新时期网络服务优化与运行保障探析

刘立罡
上海柯衍建设发展有限公司　上海　200231

摘　要：在数字经济与万物智联加速发展的新时期，网络作为“信息大动脉”，其服务质量与可靠性已关乎国家战略安全与社会经济稳定。用户需求从“连通性”升级为“高可靠、低时延、大带宽、智能化”，而云计算、AI、物联网与5G/6G等技术的融合，使网络架构日益复杂、虚拟化和动态化，传统运维体系难以为继。本文系统剖析当前网络服务的核心痛点，深入探讨智能运维（AIOps）、零信任安全、算力网络协同、自动化闭环控制等前沿范式，构建覆盖“感知-分析-决策-执行-反馈”全生命周期的新型网络服务保障体系，并阐述其在性能优化、安全防护、资源调度与韧性提升等方面的实现路径。最后，前瞻性展望网络服务向内生安全、自智自治、绿色低碳等方向演进的趋势，为建设高效、安全、韧性的新一代信息基础设施提供理论与实践指引。

关键词：网络服务优化；运行保障；智能运维；零信任；算力网络

引言

我们正处在一个数据驱动、网络互联的变革时代。总书记强调：“没有网络安全就没有国家安全”，凸显了网络作为国家战略性基础设施的核心地位。随着“东数西算”推进、产业数字化深入及元宇宙、自动驾驶等新业态兴起，网络已从通信管道升级为承载关键业务与创新的基石。然而，其复杂性也呈指数级增长：用户需求日益严苛——远程手术要求毫秒级时延与超高可靠性，云游戏需高带宽低抖动，物联网则追求高连接密度与能效；同时，网络技术栈正经历重构：SDN/NFV实现控制与转发分离及功能灵活编排，5G/6G通过网络切片提供定制化逻辑网络，边缘计算将算力下沉至网络边缘。这些变革虽提升灵活性，却使故障定位、性能调优与安全防护愈发困难。传统依赖静态告警、人工排查的“救火式”运维模式，已难以应对海量、异构、高速变化的新网络环境。因此，构建具备主动感知、智能分析、自动优化与高韧性的网络服务保障体系，成为学术界与产业界共同关注的重大课题。本文系统梳理新时期网络服务优化与运行保障的关键挑战，探究技术逻辑与解决方案，并展望未来发展路径。

1 新时期网络服务面临的核心挑战

1.1 用户体验期望与网络复杂性的矛盾加剧

新时期用户对网络服务的评价标准已从“是否可用”转向“体验如何”。这种体验是多维度的，包括但不限于端到端时延、吞吐量、丢包率、抖动以及服务的连续性和一致性。然而，现代网络是一个由数据中心、广域网、城域网、接入网以及无数虚拟化网元构成的庞大而复杂的巨系统。任何一个环节的微小波动都可能通过级联效应放大，最终导致用户体验的显著劣化。更为棘手的是，由于SDN/NFV的引入，网络拓扑和流量路径不再是静态的，而是根据策略和负载动态调整，这使得基于固定模型的传统性能监控和诊断工具失效，难以建立从用户体验指标（QoE）到网络性能指标（QoS）之间的精确映射关系。

1.2 安全威胁的泛化与高级持续性

在万物互联的背景下，网络攻击面被无限扩大。从传统的边界防御到如今遍布各处的IoT设备、云工作负载和API接口，任何一个薄弱点都可能成为攻击者入侵的跳板。攻击手段也日趋智能化和自动化，高级持续性威胁（APT）能够长期潜伏、横向移动，规避常规检测。传统的“城堡与护城河”式安全模型已无法应对这种无处不在的威胁[1]。此外，数据作为核心资产，其全生命周期的安全——从采集、传输、存储到计算和销毁——都面临着严峻挑战。如何在保证数据高效流动与共享的同时，确保其机密性、完整性和可用性，是新时期网络运行保障必须解决的核心问题。

1.3 资源利用效率与动态业务需求的失衡

云计算和虚拟化技术虽然提升了资源的抽象和池化能力，但资源的静态分配或粗粒度调度往往导致严重的浪费或瓶颈。例如，在非高峰时段，大量服务器和网络带宽处于闲置状态，造成能源和成本的浪费；而在突发流量洪峰（如大型直播、秒杀活动）到来时，又可能因资源不足而导致服务降级甚至中断。这种资源供给与业务需求在时空上的错配，要求网络具备更强的弹性伸缩能力和精细化的资源调度策略，能够根据实时的业务负载和SLA（服务等级协议）要求，动态、精准地分配计

