}}$和$\mathrm{I}_{\mathrm{mb}}$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$\mathrm{Rate}_{\mathrm{packet_in}}$和$\mathrm{I}_{\mathrm{mb}}$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。根据表 6 的单交换机仿真测量结果，控制器侧的平均消息处理与规则下发开销处于毫秒以内量级；需要指出，该结果对应本地仿真环境与特定拓扑配置，真实部署中的时延还会受到链路 RTT、交换机实现与控制器负载等因素影响。系统以 2 秒为采样周期更新三项指标，并以 5 分钟滑动窗口维护μ、σ等基线统计量；2 秒采样用于快速触发，5 分钟窗口用于平滑正常波动并稳定阈值更新，从而在实时性与鲁棒性之间取得折中。

3.3.3 张量分解模块

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 A、IP 因子矩阵 B 和特征因子矩阵 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 地址与特征维度的模态显式分离，并以三线性交互的形式保留多维协同行为信息，从而为后续检测与决策提供结构化表示。相较于 Tucker

分解，PARAFAC 分解在秩一致性假设下仅需一个公共秩R，参数量更可控且因子含义更直接，便于将‘时间–IP–特征’三模态的潜在模式以可解释方式分离，从而支撑对攻击时空协同行为的显式刻画。

(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 Pearson 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 3-2 所示[20-23]：

表 3-2 最优特征子集

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) 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$\Gamma \in R^{T\times I\times F}$，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（A,B,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$A_t \circ B_i$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为特征维度，张量元素$\Gamma_{t,i,f}$表示时间窗口t、源 IP 地址i下第f个流量特征的均值，融合时间动态、IP 空间分布及流量特征的三维关联信息。

式（2-2）中时间向量$a_r \in \mathbb{R}^T$、空间向量$b_r \in \mathbb{R}^I$、特征向量$c_r \in \mathbb{R}^F$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 $A \in \mathbb{R}^{T\times R}$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 $B \in \mathbb{R}^{I\times R}$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 $C \in \mathbb{R}^{F\times R}$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$A_t \odot B_i$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：

$$A_{:,r} \leftarrow A_{:,r} \cdot \frac{(\Gamma \times_2 B^T \times_3 C^T)_{:,r}}{A \cdot (B \odot C) \cdot A^T \cdot A_{:,r}} \tag{3-8}$$

IP 因子矩阵更新：

$$B_{:,r} \leftarrow B_{:,r} \cdot \frac{(\Gamma \times_1 A^T \times_3 C^T)_{:,r}}{B \cdot (A \odot C) \cdot B^T \cdot B_{:,r}} \tag{3-9}$$

特征因子矩阵更新：

$$C_{:,r} \leftarrow C_{:,r} \cdot \frac{(\Gamma \times_1 B^T \times_2 B^T)_{:,r}}{C \cdot (A \odot B) \cdot C^T \cdot C_{:,r}} \tag{3-10}$$

其中，$\times_k$表示沿第 k 维度的张量乘法，$\odot$为内积运算。时空交互项$A_t \odot B_i$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$S_t \in \mathbb{R}^{4R+1}$作为 Dueling DQN 的输入。如式（3-11）所示：

$$s_t = [A_t, B_i, \overline{C}_f, ln(I + A_t \odot B_i), D(t)] \tag{3-11}$$

取时间因子矩阵 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。为抑制交互项乘积的尺度膨胀并提升数值稳定性，本文对交互项取对数压缩，从而在保持相对差异的同时降低训练过程的梯度波动。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，可见算法 2：

算法 2 张量分解

输入：三阶张量Γ，分解秩 R，收敛阈值ε

输出：时间因子矩阵 A、IP 因子矩阵 B、特征因子矩阵 C

1. while 未收敛且未达到最大迭代
2. 固定 B 和 C，通过最小二乘法更新时间因子矩阵 A
3. 固定 A 和 C，通过最小二乘法更新 IP 因子矩阵 B
4. 固定 A 和 B，通过最小二乘法更新特征因子矩阵 C
5. 计算张量重构误差 $E=\Gamma-\sum_{r=1}^{R} a_r \circ b_r \circ c_r$
6. if $\|E\|_F < \varepsilon$ then 终止迭代
7. end while
8. return A, B, C

Wang 等人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。论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。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。

3.3.4 动态决策模块

为实现检测结果对防御动作选择的有效驱动，本文将 SDN 场景下的防御过程抽象为马尔可夫决策过程，并从决策建模角度引入基于 Dueling DQN 的深度强化学习方法。本节重点描述防御决策问题的状态空间构建、动作集合定义及奖励函数建模方式，而非具体系统实现细节。

本文将 SDN 场景下的防御过程建模为马尔可夫决策过程(S, A, P, R, γ)。其中，状态 S 由检测阶段输出的结构化时空表示与攻击持续信息构成；动作 A 对应控制器可执行的流表操作；转移概率 P 由网络流量的动态演化与防御动作共同作用决定，在仿真环境中通过状态更新过程隐式体现；折扣因子γ用于平衡即时抑制收益与长期稳定性收益。

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)，通过精准建模状态、动作及反馈关系，构建“检测-决策-执行”闭环，解决传统方法“重检测轻防御”导致的资源效率低下问题，实现防御动作的动态优化。转移概率 $P(s'|s, a)$由网络流量动态变化与防御动作共同决定，隐含于环境模型中，刻画

状态间的转换规律；折扣因子γ：权衡即时奖励与未来奖励的重要性，确保模型兼顾短期防御效果与长期网络安全。状态向量 S 由四部分构成：时间因子A_t（R 维）：取时间因子矩阵 A 在当前窗口对应的行向量，表征当前流量在 R 个基础时间模式上的强度；IP 因子B_i（R 维）：取空间因子矩阵 B 中 Top-k 可疑源对应的均值聚合表示，刻画可疑源的空间协同行为；全局特征统计向量（d 维）：对筛选后的 d 个关键特征在当前窗口计算均值，反映整体流量统计趋势；时空交互量$A_t \odot B_i$（R 维）：由时间因子与空间因子的逐元素乘积或内积生成，用于表征‘特定时间窗口–可疑源集合’的协同异常强度。此外，将攻击持续时间τ（1 维）拼接到状态向量中，最终状态维度为 $4R + d + 1$。其中，分解秩的选择通过如图 12 重建率确定。通过这四个分量，状态向量融合四维核心特征，避免单一模态的片面性，全面刻画网络安全态势。

动作空间 A 定义了三类防御动作，对应 SDN 控制器的流表操作，采用分级防御逻辑平衡风险与成本，具体参数如表 3-3 所示：

表 3-3 最优特征子集

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

上表中的动作基础成本为归一化后的相对开销系数，用于表达不同流表操作对控制器交互频次与资源占用的相对大小；其取值依据仿真环境下的控制器处理开销与动作引发的交互复杂度进行经验标定，并在第四章动作成本量化实验中进一步验证其一致性。“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。

(1) Dueling DQN 架构设计

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值定义如式（3-12）：

$$Q(s,a) = V(s) + [A(s,a) - \frac{1}{|A|}\sum A(s,a)] \tag{3-12}$$

减去优势均值确保$V(s)$仅表征状态固有价值，$A(s,a)$聚焦动作间的相对收益

差异，实现优势归一化，避免绝对价值评估导致的误判。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。

状态价值流$V(s)$评估当前网络整体安全状态（如资源充足度、攻击强度），输入完整状态向量，输出全局价值评分，公式为式（3-13）：

$$V(s;\theta_v) = W_v^T\psi(W_2^T ReLU(W_1^T s)) \tag{3-13}$$

其中θ_v为价值流参数，ψ为激活函数，W_1、W_2、W_v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 $\mathrm{A(s,a)}$量化每个防御动作相对于平均动作的相对收益，避免绝对价值评估导致的误判，动作优势流输出对每个动作计算相对优势如式（3-14）所示：

$$A(s,a;\theta_a) = W_a^T\varphi(W_2^T ReLU(W_1^T s)) \tag{3-14}$$

其中θ_a为优势流参数，φ为激活函数，W_a为全连接层权重；明确“封禁 IP”“限制端口”“重定向”的相对优势，指导模型在不同攻击强度下选择最优动作，在低攻击强度优先重定向，高攻击强度优先封禁 IP。

融合时空特征的状态向量输入主网络；主网络通过双流架构分别计算状态价值 $\mathrm{V(s)}$与动作优势 $\mathrm{A(s,a)}$；结合上述 Q 值公式生成动作价值向量 $\mathrm{Q(s,a)}$；目标网络定期同步主网络参数，计算目标值y_j，通过损失函数优化主网络参数，确保决策准确性，可见算法 3：

