基于云网关的边缘智能体架构方案

龚勃，曾莹，朱姝，张慷，许燕萍
（中国电信股份有限公司上海分公司，上海 200041）

摘要：基于云网关的边缘智能体是融合了边缘计算与人工智能（AI）技术，部署在边缘设备与边缘云网关的智能程序或系统。该边缘智能体具有基于云网关的应用识别能力，具备边端策略自适应、可扩展性强等优势，具有很广泛的应用前景，同时其对架构也提出了一定的要求。主要分析了基于云网关的边缘智能体架构方案如何在运营商级城域网上部署，以实现边缘智能体自适应、可扩展的优势，该架构可为后续在新型城域网部署智能体服务提供参考。

关键词：云网关；边缘智能体；虚拟化深度包检测；融合边缘
中图分类号：TP393；TN929
文献标志码：A
doi: 10.11959/j.issn.1000−0801.DXKX250650

Architecture scheme for edge AI agents based on cloud gateway

Gong Bo, Zeng Ying, Zhu Shu, Zhang Kang, Xu Yanping
China Telecom Corporation Ltd. Shanghai Branch, Shanghai 200041, China

Abstract: The edge AI agent based on the cloud gateway is an intelligent program or system which integrates edge computing and artificial intelligence technologies. This agent is deployed on edge devices and edge cloud gateways. It possesses the capability of identifying applications based on the cloud gateway, supports adaptive edge strategies, offers high scalability, and has broad application prospects. At the same time, it also can impose certain requirements on its architecture. The architectural solution of the edge AI agent based on the cloud gateway was primarily analyzed, which could be deployed and implemented on a carrier network to realize the adaptive and scalable advantages of the edge AI agent, serving as a reference for providing intelligent agent services in the deployment of next-generation metropolitan area networks.

Key words: cloud gateway, edge AI agent, vDPI, converged edge

0 引言

在智能交通、智慧城市、工业互联网、家庭智能终端等场景的驱动下，多样化的终端设备（如传感器、摄像头、工业控制器、智能家居等）在网络的“最后一公里”源源不断地产生着海量数据。若将所有原始数据不加区分地传输到云端数据中心进行处理，将导致难以忍受的网络时

收稿日期：2025−11−06；修回日期：2026−04−14

延、高昂的网络带宽成本，并引发对数据隐私和安全性的担忧[1]。

为解决这一现状，融合边缘（converged edge）的概念被提出来，它本质上并非要取代云计算，而是对其能力的延伸与补充。融合边缘指的是在网络边缘侧，将计算、网络、存储和应用核心能力进行平台化融合，形成一个就近提供终端服务的环境。

云网关（cloud gateway）作为电信运营商在边缘侧部署的虚拟化关键网元，主要负责网络协议的转换、根据数据初步汇聚，并安全地向互联网或内网特定的应用传输。

虚拟化深度包检测（virtual deep packet inspection，vDPI）技术应用于云网关，从一定意义上为云网关赋予了感知能力，它能够对网络数据包的应用层（第7层）内容进行深度解析和特征匹配，从而识别出具体的应用类型、用户行为，甚至内容中的关键信息。

当具备vDPI能力的云网关与边缘计算相结合时，边缘智能体（edge AI agent）孕育而生，其核心功能就是在离用户更近的地方实现从“感知”到“决策”再到“行动”的完整高效闭环。

1　具备vDPI能力的云网关的技术特性

传统云网关在集成vDPI功能后从“连通型”基础转发网元演进成为“感知型”智能网元。其技术特性主要体现在以下几个方面。

1.1　深度业务感知与上下文理解

传统云网关通过互联网协议（IP）地址和端口号进行策略控制，但在当前动态端口和加密流量普及的网络环境下，这种方法的有效性通常比较差，而vDPI通过特征码匹配、行为分析和加密流量分析等技术，通过机器学习和深度学习，能够从网络流量中精准识别上千种应用程序。本文讨论的vDPI技术主要使用静态规则检测、动态规则检测、基于人工智能（AI）模型的检测，本文重点针对基于AI模型的检测方案进行详细阐述。

AI模型为加密流量检测增加了泛化能力，以流量特征或原始数据流/包序列为输入，输出概率最高的业务类别或行为标签。现有基于AI模型的加密流量检测方法包括基于人工特征的经典机器模型方法（如随机森林）[2-3]以及基于使用神经网络进行自动特征提取的深度学习方法（如CNN、RNN、Transformer等）[4-6]。AI模型的优势在于其强大的拟合能力，能够自动提取超越明文特征的深层时序与结构模式，有效应对加密、混淆等对抗性场景，显著提升检测体系的覆盖范围和稳健性，常见AI模型见表1[7-9]。