算、存储和网络资源。

1.4 网络韧性与高可用性要求的提升

对于金融交易、电力调度、交通控制等关键信息基础设施而言，网络中断的代价是灾难性的。因此，网络不仅需要高可用性（High Availability），更需要高韧性（Resilience）。高可用性关注的是通过冗余设计减少故障发生的概率，而高韧性则强调在网络遭受攻击或发生故障后，能够快速感知、隔离影响、自我修复并维持核心业务的最低限度运行。在日益复杂的网络环境中，实现这种内生的、自适应的韧性能力，是保障国家和社会稳定运行的基石。

2 网络服务优化与运行保障的关键技术范式

2.1 智能运维（AIOps）：从被动响应到主动预测

智能运维（Artificial Intelligence for IT Operations, AIOps）是利用大数据、机器学习和人工智能技术来增强和部分替代传统IT运维流程的革命性方法。其核心在于构建一个数据驱动的智能中枢。首先，通过遍布全网的探针、代理和日志系统，实时、全量地采集网络设备、服务器、应用及用户体验的多维度指标数据。其次，利用流式计算和时序数据库对这些海量数据进行高效处理和存储[2]。在此基础上，应用机器学习算法（如聚类、分类、回归、异常检测）进行深度分析。例如，通过无监督学习算法（如Isolation Forest, LSTM Autoencoder）可以自动发现偏离正常基线的异常行为，实现故障的早期预警；通过根因分析（RCA）算法，可以在故障发生后，快速从成千上万的关联告警中定位到根本原因，将平均修复时间（MTTR）从小时级缩短至分钟级。AIOps将运维人员从繁琐的数据筛查中解放出来，使其能够专注于更高价值的战略决策。

2.2 零信任安全架构：重塑网络安全边界

零信任（Zero Trust）是一种“永不信任，始终验证”的安全理念，它彻底摒弃了基于网络位置的信任假设。在零信任架构下，无论是内部还是外部的用户、设备或应用，在访问任何资源之前，都必须经过严格的身份认证、授权和持续的安全状态评估。其核心技术支柱包括：强大的身份与访问管理（IAM），确保每个实体都有唯一的数字身份；微隔离（Micro-segmentation），将网络划分为细粒度的安全区域，限制攻击者的横向移动；以及持续的信任评估，结合用户行为分析（UEBA）、设备健康状态等多种上下文信息，动态调整访问权限。零信任架构将安全能力内嵌到网络的每一个环节，实现了从边界防御到全域防护的转变，有效应对了云环境和远程办公带来的安全挑战。

2.3 算力网络协同：实现资源一体化调度

随着“东数西算”等国家战略的实施，算力作为一种新型生产力，其跨地域、跨层级的高效调度成为刚需。算力网络（Computing Power Network）正是为解决这一问题而生，其目标是像调度网络带宽一样调度算力资源。算力网络的核心在于构建一个统一的“算力度量、算力标识、算力路由”体系。通过抽象和标准化不同地理位置、不同架构（CPU/GPU/FPGA）的算力资源，形成一张全局可视的算力地图[3]。当用户发起一个计算任务时，算力网络控制器能够综合考虑任务的算力需求、数据位置、网络时延、能耗成本以及SLA要求，通过智能算法（如强化学习、组合优化）计算出最优的算力节点和网络路径，并下发指令完成资源的自动部署和连接。这种算网深度融合的模式，打破了“计算孤岛”和“网络孤岛”，实现了计算、存储、网络资源的一体化供给和最优匹配。

2.4 自动化闭环控制：迈向自智网络

自动化闭环控制是实现网络自智自治（Autonomous Network）的关键一步。它借鉴了工业控制领域的“感知-决策-执行”闭环思想。在网络中，这意味着：首先，通过Telemetry等技术实现对网络状态的秒级甚至毫秒级实时感知；其次，由一个中央或分布式的策略引擎（Policy Engine）根据预设的业务意图（Intent）和当前网络状态，自动做出优化决策，例如调整路由策略、重分配带宽、迁移虚拟网元等；最后，通过南向接口（如OpenFlow, NETCONF/YANG）将决策自动下发到网络设备执行。整个过程无需人工干预，形成了一个动态、自适应的优化闭环。这种模式能够快速响应网络波动和业务变化，确保网络始终运行在最优状态，是未来6G网络“自配置、自修复、自优化、自演进”愿景的技术基石。