算法 3 Dueling DQN 防御决策

输入：系统状态特征s、经验回放池D、主网络参数θ，目标网络参数θ^-

输出：最优防御动作a

1. while 系统持续运行
2. if rand()< ε then //按探索概率随机选取动作
3. $a \leftarrow$ 随机选择动作
4. else
5. 计算状态价值$V(s)$动作优势函数$A(s,a)$
6. $Q(s,a) \leftarrow V(s) + A(s,a) - \frac{1}{|A|}\sum A(s,a')$
7. $a \leftarrow max_a Q(s,a)$
8. end if
9. 执行动作a，观测奖励r，下一状态s'

存储经验（s、a、r、s'）至经验池D
if $|D| \geq B$ then
从D采样批量样本
for 每个样本（s、a、r、s'）do
$Q_{target} \leftarrow r + \gamma \cdot max_{a'} Q(s, a; \theta^{-})$
计算损失：$L \leftarrow (Q_{target} - Q(s, a; \theta))^2$
反向传播更新主网络参数θ
end for
if 迭代次数 $\%N = 0$ then
$\theta^{-} \leftarrow \theta$
end if
return a
end while

(2) 时空感知动态奖励函数

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式（3-15），由三部分构成：

$$R(s, a) = R_{attack} + R_{cost} + R_{temporal} \tag{3-15}$$

攻击抑制奖励R_{attack}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（3-16）所示：

$$R_{attack} = \mu \times \triangle I(t) - v \times Intensity \tag{3-16}$$

其中，$\triangle I(t)$为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、v为权重系数，$Intensity$为当前攻击强度，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R_{cost}量化动作的资源消耗与潜在误伤风险，避免高成本动作滥用如式（3-17）所示：

$$R_{cost} = -\omega \times [C_a \times (1 + \delta(t)) + \lambda_{risk} \times \mathrm{H}_{false}] \tag{3-17}$$

其中C_a为动作基础成本（取自表 3）；H_{false}为当前动作导致合法流量误封的概率，与流表熵值H_{flow}负相关，熵低时实施封禁，惩罚加重；ω为权重系数，λ_{risk}为业务损失权重，依据防御动作的阻断特性差异化设定。$\delta(t)$为资源过载惩罚系数，流表熵值H_{flow}达到预定阈值过长时取 0.5，强制增加高成本动作的惩罚，避免控制器资源过载：

$$\delta(t) = \begin{cases} 0.5 \\ 0 \end{cases} \tag{3-18}$$

时间衰减因子$R_{temporal}$，鼓励模型快速响应，如式（3-19）所示：

$$R_{temporal} = \frac{R_{attack} + R_{cost}}{1 + \delta \times D(t)} \tag{3-19}$$

其中，$D(t)$为当前攻击持续时间，δ为衰减系数，当攻击持续时间大于 60s 时，

奖励减半，强制模型快速响应短时爆发攻击。

权重系数μ、υ、ω通过网格搜索确定。预设参数范围为：

$$\begin{cases} \mu \in \{0.1,0.5,1.0\} \\ \upsilon \in \{0.01,0.1,1.0\} \\ \omega \in \{0.2,0.4,0.8\} \end{cases} \tag{3-20}$$

预设参数范围内，对每组参数在仿真环境中进行多次独立训练与评估（多随机种子、多回合 episode），以平均累计回报作为主要优化目标，并以“误封率不超过 0.5%”作为约束条件，选择满足约束且平均累计回报最大的参数组合作为最终设置。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%，在该设置下，模型在本文实验条件中获得较高的检测性能且误封率保持在较低水平，同时避免高成本动作的过度使用，从而实现“检测—决策—资源”的协同权衡。”。权重参数通过离线仿真在性能与误封率约束下经验确定，其设计目标在于验证检测—防御协同机制的可行性，而非最优参数配。

(3) 训练优化策略

为确保模型稳定收敛、避免过拟合，实验采用网格优化策略，引入概率 0.2 的 Dropout 层，减少模型对局部特征的依赖。结合余弦退火学习率如式（3-21）所示：

$$lr(t) = \frac{1}{2}[1 + cos(\frac{tp}{T})] \times lr_0 \tag{3-21}$$

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（3-22）所示：

$$y_j = r_j + \gamma \times max_a Q_{target}(s^{'}, a^{'})(1 - d_j) \tag{3-22}$$

其中y_j为第 j 个样本的目标值，用于训练网络逼近真实 Q 值；γ为折扣因子；r_j为即时奖励；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。

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。$Q_{main}(s_j, a_j; \theta)$逼近上述目标值$y_j$。如式（3-23）所示

$$Loss = E[(y_j - Q_{main}(s_j, a_j; \theta))^2] \tag{3-23}$$

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$Q_{main}(s_j, a_j; \theta)$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 3-2 所示。

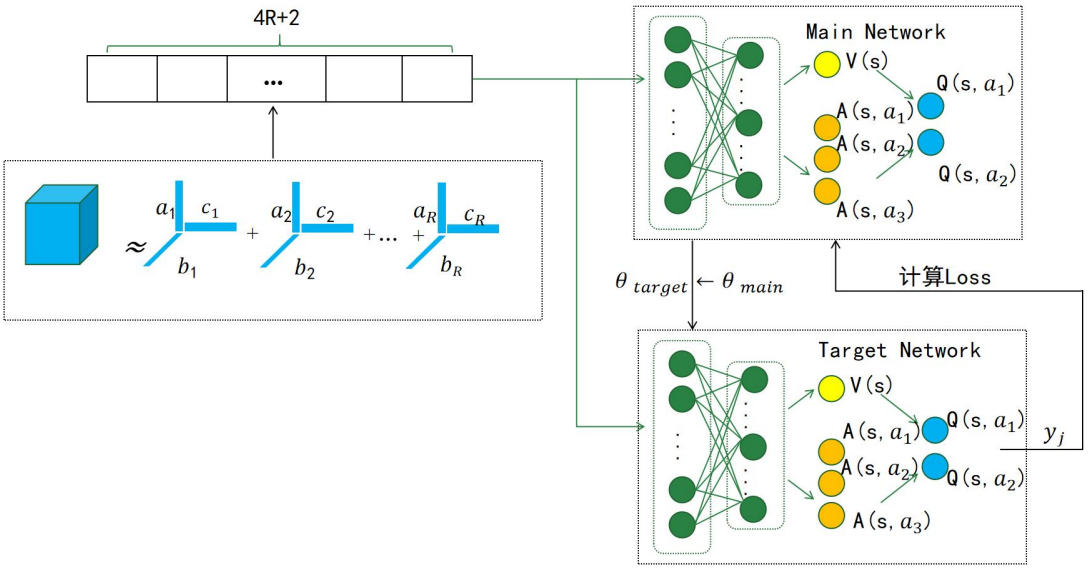


图 3-2 基于 Dueling DQN 的动态决策

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$Q(s,a)$。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。

3.4 仿真设计及结果分析

3.4.1 实验环境设置

实验基于 Ubuntu16.04LTS 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 100Mbps，延迟控制在 2ms 以内。控制器及主机 IP 地址分配如表 3-4 所示：

表 3-4 控制器及主机 IP 地址分配

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 3-3 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 DDoS 攻击检测算法。

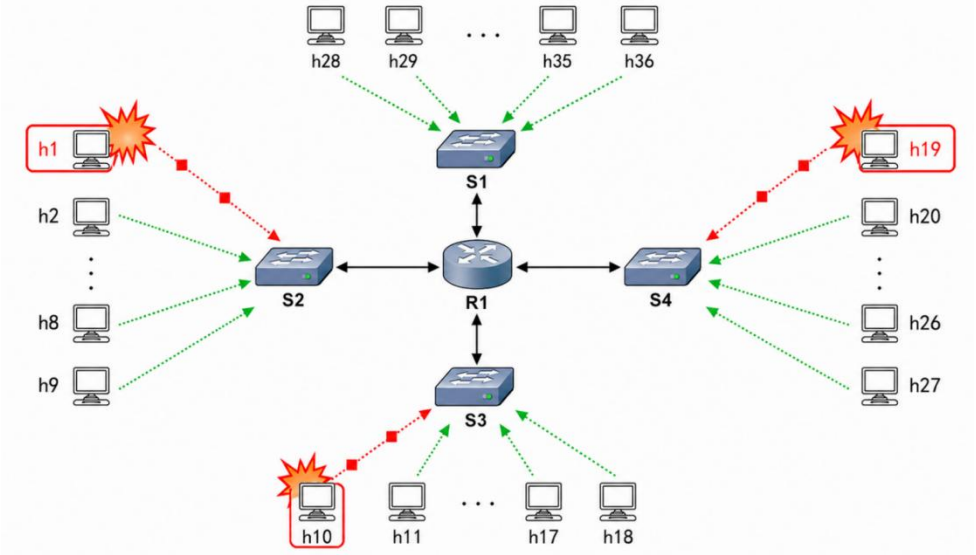


图 3-3 拓扑示意图

3.4.2 实验评估指标

如表 3- 5 所示，论文提出的“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（0.9985）、优平衡性能（0.9973），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，实现“全局状态评估+动作相对优势”的联合优化。