1.2　精细化策略与实时控制

基于深度感知的结果，云网关可以根据细颗粒度的感知设置精细化策略，通常有以下几个方面的应用策略。

（1）智能路由与负载均衡策略：将关键业务流量导向特定链路，例如，将视频监控流量导向本地存储服务器，而将普通上网流量导向互联网，提供类似局域网的边缘云存储服务。

（2）业务质量（QoE）保障策略：当vDPI识别出视频、会议或其他应用流量后，可针对该应用提供区别于其他应用更高的优先级和带宽保证，有效降低卡顿，通常应用在办公场景。

（3）安全威胁管控策略：实时检测并阻断恶意软件通信、点对点内容分发网络（PCDN）等异常网络行为，可应用在网络反诈拦截、PCDN行为管理等应用场景。

1.3　数据提取与分析

边缘智能体之所以成为可能，是因为vDPI无须将全部原始数据上传，而是可以在边缘侧进行报文的实时分析和聚合[10]。例如，当vDPI探测到用户需要发起应用保障时，根据设定的规则开展业务质量保障，当用户应用保障使用结束时，又能主动恢复常用规则。

表1 常见AI模型

模型	类别	说明
随机森林（RF）	机器学习	一种集成学习算法，通过构建多棵决策树并综合其投票结果来进行预测，具有很好的抗过拟合能力
支持向量机（SVM）	机器学习	一种寻找能将不同类别样本在特征空间中最佳分离的最大间隔超平面的分类算法
K-近邻（KNN）	机器学习	一种基于实例的懒惰学习算法，通过判断样本在特征空间中最近邻的*K*个样本的多数类别来进行分类
决策树（DT）	机器学习	一种模拟树形决策过程的模型，通过一系列基于特征的if、then规则，将数据递归分割成更纯的子集
卷积神经网络（CNN）	深度学习	一种专为处理网格状数据（如图像、序列等）而设计的神经网络，通过卷积核来提取局部空间的特征
循环神经网络（RNN）	深度学习	一种为处理序列数据而设计的神经网络，其内部循环连接允许信息持久化，可捕捉序列中的时间依赖关系
自编码器（AutoEncoder）	深度学习	一种通过无监督学习将输入数据压缩成低维编码后再重构输出的神经网络
图神经网络（GNN）	深度学习	一种直接对图结构数据进行操作的神经网络，通过聚合邻居节点信息来学习节点和图的表示[7-9]
自注意力网络（Transformer）	深度学习	一种基于自注意力机制的深度学习架构，摒弃了传统循环神经网络（RNN）的序列依赖结构，通过并行化处理序列数据实现了高效的全局依赖建模

1.4 虚拟化与按需部署

vDPI系统基于容器方案部署（即docker-container方式），以容器编排平台（Kubernetes，K8s）作为控制平面，实现资源调度、隔离与弹性扩缩容。vDPI将深度包检测（deep packet inspection，DPI）引擎封装为容器镜像，并以守护进程集（DaemonSet）或单独工作负载方式部署至具备数据平面开发组件（data plane development kit，DPDK）能力的节点。部署时K8s的CPU Manager、拓扑管理器（topology manager）与大页内存（HugePages）管理模块共同保证vDPI的数据面线程能够获得连续的大页内存、独占中央处理器（CPU）核心，并避免跨非一致性内存访问（non-uniform memory access，NUMA）节点调度。vDPI部署架构如图1所示，包括控制平面、工作节点、DPDK Host主实例，以及运行DPI引擎的容器。

2 基于具备vDPI云网关边缘智能体的技术架构

在了解具备vDPI云网关的特性后，云端智能方案可以得到进一步优化，从而设计一个新的部署架构，根据应用场景的不同，基于新型城域网分别构建云侧、边侧、端侧的智能体架构，云边端智能体部署架构如图2所示。基于图2所示的架构，边缘智能体的应用方案一般有两种。

第一种是仅有边缘智能体提供的应用场景的方案。这一方案通常应用于某个特殊的智能应用场景，例如，当某个园区针对智能视频需求进行部署，这种大模型算法一般在本地部署，现在具备了融合边缘部署边缘智能体的架构后，园区可以将这些大模型算法部署在就近的边缘算力上，同时结合基于vDPI的边缘智能体，可以感知流量中的异常访问并根据策略实施异常管控。

第二种是云、边、端协同的智能体应用场景的方案。当智能应用的服务对象覆盖面广的时候，通常利用云端智能体与端侧进行协同的方案来实现。针对某些有一定实时性要求的场景，云、边、端智能体协同是一个优选方案，实时应用场景边端应用，应用结果汇总到云端，云端智能体再根据不同边端应用要求给予策略指导。