3 新型网络服务保障体系的构建

基于上述关键技术范式，可以构建一个层次化、模块化的新型网络服务保障体系。该体系可划分为四个核心层次：

3.1 全景感知层

这是体系的基础。通过部署轻量级的eBPF程序、gRPC/gNMI接口、以及各类日志和指标采集器，实现对网络基础设施、虚拟化平台、上层应用及最终用户体验的全方位、无侵入式数据采集。重点在于打破数据孤岛，构建一个统一的数据湖，为上层分析提供高质量的“燃料”。

3.2 智能分析层

这是体系的大脑。依托大数据平台和AI引擎，对感

知层汇聚的数据进行实时流处理和离线批处理。该层包含多个智能分析模块，如性能基线建模、异常检测、根因定位、容量预测、安全威胁狩猎等。通过不断训练和迭代AI模型，提升分析的准确性和前瞻性。

3.3 策略决策层

这是体系的指挥中心。它接收来自智能分析层的洞察，并将其转化为具体的、可执行的网络策略。这些策略以高层次的业务意图为输入（例如，“保证视频会议的端到端时延低于50ms”），并通过意图解析引擎转换为底层的、与厂商无关的配置指令。该层还负责维护一个全局的、实时更新的数字孪生（Digital Twin）网络模型，用于在策略执行前进行仿真验证，确保变更的安全性。

3.4 自动执行层

这是体系的手脚。它通过标准化的南向接口，将策略决策层生成的指令自动、批量、一致地推送到相应的网络设备、服务器或云平台。该层强调执行的原子性和事务性，确保变更要么全部成功，要么全部回滚，避免网络进入不一致的中间状态。

这四个层次紧密协作，形成了一个完整的“感知-分析-决策-执行”闭环，并通过持续的反馈机制不断优化自身，从而实现网络服务的持续优化与可靠保障。

4 未来发展趋势与展望

4.1 内生安全与自智网络的深度融合

未来的网络将不再将安全视为一个附加功能，而是将其能力内生于网络的基因之中。安全策略将与网络路由、资源调度等核心功能深度融合，形成“安全即服务”（Security as a Service）的范式[4]。同时，自智网络（Autonomous Network）的发展将进入更高阶段，网络不仅能自主优化性能，还能自主识别和抵御未知威胁，实现安全与效能的双重自洽。

4.2 绿色低碳成为核心设计原则

在全球“双碳”目标的驱动下，网络的能耗问题日益受到关注。未来的网络服务优化将把能效比（Performance per Watt）作为核心KPI之一。通过采用更高效的硬件（如DPU、CXL内存池化）、更智能的休眠与唤醒策略、以及基于AI的绿色路由算法，最大限度地降低网络基础设施的碳足迹，推动信息通信业的可持续发展。

4.3 标准化与开放生态的加速构建

技术的碎片化是阻碍大规模应用的主要障碍。未来，围绕AIOps数据模型、零信任接口、算力网络协议等关键领域，行业联盟和标准组织将加速制定和推广统一的开放标准。一个繁荣的、基于开放API的生态系统将吸引更多的开发者和创新者，共同丰富网络服务优化与保障的能力集，最终惠及整个产业。

5 结语

新时期赋予了网络服务优化与运行保障以全新的内涵和更高的使命。面对日益增长的用户体验需求、复杂多变的安全威胁以及动态弹性的资源调度挑战，传统的运维模式已难以为继。以智能运维、零信任、算力网络和自动化闭环控制为代表的新一代技术范式，为我们指明了破局之道。通过构建一个覆盖全生命周期、具备感知、分析、决策、执行能力的新型保障体系，我们有望实现从“被动救火”到“主动免疫”、从“尽力而为”到“确定性服务”的根本性转变。展望未来，网络将不仅仅是信息的通道，更将成为一个智能、安全、绿色、自治的生命体，为数字中国建设和全球数字经济发展提供坚实、可靠的底座支撑。

参考文献

[1]贺永祥.深化在地服务优化网络生态[J].中国网信,2026,(02):54-56.

[2]保障能级持续提升服务网络不断优化[N].新民晚报,2025-12-22(006).DOI:10.28892/n.cnki.nxmwb.2025.002881.

[3]蔡自伟,盛敏,刘俊宇,等.空地一体化网络服务连续性保障的低功耗通信与控制联合优化方法[J].电子与信息学报,2024,46(05):1920-1930.

[4]刘双月,尹君.基于NWDAF的5G-A网络智能化服务质量保障方案研究[J].广东通信技术,2026,46(03):8-14.