表 3-5 五折交叉验证的性能

交叉验证	Accuracy	AUC	F1
1	0.9946	0.9992	0.9969
2	0.9951	0.9989	0.9972
3	0.9972	0.9989	0.9983
4	0.9971	0.9991	0.9984
5	0.9965	0.9966	0.9956
平均值	0.9961	0.9985	0.9973

图 3-4 展示了在数据集 CIC-DDoS2019 上本方案与使用 Q-Learning、目标网络和经验回放的文献[56]、使用 DQN 和迁移学习的文献[57]、使用 Dueling DDQN 和优先经验回放的文献[58]、使用 DQN 和 BiLSTM 时序分析的文献[59]的误封率对

比[56-59]。

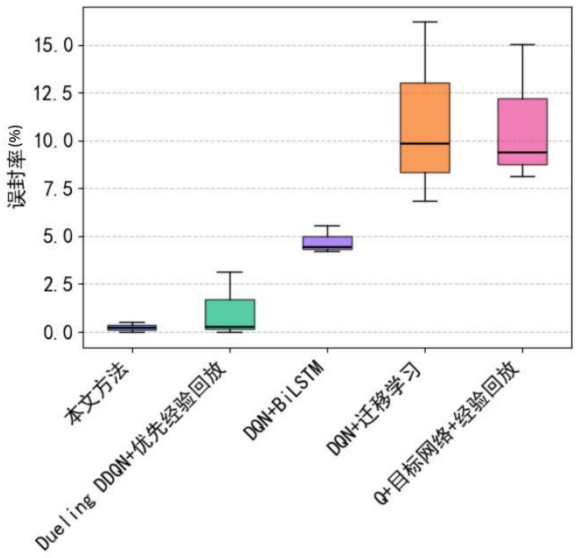
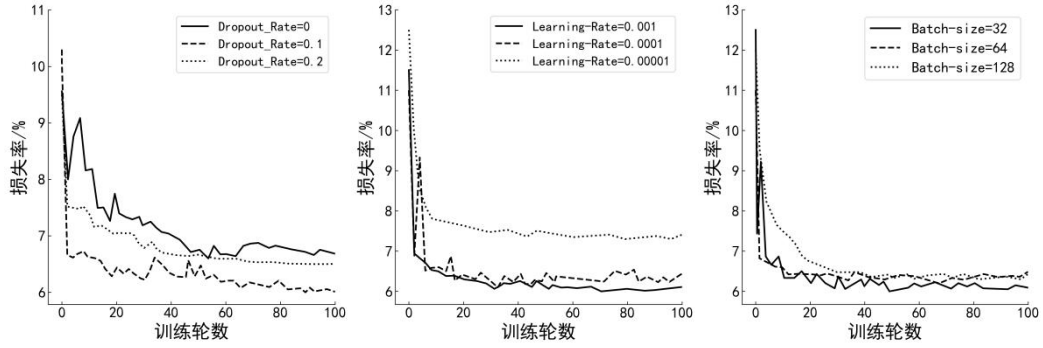


图 3-4 不同方法的误封率

从箱线图可见，本文方法的误封率分布更集中且中位数更低，表明在本文实验设置下其对正常流量的误封情况得到有效抑制。该现象与一级监测的多指标融合触发机制以及决策阶段的风险惩罚设计相关。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[56-59]的方法，本方案误封率显著更低，现有方法仅拼接多模态特征，未显式分离时空交互关系；而本方案通过 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。在本文实验条件下，本文方法的误封率总体处于较低水平，最大值不超过 0.5%，说明该方案在误识别控制方面具有可用性。

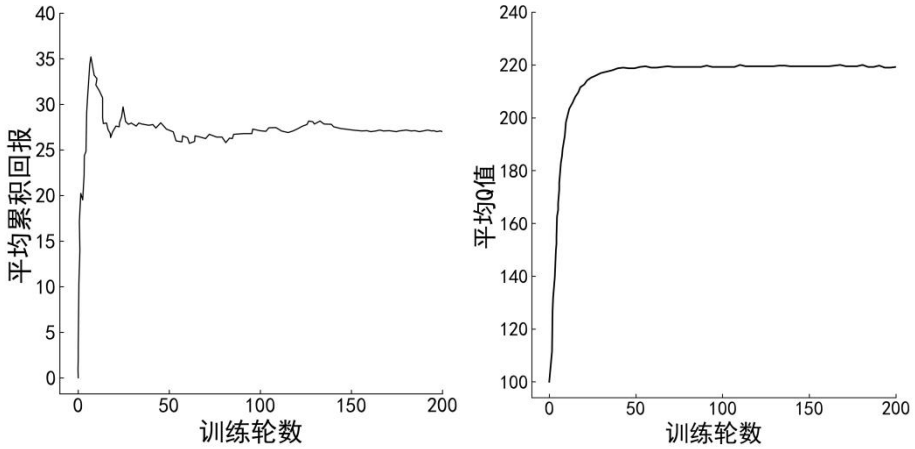
经过实验，丢弃率、批量大小和学习率的最佳取值分别为 0.2、64 和 0.001，结果如图 3-5 所示：



a) 丢弃率　　b) 学习率　　c) 批量大小

图 3-5 不同参数对模型的影响

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，学习率为 0.0001 时虽也可以迅速降低但是波动较大，更低的学习率会导致损失率更高。图 3- 6 展示了不同训练轮数下平均累积回报和 Q 值的变化情况。



a)平均累积回报　　b)平均 Q 值

图 3-6 平均累积回报和 Q 值

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：

$$1-\frac{||\Gamma-\hat{\Gamma}||_F^2}{||\Gamma||_F^2}\times 100\% \tag{3-24}$$

公式表示分解后的近似张量$\hat{\Gamma}$对原始张量Γ的还原程度。如图 3-7 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，本研究的秩选择了最小值 10。实验显示单次分解耗时约 50ms（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 8ms，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（公式 1-3），单次检测耗时小于 1ms。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 3.99s。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。

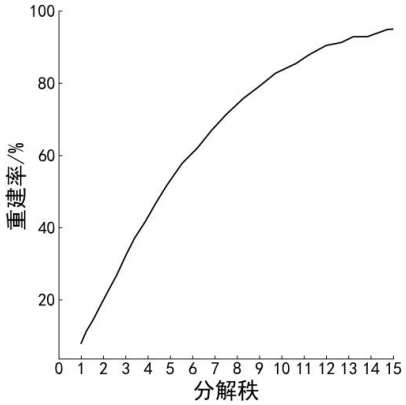


图 3-7 分解秩与重建率

3.5 本章小结

本章围绕 SDN 场景下 DDoS 攻击检测过程中多源流量特征难以协同建模、检测与防御决策割裂等问题，在控制器计算资源相对充足的前提条件下，提出了一种基于流表多模态时空感知与深度强化学习协同的 DDoS 攻击检测方法。

首先，从时间演化、空间分布及统计特征等多个维度对 SDN 流量进行建模，构建了多模态时空流量张量表示形式，为刻画 DDoS 攻击的协同行为特征提供了统一的数据结构；其次，引入 PARAFAC 张量分解方法，对高维时空特征进行显式解耦，实现了对攻击流量潜在模式的有效提取；在此基础上，将深度强化学习机制引入攻击检测与防御决策过程，构建了检测结果与防御策略协同联动的智能

防御框架。通过仿真实验对所提方法的检测性能与防御效果进行了验证，实验结果表明，所提出方法在攻击检测准确率与误封率控制等指标上取得了较好的实验性能，验证了多模态张量建模与深度强化学习协同机制在 DDoS 攻击检测中的方法可行性与有效性。

需要指出的是，本章研究主要用于验证多模态时空特征显式建模与检测—防御协同机制在理想计算条件下的可行性，其结论并不直接等同于资源受限场景下的实际部署效果。针对实际部署中资源受限与网络负载动态变化等问题，将在第四章中进一步研究。

4 面向资源约束的 DDoS 防御决策优化与轻量化动态调度方法

4.1 引言

在第三章验证多模态时空感知与深度强化学习协同防御方法可行性的基础上，进一步考虑实际 SDN 网络环境中控制器资源受限与网络负载动态变化等约束条件，有必要从决策建模与求解优化角度对防御策略进行扩展研究。具体而言，当计算资源与处理时延成为约束因素时，原有基于全量特征建模与决策的方法在实时性与稳定性方面可能面临挑战。因此，本章围绕防御效能与系统资源消耗之间的权衡关系，研究引入资源感知机制与轻量化建模策略的防御决策优化方法[60]。