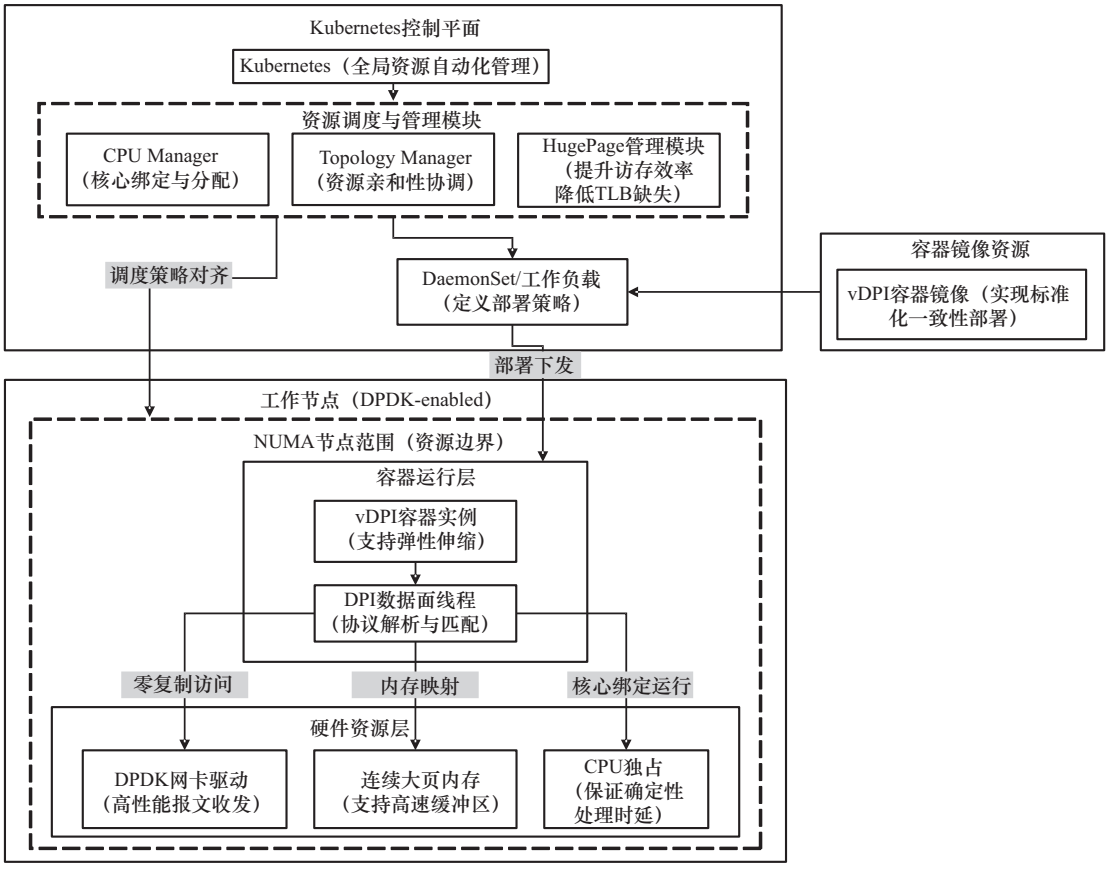


图1　vDPI 部署架构

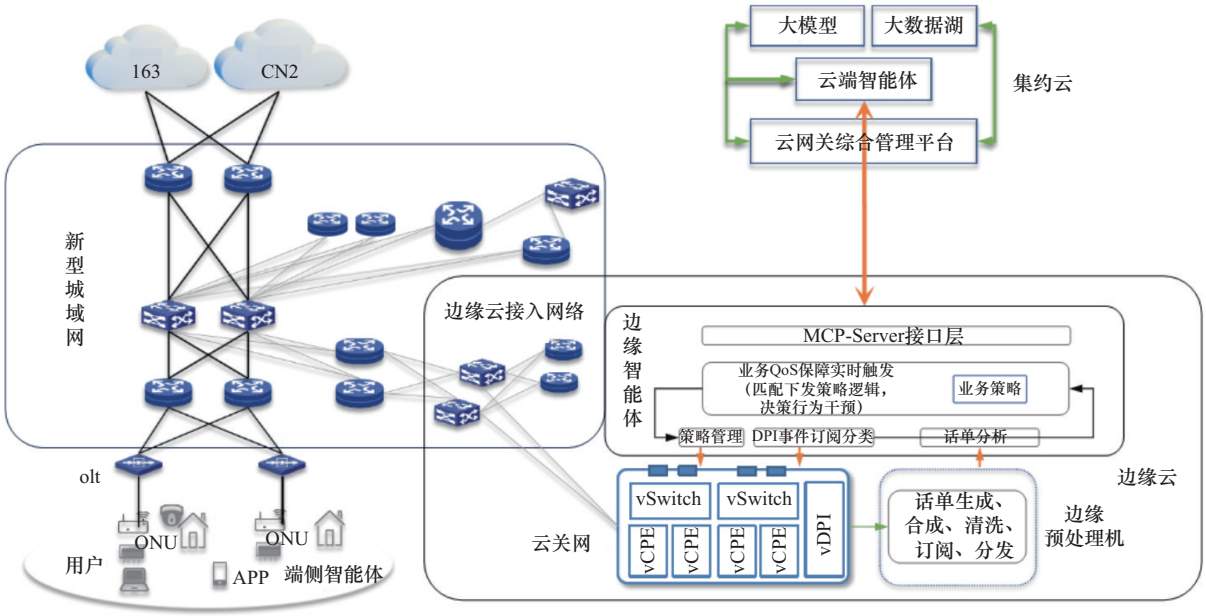


图2　云边端智能体部署架构

基于上述两个不同场景的应用方案，结合具备 vDPI 能力的云网关能力，边缘智能体的架构可以进行分层设计，基于云网关的边缘智能体架构如图3所示。

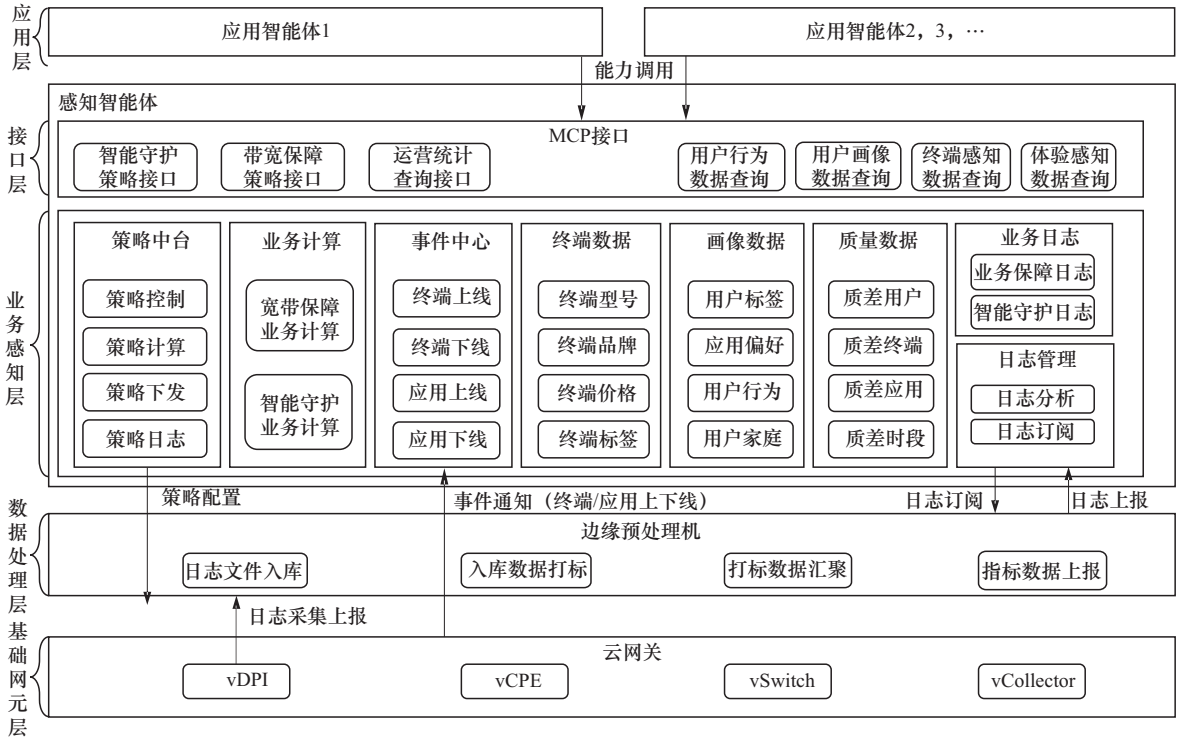


图3　基于云网关的边缘智能体架构

2.1　边缘预处理机

边缘预处理机采用流式计算引擎对接收的话单进行实时处理：首先基于用户账号与终端MAC进行会话关联；随后按业务规则打标（如“视频类”“办公类”“高风险PCDN”）；继而在指定时间窗口内按用户–应用维度聚合关键性能指标（KPI），包括上行/下行速率、平均时延、丢包率、QoE评分（基于ITU-T G.107[11]等模型计算，QoE评分规则见表2）等；最终输出标准化的指标数据记录，写入低时延内存数据库。

2.2　感知智能体策略中台

策略中台是系统的决策核心，集成轻量化AI模型。它基于感知层提供的数据进行智能分析，并驱动业务逻辑，包含策略控制、策略计算、策略下发及日志功能。

为强化边缘智能体的自主决策能力，策略中台集成了轻量化AI模型作为核心推理引擎。AI模型架构原理如图4所示。当前部署的模型主要包括基于MobileNetV2[12]改进的流量分类器、用于QoE预测的轻量长短期记忆（LSTM）网络[13]，以及支持在线策略优化的深度Q网络（deep Q network，DQN）强化学习模块[14]。模型压缩封装后，运行于Kubernetes管理的边缘容器内，单模型推理时延控制在10 ms以内。模型的输入源自数据处理层生成的标准化指标数据（如应用类型、带宽占用、丢包率等），输出为具体的策略动作（如优先级调整、带宽配额、限速阈值等）。模型更新采用联邦学习框架[15]：各边缘节点在本地训练模型增量，仅将加密梯度上传至区域聚合服务器，避免原始用户数据外泄，同时实现全局模型协同进化。该机制使边缘智能体不仅可执行预设规则，更能基于历史经验动态优化决策策略，真正体现“智能体”的自适应特性。

策略中台的策略计算模块是提升网络智能化、实现主动服务能力的核心模块，它可将抽象的业务需求通过数据与规则匹配转化为精准、动态、可执行的具体配置策略，并具备高效性、可

表2　QoE 评分规则

应用类别	需求及权重	等级	评分区间	时延阈值 /ms	丢包率阈值
在线游戏	核心需求：极低时延（操作响应速度）、低丢包（避免卡顿或掉线） 权重：时延 70%，丢包率 30%	极好	90~100	≤20	≤0.1%
		良好	75~89	20~50	0.1%~1%
		一般	60~74	50~100	1.0%~3.0%
		较差	<60	>100	>3.0%
实时音视频通信	核心需求：超低时延（语音/视频同步）、极低丢包（避免断续或失真） 权重：时延 70%，丢包率 30%	极好	90~100	≤50	≤0.5%
		良好	75~89	50~100	0.5%~2%
		一般	60~74	100~150	2.0%~5.0%
		较差	<60	>150	>5.0%
在线会议	核心需求：低时延（互动流畅性）、低丢包（画面/语音清晰） 权重：时延 50%，丢包率 50%	极好	90~100	≤50	≤0.5%
		良好	75~89	50~100	0.5%~2%
		一般	60~74	100-150	2.0%~5.0%
		较差	<60	>150	>5.0%
网页浏览	核心需求：中等时延（页面加载速度）、中等丢包（避免重传时延） 权重：时延 50%，丢包率 50%	极好	90~100	≤100	≤0.1%
		良好	75~89	100~200	0.1%~1%
		一般	60~74	200~300	1.0%~3.0%
		较差	<60	>300	>3.0%
文件下载	核心需求：低丢包（避免重传）、中等时延（用户对时延容忍度较高） 权重：时延 40%，丢包率 60%	极好	90~100	≤200	≤0.1%
		良好	75~89	200~500	0.1%~1%
		一般	60~74	500~1 000	1.0%~3.0%
		较差	<60	>1 000	>3.0%
直播流媒体	核心需求：低丢包（避免卡顿）、中等时延（用户对时延容忍度较高） 权重：时延 40%，丢包率 60%	极好	90~100	≤300	≤0.5%
		良好	75~89	300~800	0.5%~2%
		一般	60~74	800~1 500	2.0%~5.0%
		较差	<60	>1 500	>5.0%