针对上述问题，本章不再关注检测模型本身的有效性，而是以分析防御系统在资源受限环境下的实时响应特性及运行开销变化为核心目标，对第三章提出的方法进行进一步优化与扩展。具体而言，本章引入增量式 PARAFAC 张量分解算法，将原有全量分解过程转化为在线更新机制，以降低时空特征提取阶段的计算开销[61]；同时，在深度强化学习决策过程中引入资源感知机制，使防御策略能够根据控制器实时负载状态动态调整防御动作；并通过模型轻量化与加速策略，进一步提升防御系统的工程可部署性[62]。通过上述优化，本章旨在探索一种面向实际 SDN 部署需求的资源感知自适应 DDoS 防御方法，在基本保持第三章方法检测精度表现的前提下，分析防御效能与系统资源消耗之间的权衡关系。

4.2 问题描述

在第三章方法基础上，为刻画资源约束条件对防御决策过程的影响，本节从建模角度对控制器资源状态、防御动作成本及其与攻击态势之间的关系进行形式化描述。

4.2.1 问题背景

第三章中，本文提出了一种面向 SDN 流表多模态感知与深度强化学习协同防御的 DDoS 攻击防御方法，通过“统计初筛—张量分解—Dueling DQN 决策”的三级递进式架构，在检测精度与防御有效性方面取得了良好效果。实验结果表明，该方法能够显著降低误封率，并在动态攻击场景下实现防御策略的自适应优化。然而，由于默认控制器具备相对充足的计算与存储资源，其核心模块全量张

量分解与完整 DRL 网络推理在网络规模扩大、攻击频率升高或部署于资源受限控制节点时，将不可避免地引入以下问题：

(1) 计算延迟累积：高维流量数据触发频繁的全量张量分解，导致防御响应时延上升；

(2) 资源占用不可感知：防御决策未显式建模控制器资源状态，可能在高负载下触发高成本动作；

(3) 模型体积冗余：DRL 模型参数规模较大，不利于在边缘或低算力控制器部署。

上述问题表明，仅依赖第三章的“高精度协同防御模型”，尚不足以满足实际 SDN 场景中对实时性、轻量化与环境自适应性的综合要求。因此，在资源受限条件下，需要在检测精度、防御响应时延与系统计算开销之间建立明确的权衡机制，以支撑防御策略的持续运行。

4.2.2 核心问题

结合 SDN 控制器的运行特性与 DDoS 攻击的动态演化规律，第四章研究的问题可抽象为以下三个相互关联的子问题。

(1) 高维流量感知的实时性瓶颈问题

在第三章中，张量分解模块通过构建“时间–IP–特征”三阶张量，实现了对攻击时空特征的显式解耦。然而，该方法默认对每个触发窗口执行全量 PARAFAC 分解，其计算复杂度与时间窗口数、IP 数量及特征维度呈线性甚至超线性增长。在实际网络中，流量呈现出明显的时间连续性，相邻时间窗口之间的数据变化往往局部且渐进。若每次仅因少量新流量到达便重新执行全量分解，将导致大量冗余计算，难以满足实时防御需求。因此，亟需一种能够利用历史分解结果、支持在线更新的张量分解机制，以降低计算开销并提升检测阶段的实时性。

(2) 防御决策对控制器资源状态不敏感问题

第三章中构建的 Dueling DQN 防御模型主要以流量时空特征为决策依据，通过奖励函数平衡攻击抑制收益与防御动作成本。然而，该成本建模主要关注防御动作本身的风险与影响，尚未将控制器当前的资源状态（如 CPU 负载、流表占用率）显式纳入状态空间。在 SDN 场景下，控制器既是防御决策的执行者，也是潜在的攻击目标。当防御策略在资源紧张状态下仍频繁触发高成本动作，可能导致控制器过载，反而降低整体网络稳定性。因此，防御决策机制亟需具备资源感知能力，能够根据控制器实时负载状态动态调整防御策略强度，实现“攻击风险—防御收益—资源消耗”之间的协同优化。

(3) 深度强化学习模型的部署可行性问题

深度强化学习模型在训练阶段通常采用较深网络结构以提升策略表达能力，但在实际部署阶段，这种过参数化设计会带来额外的存储与推理开销。对于部署

在边缘节点或轻量级 SDN 控制器上的防御系统而言，模型体积过大不仅增加内存占用，还会延长单次决策时间，影响对突发攻击的快速响应能力。因此，有必要在模型训练完成后，通过模型压缩与策略迁移技术对 DRL 网络进行轻量化处理，在基本保持决策性能的前提下，提高其工程可部署性。

4.2.3 总体思路

针对上述问题，第四章的研究目标不再单纯追求检测精度的提升，而是从工程可部署性与资源自适应性出发，对第三章方法进行系统性优化，具体思路如下：

(1) 在感知阶段，将全量张量分解优化为增量式张量分解，利用时间连续性减少重复计算，降低高维特征解耦的实时性开销；

(2) 在决策阶段，将控制器资源状态引入 DRL 状态空间与奖励函数设计中，构建资源感知的自适应防御决策机制；

(3) 在模型层面，通过模型知识蒸馏技术对 DRL 网络进行轻量化处理，减少模型规模与推理延迟。

通过上述优化，本文旨在构建一种面向资源受限环境的轻量化自适应 DDoS 防御方法，在保证检测精度与防御有效性的同时，显著提升系统的实时性、稳定性与实际部署价值。

4.3 问题求解

针对上述问题，本章设计“感知阶段轻量化-决策阶段智能化-模型本体精简化”三级优化方案。通过增量式张量分解提升特征解耦速度，资源感知 DRL 决策实现攻防与资源的动态平衡，模型蒸馏降低部署开销，最终达成优化目标。

4.3.1 增量式 PARAFAC 张量分解算法

为解决全量分解的实时性瓶颈，设计基于滑动窗口的增量式 PARAFAC 分解算法，利用历史分解结果快速更新因子矩阵，避免重复计算。

(1) 算法原理：

设$\mathcal{T}_{t-1} \in \mathbb{R}^{T_{t-1}\times I\times F}$是上一时刻已分解的三阶张量，其因子矩阵为$A_{t-1} \in \mathbb{R}^{T_{t-1}\times R}$，$B_{t-1} \in \mathbb{R}^{I\times R}$，$C_{t-1} \in \mathbb{R}^{F\times R}$。当新流量数据切片$\mathcal{X}_t \in \mathbb{R}^{T_t\times I\times F}$到达时，当前时刻张量为$\mathcal{T}_t = [\mathcal{T}_{t-1}; \mathcal{X}_t] \in \mathbb{R}^{T_t\times I\times F}(T_t = T_{t-1} + 1)$。增量分解的核心是固定两个因子矩阵，通过最小二乘法迭代更新第三个因子，同时引入正则项保留历史信息平滑性。以更新时间因子矩阵A_t为例，目标函数为式（4-1）：

$$\mathcal{L}(A_t) = ||X_t - A_t(B_{t-1}\odot C_{t-1})^{\mathrm{T}}||_{\mathrm{F}}^2 + \lambda||A_t - A_{t-1}||_{\mathrm{F}}^2 \tag{4-1}$$

其中，⊙表示 Khatri-Rao 积，λ是正则化参数，用于平衡新数据拟合与历史信息的保留。通过对目标函数求导并令导数为零，可得时间因子A_t的更新公式（4-2）：

$$A_t \leftarrow (\mathrm{x}_t^{(1)}(B_{t-1} \odot C_{t-1}) + \lambda A_{t-1})((\mathrm{B}_{t-1}^{\mathrm{T}} B_{t-1}) * (\mathrm{C}_{t-1}^{\mathrm{T}} C_{t-1}) + \lambda \mathrm{I}) \quad (4\text{-}2)$$

其中，$\mathrm{x}_t^{(1)}$是张量$\boldsymbol{X_t}$沿时间维度的模式-1 展开矩阵，$*$表示逐元素乘，I为单位矩阵。因为避免了直接处理高维张量，计算复杂度显著低于全量分解。同理，可推导出固定A_t和C_{t-1}时 IP 因子B_t的更新公式，以及固定A_t和B_t更新C_t的公式。通过多次交替迭代完成增量分解。

(2) 算法优势与复杂度分析

与全量 PARAFAC 分解相比，增量式算法的核心优势的是将时间复杂度从$O(R \times T \times I \times F)$降至$O(T \times I \times F)$，无需重复计算历史数据的因子矩阵，单次分解耗时可控制在 8ms 以内。该算法通过对新增数据进行局部更新，在一定程度上降低了重复计算带来的开销，同时尽量保持对流量时空特征的刻画能力。同时，通过正则项保留历史分解的模式信息，确保分解结果的一致性与稳定性，增量更新后的因子矩阵与全量分解的相似度超过 95%，不影响后续 DRL 决策的准确性。

4.3.2 源感知的自适应 DRL 决策机制

为解决 DRL 决策的资源感知缺失问题，通过扩展状态空间、重构奖励函数，实现“攻防收益-资源成本-实时负载”的三维量化权衡。

(1) 状态空间扩展

在第三章状态向量的基础上，新增控制器实时资源状态维度，扩展后的状态向量为式（4-3）：

$$s_t^{'} = [s_t, CPU_{util}(t), Mem_{util}(t)] \quad (4\text{-}3)$$

通过将系统资源状态引入决策依据，模型能够根据攻击态势与资源变化自适应调整防御动作选择。其中，$\mathrm{CPU_{util}(t)}$为当前时间窗口控制器平均 CPU 利用率（取值范围[0,1]），$\mathrm{Mem_{util}(t)}$为平均内存利用率（取值范围[0,1]），通过 SDN 控制器北向 API 实时采集（采样周期 200ms）。扩展后的状态向量维度为 $4R + 3$（$R = 10$ 时为 43 维），既保留时空特征信息，又实现对控制器健康状态的精准感知。

(2) 动态奖励函数重构

重构第三章的奖励函数，引入资源代价项 Rresource(s,a)，新奖励函数式（4-4）为：

$$R_{new}(s, a) = R_{attack} + R_{cost} + R_{temporal} + R_{resource}(s, a) \quad (4\text{-}4)$$

攻击抑制奖励$\mathrm{R_{attack}}$、时间衰减因子$\mathrm{R_{temporal}}$、防御成本惩罚$\mathrm{R_{cost}}$沿用第三章，量化攻击流量压制效果、防御动作固有成本与误封风险，鼓励快速响应短时攻击。量化防御动作对控制器实时负载的影响，资源代价为式（4-5）：

$$R_{resource}(s^{'},a) = -\eta \cdot C_a \cdot (1 + \alpha \cdot CPU_{util} + \beta \cdot Mem_{util}) \quad (4\text{-}5)$$

其中，η是资源代价权重，C_a为防御动作固有成本，α、β分别为 CPU 和内存负载的影响系数。该设计使高负载时高成本动作的惩罚显著增加，引导模型优先选择轻量级防御策略。

(3) 网络架构与训练优化

DRL 网络沿用第三章的 Dueling DQN 双流架构，仅调整输入层神经元数量从 41 个增至 43 个，保持状态价值流与动作优势流的解耦设计。训练参数与第三章保持一致：Dropout 率 0.2、批量大小 64、初始学习率 0.001，采用余弦退火学习率策略与目标网络同步机制（同步周期 100 轮），确保训练稳定性与结果可比性。

4.3.3 防御模型的轻量化与加速

在 SDN 防御场景中，控制器需要同时承担拓扑维护、流表下发与事件处理等任务，在线防御决策模块若模型体积过大或推理开销过高，将造成控制平面资源竞争并引入决策延迟，从而降低对突发 DDoS 攻击的响应效率。因此，本文在保证防御效果的前提下，采用“教师—学生蒸馏压缩”策略对防御决策模型进行轻量化，以实现模型推理加速与部署成本降低。

教师模型（Teacher）：采用已训练收敛的 Dueling Double DQN，具备更强表达能力与更稳定的价值估计能力，适合作为高质量策略的知识来源。学生模型（Student）：采用结构更简洁的轻量 Double DQN，以降低参数量与 FLOPs，从而满足在线推理的时延约束。该结构设计遵循“离线强模型—在线轻模型”的工程原则：教师负责学习最优策略，学生通过蒸馏获得接近教师的决策能力并用于实际部署。为避免轻量化带来的性能退化，本文对学生采用自适应蒸馏训练，联合优化。其中，L_{soft}通过带温度 softmax 将教师、学生的Q值映射为动作分布，并最小化 KL 散度以迁移教师策略偏好；L_{hard}采用 Double DQN 的 TD 误差以保持对环境回报信号的拟合。训练过程中使用参数λ控制α、β，并引入惯性系数$z = 0.9$ 与 Sigmoid 步长压缩实现权重自适应更新，从而在“模仿教师策略”与“贴合环境回报”之间动态平衡。部署阶段仅保留学生网络进行动作选择降低在线推理的计算开销与内存占用：

$$a_t = arg \max_a Q_S(s_t, a) \quad (4\text{-}6)$$

教师网络仅用于离线训练与蒸馏，不参与在线推理。通过蒸馏压缩后，学生模型在参数规模与计算复杂度上显著降低，使控制器在高负载事件下仍能维持稳定的决策频率与响应时延。同时，自适应蒸馏在训练阶段动态调整软/硬监督占比，减小“模型变小导致策略退化”的风险，使学生在推理加速的同时仍保持较

高的防御收益与鲁棒性。

4.4 仿真设计及结果分析

4.4.1 实验评估指标

本章的实验环境沿用第三章，在第三章 Accuracy、AUC、F1、误封率的基础上，新增 2 类部署相关指标：
模型参数量和浮点运算次数 FLOPs。

4.4.2 平衡能力验证

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 0.2s，周期 2s），其余主机以$[0, f_{max}]$随机速率发送正常流量。以 0.2s 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 20000 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 10Kf/s 持续 40s，之后再在 10s 之内达到最高值 38Kf/s，最后逐渐减少在 80s 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 4-1 所示。

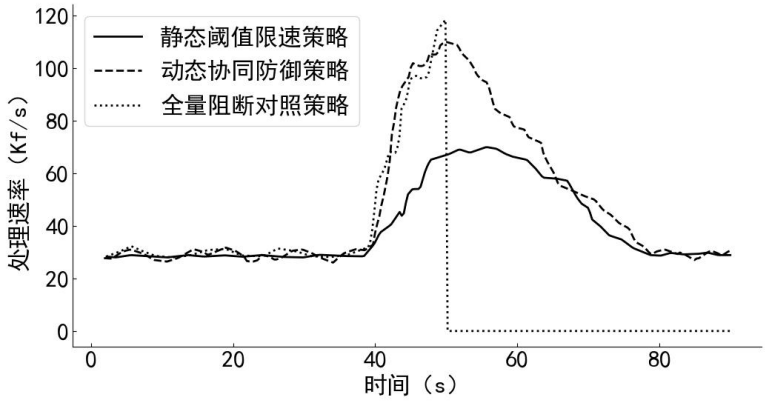


图 4-1 模型效果图

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 4- 1 所示。

表 4-1 不同负载下的实时性

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

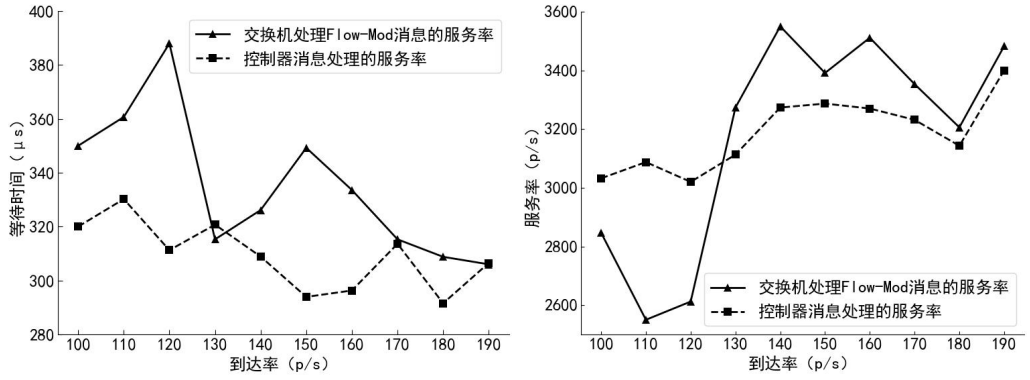
由实验结果可知，在剩余资源较为不足时候（20%的剩余资源和 45Kf/s 攻击）因为资源容易耗尽触发缓解机制更加迅速，控制器响应更快，证明了对高速攻击的快速反应能力；在剩余资源充足的情况下（90%的剩余资源和 30Kf/s）控制器响应稍慢但是资源缓冲更加充足避免误封，表明了高容量下仍能在合理时间内缓解攻击。

4.4.3 动作成本量化

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。

(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 4-2 所示：



a)等待时间　　b)服务率

图 4-2 交换机和控制器在不同到达率下的服务率和等待时间

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。

(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 4-2 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。

表 4-2 交换机与控制器的平均等待时间

统计量	值
Arrival rate	100-190(p/s)
Flow-Mod service rate	3077(p/s)
Controller service rate	3198(p/s)
Flow-Mod waiting time	0.335(ms)
Controller waiting time	0.309(ms)

量化御动作的综合成本C_{action}如下所示：

$$C_{action} = \lambda_{res} \times \frac{W_{wait}}{S_{service}} + \lambda_{risk} \times (1 - \frac{R_{clean}}{R_{total}}) \tag{4-7}$$

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$(1 -$

$\frac{R_{clean}}{R_{total}}$)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。