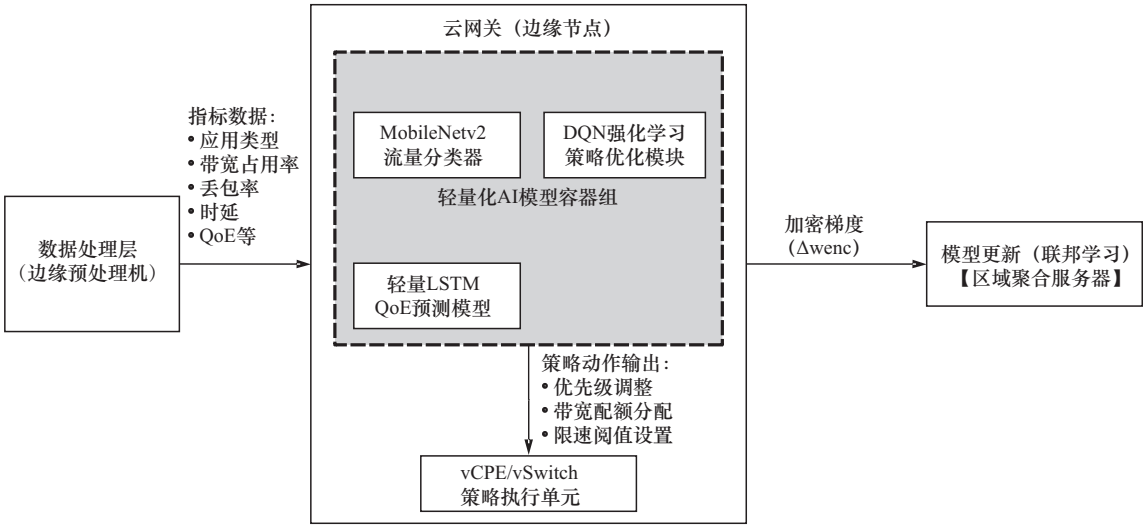


图4　AI 模型架构原理

扩展性与可靠性，为后续策略执行与效果评估奠定基础。

以“上网保障”业务为例，策略计算模块的工作可进一步细化为如下 5 点。

（1）指令解析与场景识别

系统解析策略指令，识别业务类型（如“应用上网保障”）、目标用户、应用标识、保障时段及优先级等信息。

（2）历史数据提取与建模

根据指令中的应用标识与时段，查询历史流量数据库，提取该应用在相似场景下的最大、平均、分位数流速等统计特征，并建立带宽需求基线模型。

（3）实时数据融合

结合用户当前网络接入质量、设备性能、并发应用状态等实时数据，判断当前是否具备保障条件，并预测保障可能对同一链路其他用户的影响。

（4）规则匹配与动态计算

依据“保障优先但不独占”“阶梯式保障”等业务规则计算具体保障参数。例如：

基础保障带宽=历史最大流速×动态权重 （1）

突发容忍阈值=根据当前链路空闲带宽动态调整 （2）

保障生效/退出机制：设置应用流量检测窗口，上线后自动触发，下线后延迟释放资源，避免频繁切换。

（5）策略方案生成

输出结构化策略方案，例如：

```
{
 "user_id": "{目标用户}",
 "app_id": "{应用标识}",
 "action": "{应用上网保障–保障生效 / 应用上网保障-保障退出}",
 "bandwidth_up": "{保障带宽：上行速率}",
 "bandwidth_down": "{保障带宽：下行速率}",
 "priority": {优先级},
 "valid_from": "{执行_开始时间}",
 "valid_until": "{执行_持续时间}",
 "fallback_policy": "{突发异常应对策略}"
}
```

除“上网保障”外，该模块还可支持下列策略场景，体现其通用性与扩展性。

（1）智能流量管控：在高峰时段对非关键应用进行动态限速，保障整体网络公平性。

（2）突发异常应对：检测到网络时延突增或丢包时，自动切换路由或启用冗余链路。

3 边缘智能体应用实例与仿真

3.1 边缘智能体应用案例

为了加深理解边缘智能体的运行机制，现以家庭宽带用户视频体验劣化场景为例，说明智能体如何实现从“被动投诉”到“主动干预”，从而体现以客户为中心的云网智能化服务能力提升。

某日晚高峰19:45，部署于城域网的云网关中的vDPI模块持续监测到用户U886753（标签：“远程办公+在线教育家庭”）的Zoom会议流量出现异常：连续3个10 s窗口内，上行丢包率超过12%，往返时延（RTT）达320 ms，QoE评分由0.9骤降至0.55。在无新设备上线的情况下，其高带宽娱乐应用（如抖音、腾讯视频）的使用带宽较前一日上升68%。

边缘预处理机将上述多维指标（Zoom QoE下降+娱乐应用流量显著增加+无终端变更）汇聚后，生成“疑似办公体验劣化”事件，并推送至业务感知层。策略中台中的轻量化异常检测模型判定该事件置信度达91%，立即触发以下两级响应。

第一级（本地自治）：自动提升Zoom流量的差分服务代码点（DSCP）优先级至EF（expedited forwarding），并临时限制后台P2P及大文件下载带宽，500 ms内完成策略下发至vCPE，用户会议卡顿现象显著缓解；5 min后，系统检测到QoE恢复至0.85以上，自动解除限速。