4.4.4 实验结果分析

(1) 增量分解效果验证

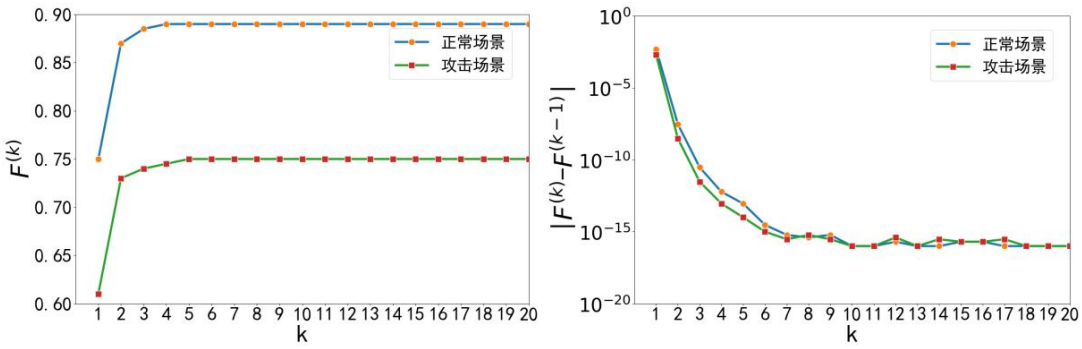
为了衡量增量分解对新流量切片的特征解耦效果，定义第k次迭代时时空特征解耦精准度式（4-8）：

$$F^{(k)} = 1 - \frac{||X_t - A_t(B_{t-1} \odot C_{t-1})^T||}{||X_t||} \tag{4-8}$$

其中X_t为新流量切片，A_t、B_{t-1}、C_{t-1}为迭代更新后的因子矩阵，$F^{(k)}$越接近 1，说明时空特征解耦效果越好。定义迭代差值式（4-9）：

$$|F^{(k)} - F^{(k-1)}| \tag{4-9}$$

衡量相邻两次迭代的拟合度变化幅度，反映分解算法的收敛速度，收敛时间主要取决于流量场景的解耦难度，以“迭代差值$|F^{(k)} - F^{(k-1)}| < 10^{-15}$”为收敛判定标准，如图 4- 3 所示，正常流量场景 7 次迭代、DDoS 攻击场景 9 次迭代后能达到收敛。



a) 解耦精准度　　b) 迭代差值

图 4-3 k 次迭代的解耦效果和收敛速度

可以看到正常流量场景：$F^{(k)} \in [0.75,0.9]$，特征分布稳定，解耦难度低；而当 DDoS 攻击场景时$F^{(k)} \in [0.6,0.75]$，攻击流量特征复杂，存在随机伪造 IP 和异常包长，解耦难度升高。

(2) 资源感知决策效果

设置控制器不同初始负载（低负载：CPU≤30%；高负载：CPU≥80%），对比第三章 DRL 与本章资源感知 DRL 的动作选择策略，结果如图 4-4 所示：

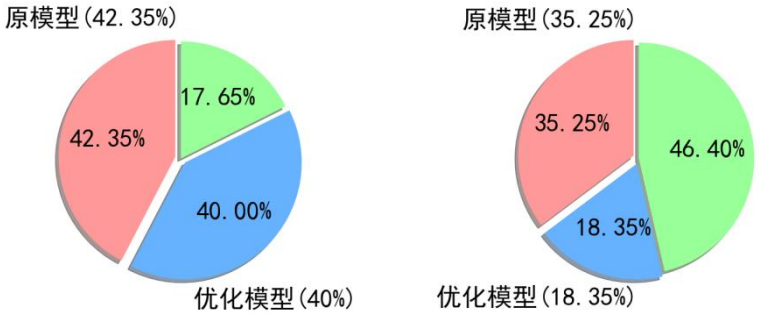


图 4-4 不同初始负载下的动作选择

低负载场景下，两类模型均优先选择高收益的封禁 IP 动作，比例在 40%以上；高负载场景下，第三章模型仍有 35.25%的概率选择封禁 IP，导致 CPU 利用率进一步升至 90%以上；而本章模型封禁 IP 选择比例降至 18.35%，控制器 CPU 利用率稳定在 75%左右，有效缓解了“防御性宕机”。

(3) 模型轻量化效果

为验证轻量化带来的真实收益，本文在选取 10 维关键特征的配置下，对教师模型与蒸馏后的学生模型进行参数规模与 FLOPs 对比，并同步考察检测性能变化。结果如表 4-3 所示。在经过知识蒸馏之后，模型参数的规模明显缩小。具体来说，与教师模型的参数相比，学生模型规模与推理开销分别降低约 63.85%与 59.00%。在检测性能方面，教师模型在 CIC-DDoS2019 数据集上取得了 0.9961 的 Precision、0.9958 的 Recall 以及 0.9957 的 F1-score。学生模型在模型规模显著压缩的情况下，Precision 与 Recall 分别保持在 0.9843 和 0.9862，F1-score 为 0.9854，性能下降幅度有限。结果表明，知识蒸馏有效地将教师模型的高质量决策策略迁移至轻量化学生模型，在基本保持高检测精度和低误封率优势的同时，大幅降低了计算与存储开销，验证了所提出轻量化方法在实际 SDN 场景中的工程可行性。

表 4-3 模型轻量化效果

模型	参数量	FLOPs	Precision	Recall	F1
教师	136982	331452	0.9961	0.9958	0.9957
学生	49518	135891	0.9843	0.9862	0.9854
缩减比（%）	63.85	59.00			

4.5 本章小结

本章在第三章方法的基础上，引入资源约束条件，对防御决策过程进行了进

一步建模与优化，验证了所提出协同防御机制在资源受限环境下的可部署性与运行稳定性。与第三章侧重方法可行性验证不同，本章重点关注防御策略在工程部署条件下的持续运行能力，为实际 SDN 环境中的 DDoS 防御应用提供了实验参考。

首先，针对全量张量分解在高维动态流量场景下计算开销较大的问题，引入增量式 PARAFAC 张量分解算法，实现了时空特征的在线更-新，在保证特征表达能力的同时有效降低了计算复杂度；其次，在深度强化学习防御决策过程中引入资源感知机制，使防御策略能够综合考虑攻击态势与控制器实时负载状态，实现防御效能与系统资源消耗之间的动态平衡；同时，通过模型轻量化与加速策略，进一步提升了防御系统在资源受限环境下的实时性与稳定性。实验结果表明，相较于第三章方法，本章所提出的优化策略在基本保持检测与防御性能的前提下，显著降低了系统计算开销与决策延迟，增强了防御机制在复杂网络环境中的可持续运行能力。

综上所述，本章从工程实现与系统优化角度对 DDoS 防御机制进行了完善，为所提方法在实际 SDN 网络中的部署应用提供了可行支撑。

5 结论与展望

本章在前文研究工作的基础上，对全文的主要研究内容与成果进行系统总结，并凝练本文的创新点，同时结合实际应用需求与研究过程中的局限性，对未来可能的研究方向进行展望。

5.1 主要工作总结

本文围绕 SDN 场景下 DDoS 攻击检测与防御问题，系统研究了多模态时空特征建模、检测结果驱动防御决策以及资源受限条件下防御策略优化等关键问题，针对传统方法在时空特征建模能力不足、检测与防御割裂以及工程可部署性受限等不足，开展了系统性研究，主要工作总结如下。

(1) 面向 SDN 场景下复杂多变的 DDoS 攻击流量特征，本文构建了一种基于多模态时空感知的流量特征表示方式。通过对流量统计特征、时间关联特征与空间分布特征进行统一建模，有效刻画了正常流量与攻击流量在时空维度上的差异性，为后续攻击检测提供了高区分度的特征基础。

(2) 针对传统矩阵或向量建模难以显式表达多维关联关系的问题，本文在第三章中引入张量建模思想，构建了“时间–IP–特征”三阶张量模型，并基于 PARAFAC 张量分解方法对高维流量数据中的潜在模式进行解耦分析。在默认控制器资源条件下，实验结果表明该方法能够有效提升 DDoS 攻击检测的准确率与稳定性，并验证了检测结果与防御决策协同的可行性。

(3) 针对第三章方法在实际 SDN 控制器部署中可能面临的资源受限与动态负载问题，本文在第四章中从工程可持续运行的角度对检测与防御框架进行了进一步扩展。通过引入增量式张量分解机制，降低了高维时空特征在线更新过程中的计算复杂度；同时，在防御决策层设计了资源感知的深度强化学习机制，使防御策略能够根据控制器实时负载状态在攻击抑制效果与资源消耗之间进行动态权衡，从而提升系统在复杂网络环境下的实时性与稳定性。