第二级（主动服务）：系统将该事件同步写入运营事件中心，并通过模型上下文协议（MCP）接口通知客服智能体。20:00，AI外呼平

台自动拨打用户电话：“您好！我们监测到您刚才的视频会议可能存在卡顿，是否需要工程师远程协助优化网络?”用户确认后，工单自动生成。

此案例中，常规模式需用户主动报障（平均滞后2~24 h），而本文架构通过边端实时感知+智能决策+服务联动，在用户尚未投诉前即完成问题识别、缓解与主动触达，不仅提升净推荐值（NPS），更降低运维成本，充分体现“以用户为中心”的主动服务理念。

3.2　仿真实验与性能评估

为验证本文提出的边缘智能体架构在实际网络环境中的有效性，构建了一套高保真仿真平台，从策略响应时延、带宽成本节约及安全事件拦截时效性3个维度开展对比实验。

3.2.1　实验目的

评估本文所述架构相较于传统云网关方案在以下3方面的能力提升：

（1）本地化实时策略决策的响应速度；

（2）边缘侧流量识别与分流降低上行带宽消耗；

（3）安全事件拦截时效性。

3.2.2　实验环境

流量模拟：使用 T-Rex 流量生成器模拟家庭用户混合业务流（含 Zoom、腾讯会议、抖音、Netflix、PCDN、Web 浏览等），总吞吐量约 8 Gbit/s，其中加密流量占比 82%。

对照组设置：

（1）方案 A（传统架构），仅具备基础网络地址转换（NAT）与服务质量（QoS）功能，策略由远端管理系统下发。

（2）方案 B（本文架构），集成 vDPI+边缘预处理机+本地 AI 策略中台，实现边端闭环决策。

3.2.3　实验结果与分析

实验结果对比见表3。

（1）响应时延：方案 B 因策略计算与执行均在边缘完成，避免了往返云端的 RTT 开销。

（2）带宽节约：在 vDPI 精准识别本地视频流后，将视频应用流量导向边缘存储或 CDN 节点，减少无效上云流量对互联网带宽的占用。

（3）安全拦截：在对模拟的 PCDN 异常外联行为识别后，方案 B 可在首包后 300 ms 内完成识别并下发阻断策略，实现准实时精准防护。

表3　实验结果对比

评估指标	方案 A（传统）	方案 B（本文）	提升效果
策略响应时延（均值）	820 ms	78 ms	↓90.5%
上行带宽占用（峰值）	6.2 Gbit/s	4.0 Gbit/s	↓35.5%
安全事件拦截时效	>5 s	<300 ms	实时阻断

3.2.4　实验结论

该仿真实验结果表明，本文提出的架构在保障低时延决策、优化网络资源利用及提升业务感知精度方面具有显著优势，为在运营商级城域网中规模化部署边缘智能体提供了技术可行性与性能依据。

4　后续边缘智能体演进方向

目前边缘智能体可能仅具备单节点自主决策（如流量调度、安全防护）能力，但在未来2~5年，可逐步实现向多维协同智能跃迁，并与云端智能体协同，实现协同管控，既可单兵作战，又可化零为整开展团队作战，下面是基于技术可行性与近期行业发展趋势，提出的几个演进方向和场景。

（1）主动服务：如未来结合云网关的质差数据，在用户上网体验可能出现质差时，边缘智能体主动预警，提前 AI 外呼、客服或工程师介入，从被动响应到预测式服务，可有效改善用户上网体验。

（2）联动诊断：边缘智能体如结合端侧、云侧智能体，处理故障时，多端会诊，快速定位，降低故障排查时长，有效保障网络稳定。

（3）营销场景：原有用户营销、流失都较依赖月度账单分析，滞后7~15天，通过实时分析用户真实数据，边缘智能体能够刻画用户画像，并

不断根据数据反馈矫正模型，降低原有营销数据孤岛，提高转化率。

5 结束语

本文仅从运营商在融合边缘构建基于云网关的边缘智能体的架构进行了阐述，为后续研究表明：当云网关具备vDPI能力后，可以便利地叠加轻量化AI模型，使得融合边缘节点部署具备自主决策能力的智能体的基础条件，不仅能实现流量精准识别与实时策略执行，未来，随着智能体调用标准的确立与云边协同进化机制的完善，边缘智能体将形成自生长能力底座，成为“融合边缘”战略落地的核心引擎。

本文研究成果为运营商数字化转型提供了可落地的技术框架，也为构建“以用户为中心”的下一代智能网络奠定了理论基础。

参考文献：

[1] 张晓东, 张朝昆, 赵继军. 边缘智能研究进展[J]. 计算机研究与发展, 2023, 60(12): 2749-2769.
Zhang X D, Zhang C K, Zhao J J. State-of-the-art survey on edge intelligence[J]. Journal of Computer Research and Development, 2023, 60(12): 2749-2769.

[2] 田睿, 张雅勤, 董伟, 等. 机器学习在恶意加密流量检测中的应用及研究[J]. 电子技术应用, 2025, 51(4): 1-11.
Tian R, Zhang Y Q, Dong W, et al. The application and research of machine learning in malicious encrypted traffic detection[J]. Application of Electronic Technique, 2025, 51(4): 1-11.

[3] Lu C W, Cao Y X, Wang Z B. Research on intrusion detection based on an enhanced random forest algorithm[J]. Applied Sciences, 2024, 14(2): 714.

[4] 赵馨, 李文博. 基于ASPP-Swin Transformer模型的加密流量识别方法[J]. 通信世界, 2025(20): 29-35.
Zhao X, Li W B. Encrypted traffic identification method based on ASPP-Swin Transformer model[J]. Communications World, 2025(20): 29-35.

[5] Binbusayyis A. Hybrid VGG19 and 2D-CNN for intrusion detection in the FOG-cloud environment[J]. Expert Systems with Applications, 2024, 238: 121758.

[6] 何明枢. 基于机器学习的网络流威胁行为认知分析与研究[D]. 北京: 北京邮电大学, 2022.
He M S. Research on network flow threat behavior cognition based on machine learning[D]. Beijing: Beijing University of Posts and Telecommunications, 2022.

[7] Ahmed M J, Mozo A, Karamchandani A. A survey on graph neural networks, machine learning and deep learning techniques for time series applications in industry[J]. PeerJ Computer Science, 2025, 11: e3097.

[8] 李孟想, 彭闯, 王浩, 等. 基于图神经网络的鲁棒加密流量识别[J]. 电信科学, 2024, 40(6): 89-99.
Li M X, Peng C, Wang H, et al. A robust encrypted traffic identification scheme based on graph neural network[J]. Telecommunications Science, 2024, 40(6): 89-99.

[9] 王志宏, 刘昇然, 池泽桂, 等. 基于多层级图表征增强的加密应用流量识别方法[J]. 计算机科学, 2025, 52(S2): 871-877.
Wang Z H, Liu S R, Chi Z G, et al. Classification of encrypted application traffic enhanced by multi-level graph representation[J]. Computer Science, 2025, 52(S2): 871-877.

[10] Cui T , Lin X , Li S ,et al.TrafficLLM: enhancing large language models for network traffic analysis with generic traffic representation[PP]. (2025-04-15)[2025-10-11]. arXiv:2504.04222.

[11] Wang X, Han Y, Leung V C M, et al. Edge intelligence: on-demand deep learning model co-inference with mobile edge computing for smart city applications[J]. IEEE Communications Magazine, 2023, 61(4): 28-34.

[12] ITU-T Recommendation G.107: The E-model: a computational model for use in transmission planning[S].2022

[13] Sandler M, Howard A, Zhu M L, et al. MobileNetV2: inverted residuals and linear bottlenecks[C]//Proceedings of the 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition. Piscataway: IEEE Press, 2018: 4510-4520.

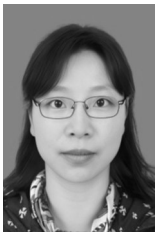
[14] Zhang K, Li M, Liu Z, et al. Federated QoE prediction in telecom networks using lightweight LSTM models[C]//Proceedings of the IEEE International Conference on Communications (ICC). Piscataway: IEEE Press, Seoul, 2024: 1-6.

[15] Chen X, Shi W, Liang W, et al. AI agents in edge computing: architectures, challenges, and opportunities[J]. ACM Computing Surveys, 2025, 57(3): 1-36.

[作者简介]

龚勃（1969−），男，中国电信股份有限公司上海分公司高级工程师，主要研究方向为云网融合、固移融合、物联网及智算网络。

曾莹（1977– ），女，中国电信股份有限公司上海分公司总工程师室高级工程师，集团公司高级专家，主要研究方向为新型城域网、融合边缘、云化网关、vDPI、网络安全、数据安全及应用安全。



朱姝（1981– ），女，中国电信股份有限公司上海分公司总工程师室副总工程师，主要研究方向为新型城域网、云网融合、云化网关、人工智能。

张慷（1968– ），男，中国电信股份有限公司上海分公司副总工程师，主要研究方向为云网融合、算力网络、人工智能。

许燕萍（1980– ），女，中国电信股份有限公司上海分公司智能云网操作维护中心高级工程师，上海公司一级专家，主要研究方向为云化网关、智慧家庭终端、政企智能终端及终端运营支撑系统实现。