综上，本文围绕 SDN 场景下 DDoS 攻击的检测与防御问题，构建了基于多模态时空感知与深度强化学习的协同防御框架，并进一步从资源受限环境出发对防御机制进行了优化，为 DDoS 防御方法的实际部署提供了有益参考。本文实验主要用于验证所提方法在典型 DDoS 攻击场景下的有效性，其跨数据集与跨拓扑泛化能力仍有待进一步研究。

5.2 创新点

围绕 SDN 场景下 DDoS 攻击检测与防御中时空特征建模不足以及检测与防御协同缺失的问题，本文在攻击流量建模方法与防御决策机制方面开展研究，主要创新点体现在以下两点：

(1) 提出了面向 SDN 场景的 DDoS 多模态时空感知与协同防御方法。

针对传统方法难以显式刻画攻击流量时间演化、空间分布与统计特征之间高阶耦合关系的问题，本文构建了“时间—IP—特征”三阶张量表示模型，并结合 PARAFAC 张量分解提取具有可解释性的时空交互因子，实现了对 DDoS 攻击多源协同、时序突发与特征隐蔽性的结构化表征。在此基础上，将张量分解结果进一步作为深度强化学习状态输入，构建检测与防御协同联动的闭环机制，提升了 DDoS 攻击检测与防御决策的一体化能力。

(2) 提出了面向资源受限环境的 SDN DDoS 防御优化方法。

针对实际部署中控制器资源有限、网络负载动态变化导致在线检测与防御难以兼顾实时性和系统开销的问题，本文在前述方法基础上引入增量式 PARAFAC 分解机制，降低了新增流量在线更新的计算复杂度；同时设计资源感知的深度强化学习决策机制，并结合模型轻量化与加速策略，实现了防御效果、资源消耗与推理时延之间的动态权衡，从而增强了所提方法在资源约束场景下的工程可部署性与稳定运行能力。

5.3 不足与展望

尽管本文围绕 SDN 场景下 DDoS 攻击检测与防御问题开展了系统研究，并通过实验验证了所提方法的有效性，但仍存在一些有待进一步研究和完善的方面。

首先，在攻击流量建模方面，本文采用三阶张量对时间、空间与特征信息进行联合表示，虽然能够较好地刻画攻击流量的时空协同行为，但在网络规模进一步扩大或流量维度持续增加的情况下，张量建模与分解的计算复杂度仍可能对实时性产生影响。后续研究可结合更高效的在线张量分解算法或维度自适应机制，进一步降低计算开销。

其次，在防御决策建模方面，本文采用深度强化学习方法对防御策略进行优化，奖励函数中对攻击抑制效果与资源消耗的权衡主要依赖经验参数设定。如何在不同网络环境和业务场景下实现奖励参数的自适应调整，仍有待进一步研究。

此外，本文的实验验证主要基于仿真环境与公开数据集，在真实大规模网络环境中的部署效果尚未得到充分验证。未来可在更复杂的网络拓扑和多类型攻击场景下，对所提方法的鲁棒性与可扩展性进行进一步评估。

在未来研究中，可考虑将本文提出的多模态时空建模思想与更复杂的网络行为分析模型相结合，并探索联邦学习或分布式学习框架下的协同防御机制，以提升方法在异构网络环境中的适用性。

参考文献

[1] Karakus M ,Durresi A .Quality of Service (QoS) in Software Defined Networking (SDN): A survey[J].Journal of Network and Computer Applications,2017.

[2] Bonfim S M ,Dias L K ,Fernandes L F S .Integrated NFV/SDN Architectures[J].ACM Computing Surveys (CSUR) ,2019,51(6):1-39.

[3] Najar A A, Naik S M, Lone F R, et al. A novel CNN-enhanced detection and mitigation of DDoS attacks in SDN[J]. Cluster Computing, 2025, 28(6): 347.

[4] Wang J, Wang L, Wang R. MFFLR-DDoS: An encrypted LR-DDoS attack detection method based on multi-granularity feature fusions in SDN[J]. Mathematical Biosciences and Engineering, 2024, 21(3): 4187-4209.

[5] Gao D, Liu Z, Liu Y, et al. Defending against Packet-In messages flooding attack under SDN context: D. Gao et al[J]. Soft Computing, 2018, 22(20): 6797-6809.

[6] Ahmad I, Namal S, Ylianttila M, et al. Security in software defined networks: A survey[J]. IEEE Communications Surveys & Tutorials, 2015, 17(4): 2317-234.

[7] 葛晨洋, 刘勤让, 裴雪, 等. 软件定义网络中高效协同防御分布式拒绝服务攻击的方案[J]. 计算机应用, 2023, 43(08): 2477-2485.

[8] El Kamel A, Eltaief H, Youssef H. On-the-fly (D) DoS attack mitigation in SDN using Deep Neural Network-based rate limiting[J]. Computer Communications, 2022, 182: 153-169.

[9] Elubeyd H, Yiltas-Kaplan D. Hybrid deep learning approach for automatic DoS/DDoS attacks detection in software-defined networks[J]. Applied Sciences, 2023, 13(6): 3828.

[10] Yuan B, Zhang F, Wan J, et al. Resource investment for DDoS attack resistant SDN: a practical assessment[J]. Science China Information Sciences, 2023, 66(7): 172103.

[11] Xu J, Li X, Wang P, et al. Multi-modal noise-robust DDoS attack detection architecture in large-scale networks based on tensor SVD[J]. IEEE Transactions on Network Science and Engineering, 2022, 10(1): 152-165.

[12] Bakar R A, De Marinis L, Cugini F, et al. FTG-Net-E: A hierarchical ensemble graph neural network for DDoS attack detection[J]. Computer Networks, 2024, 250: 110508.

[13] 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.

[14] Santos R, Souza D, Santo W, et al. Machine learning algorithms to detect DDoS attacks in SDN[J]. Concurrency and Computation: Practice and Experience, 2020, 32(16): e5402.

[15] Madoune S A, Senouci S, De Jiang D, et al. A novel approach for real-time DDoS detection in SDN using dimensionality reduction and ensemble learning[J]. Journal of Information Security and Applications, 2025, 94: 104195.

[16] Perez-Diaz 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.

[17] Chen S R, Chen S J, Hsieh W B. Enhancing Machine Learning-Based DDoS Detection Through Hyperparameter Optimization[J]. Electronics, 2025, 14(16): 3319.

[18] Abu Bakar R, Huang X, Javed M S, et al. An intelligent agent-based detection system for

DDoS attacks using automatic feature extraction and selection[J]. Sensors, 2023, 23(6): 3333.
[19] Prabhu V, Balamurugan P. Low-rate DDoS attack detection in SDN using modified condense net and adaptive snow leopard optimization: Prabhu and Balamurugan[J]. Journal of Computer Virology and Hacking Techniques, 2025, 22(1): 6.
[20] Sun W, Guan S, Wang P, et al. A hybrid deep learning model based low‐rate DoS attack detection method for software defined network[J]. Transactions on Emerging Telecommunications Technologies, 2022, 33(5): e4443.
[21] Omer S Z E, Hashim F, Sali A, et al. Binary classification of low-rate DoS attacks using long short-term memory feed-forward (LSTM-FF) intrusion detection system (IDS)[J]. Engineering Science and Technology, an International Journal, 2025, 66: 102049.
[22] Li K, Zhou H, Tu Z, et al. AT-GCN: A DDoS attack path tracing system based on attack traceability knowledge base and GCN[J]. Computer networks, 2023, 236: 110036.
[23] Biradar J, Shah S, Naik T. Attention Augmented GNN RNN-Attention Models for Advanced Cybersecurity Intrusion Detection[J]. arXiv preprint arXiv:2510.25802, 2025.
[24] Lyu M, Gharakheili H H, Russell C, et al. Hierarchical anomaly-based detection of distributed DNS attacks on enterprise networks[J]. IEEE Transactions on Network and Service Management, 2021, 18(1): 1031-1048.
[25] Wang X, Liu J, Wu Y, et al. Dynamic event‐triggered leader‐following bipartite consensus of second‐order multi‐agent systems under DoS attacks[J]. International Journal of Robust and Nonlinear Control, 2024, 34(15): 10731-10749.
[26] Fan Q, Li X, Wang P, et al. IDAD: An improved tensor train based distributed DDoS attack detection framework and its application in complex networks[J]. Future Generation Computer Systems, 2025, 162: 107471.
[27] Li S, Xu J, Liu P, et al. Truncated lanczos-TSVD: An effective dimensionality reduction algorithm for detecting DDoS attacks in large-scale networks[J]. IEEE Transactions on Network Science and Engineering, 2024, 11(5): 4689-4703.
[28] Ekle O A, Eberle W. Adaptive-GraphSketch: Real-Time Edge Anomaly Detection via Multi-Layer Tensor Sketching and Temporal Decay[J]. arXiv preprint arXiv:2509.11633, 2025.
[29] Tebbaa K, Chakir O, Maleh Y, et al. Mitigating DDoS attacks in software-defined networks: a systematic literature review of machine learning and deep learning approaches[J]. Iran Journal of Computer Science, 2026, 9(1): 5.
[30] Kabdjou J, Shinomiya N. Improving quality of service and HTTPS DDoS detection in MEC environment with a cyber deception-based architecture[J]. IEEE Access, 2024, 12: 23490-23503.
[31] 王涛, 陈鸿昶, 程国振. 基于网络资源管理技术的 SDN DoS 攻击动态防御机制[J]. 计算机研究与发展, 2017, 54(10): 2356-2368.
[32] Kumar A, Agarwal M. Quick service during DDoS attacks in the container-based cloud environment[J]. Journal of Network and Computer Applications, 2024, 229: 103946.
[33] Janakiraman S, Deva Priya M. A deep reinforcement learning-based DDoS attack mitigation scheme for securing big data in fog-assisted cloud environment[J]. Wireless Personal Communications, 2023, 130(4): 2869-2886.
[34] Ji L, Zhao R, Dang Y, et al. Query join order optimization method based on dynamic double deep q-network[J]. Electronics, 2023, 12(6): 1504.
[35] Dong S, Cheng G, Liu W. Poseidon: Intelligent Proactive Defense against DDoS Attacks in

Edge Clouds[J]. Computer Networks, 2026: 112025.
[36] Aydin H, Aydin G Z G, Sertbaş A, et al. Design of an autonomous multi-agent-based defense system against DDoS attacks in the Industrial Internet of Things (IIoT) environment[J]. The Computer Journal, 2025, 68(11): 1711-1731.
[37] Feng H, Zhang W, Liu Y, et al. Multi-domain collaborative two-level DDoS detection via hybrid deep learning[J]. Computer Networks, 2024, 242: 110251.
[38] Chen X, Chen Y, Feng W, et al. Real-time DDoS defense in 5G-enabled IoT: A multidomain collaboration perspective[J]. IEEE internet of things journal, 2022, 10(5): 4490-4505.
[39] 冯惠粉. 可编程网络中多域协作式 DDoS 攻击防御机制研究[D]. 北京交通大学, 2025.
[40] 朱海婷, 魏明岗, 刘丰宁, 等. 基于异步个性化联邦学习的 DDoS 攻击检测与缓解[J]. 计算机学报, 2025, 48(04): 808-827.
[41] 周海, 沈岳, 李伟. SDN 中 DDoS 攻击与防御研究综述[J]. 网络安全技术与应用, 2025, (01): 12-21.
[42] Sinha M. A comprehensive survey of DDoS attack defense systems for different SDN architectures[J]. Computer Networks, 2025: 111711.
[43] 许静. 基于张量模型的大规模 DDoS 攻击检测方法研究[D]. 云南大学, 2023.
[44] Satpathy S, Tripathy U, Swain P K. Cloud-based DDoS detection using hybrid feature selection with deep reinforcement learning (DRL)[J]. Scientific Reports, 2025, 15(1): 36546.
[45] 左青云, 陈鸣, 赵广松, 等. 基于 OpenFlow 的 SDN 技术研究[J]. 软件学报, 2013, 24(05): 1078-1097.
[46] Li Q, Zou X, Huang Q, et al. Dynamic packet forwarding verification in SDN[J]. IEEE Transactions on Dependable and Secure Computing, 2018, 16(6): 915-929.
[47] 陈兴蜀, 滑强, 王毅桐, 等. 云环境下 SDN 网络低速率 DDoS 攻击的研究[J]. 通信学报, 2019, 40(06): 210-222.
[48] Lee J, Choi D, Sael L. CTD: Fast, accurate, and interpretable method for static and dynamic tensor decompositions[J]. PloS one, 2018, 13(7): e0200579.
[49] 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.
[50] 高阳, 陈世福, 陆鑫. 强化学习研究综述[J]. 自动化学报, 2004, (01): 86-100..
[51] 刘全, 翟建伟, 章宗长, 等. 深度强化学习综述[J]. 计算机学报, 2018,41(01): 1-27.
[52] Chahoud M, Sami H, Mizouni R, et al. Reward shaping in DRL: A novel framework for adaptive resource management in dynamic environments[J]. Information Sciences, 2025, 715: 122238.
[53] Lee S, Song B C. Knowledge transfer via decomposing essential information in convolutional neural networks[J]. IEEE Transactions on Neural Networks and Learning Systems, 2020, 33(1): 366-377.
[54] Diao H ,Li G ,Xu S , et al.Self-distillation enhanced adaptive pruning of convolutional neural networks[J].Pattern Recognition,2025,157110942-110942.DOI:10.1016/J.PATCOG.2024.110942.
[55] 杨高磊. 基于 SDN 可编程数据面的 DoS 攻击检测方法研究[D]. 西安电子科技大学, 2022.
[56] M. N Y ,Cesar V ,Arturo J P , 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.
[57] 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.

[58] Yao Yuan ,He Junjiang ,Li Tao , et al.An Automatic XSS Attack Vector Generation Method Based on the Improved Dueling DDQN Algorithm[J].IEEE Transactions on Dependable and Secure Computing,2024,21(4):2852-2868.

[59] Wu Y ,Hu Y ,Wang J , et al.An active learning framework using deep Q-network for zero-day attack detection[J].Computers & Security,2024,139,103713.

[60] Wainwright R, Bagheri M, Salama A, et al. Software-Defined Networking Security Detection Strategies and Their Limitations with a Focus on Distributed Denial-of-Service for Small to Medium-Sized Enterprises[J]. Applied Sciences, 2025, 15(23): 1-21.

[61] Liu H, Zhang Y, Ding J, et al. Tensor-train-based incremental high order dominant z-eigen decomposition for multi-modal intelligent transportation prediction[J]. IEEE Transactions on Intelligent Transportation Systems, 2023, 25(3): 2534-2544.

[62] 杨贤志. 基于深度学习的目标检测网络轻量化方法[D]. 南京邮电大学, 2021.

攻读学位期间的学术论文与研究成果

论文情况：

[1] 徐泽鹏, 舒兆港, 陈淑武, 等. 面向SDN流表多模态感知与DRL协同防御DDoS方法[J]. 计算机应用研究, 2026, 43(02):596-603. DOI:10.19734/j.issn.1001-3695.2025.06.0219.（第一作者，已发表）

[2] Zhuang T,Shu Z,Chen S,et al. Intelligent algorithm for dynamic handling of DDoS based on action cost in a dual-Stack environment[J]. Computer Networks,2026（278）：112105.（第六作者，已发表）

科研项目：

[1] 福建省科技厅福厦泉协同创新平台项目，“Research and industrial application of high reliability intelligent gateway devices and systems based on LLM and SD-WAN”，No. 2025E3012，2025.09-2027.09（项目主要成员，负责智能网关资源感知和动态防御相关任务）

[2] 来自网络通信公司的产学研项目，“Research on intelligent monitoring and optimization of power information network and its industrial application”，No. KH240131A，2024.04-2027.04（项目主要成员，负责电力网络资源感知优化算法设计相关任务）

获得奖项：

[1] 获得奖项：学业三等奖学金

[2] 获得奖项：院三好学生

[3] 获得奖项：校社会先进个人

[4] 获得奖项：优秀毕业生

[5] 获得奖项：福建农林大学数学建模竞赛（三等奖）

[6] 获得奖项：2024 中国高校计算机大赛-网络技术挑战赛省赛（三等奖）

[7] 获得奖项：第九届华为 ICT 大赛实践赛省赛网络赛道高教组（三等奖）

[8] 获得奖项：2025 中国高校计算机大赛-网络技术挑战赛省赛（三等奖）

致谢

白驹过隙，三年的读书生涯即将走入尾声，回首往日，仿佛开学还在昨天。一直期待毕业走进社会的我，此刻更多的是不舍和遗憾。三年时间很短，但是这期间却发生了很多事。亲人离世的悲痛、获奖的喜悦，亦或反复推倒重来实验的疲倦，在此刻、无论怎样，都画上了句号。

在此，首先要感谢舒兆港老师带我迈进 SDN 研究的大门。这一领域前景广阔、分支庞大，与深度学习的结合，极大扩展了我的视野。在这段求知路上，不仅给予了我悉心的指导，还教会了我如何独立思考、勇敢探索，为我提供了良好的学习环境。其次我要感谢诸位师兄师姐与同门，不管是生活还是学习，都帮我甚多，也给我的校园生活增添了很多欢乐。最后，感谢我的父母和爷爷奶奶，是他们的支持和理解，让我顺利完成了读研。

时维孟夏、岁在丙午，三载寒窗、一朝结业，回首来路，有悲有喜，有苦有甘。所谓 “纸上得来终觉浅，绝知此事要躬行”。今将辞校入社，必以所学致所用，以初心致远方。愿此去前程似锦，再相逢依旧如故。