大数据与人工智能技术在计算机网络系统中的应用研究

王子虎
江西工程学院智慧产业学院　江西新余　338000

摘　要：在通信需求不断增长的背景下，计算机网络系统需更高效的智能化支撑。大数据与人工智能技术的融合应用能够为网络架构优化、数据处理提速及安全机制升级提供技术基础。本文聚焦大数据与人工智能技术在计算机网络系统中的应用研究，分析了其在提升网络数据处理能力、提高信息智能识别效率及增强系统协同运行能力等方面的重要意义，提出构建智能采集系统、引入深度学习算法及强化多源数据融合等策略，旨在推动网络系统向智能方向发展。

关键词：大数据；人工智能；计算机网络

引言

计算机网络是信息社会的基础设施，其运行效率能够关系到数据时代的技术支撑力。数据规模不断增长，传统网络体系在处理效率、资源调配及响应能力方面面临日益严峻的挑战。大数据技术能够提供整合数据资源的能力，帮助网络系统识别结构复杂、更新频繁的信息内容；人工智能技术则能为网络运转提供算法支持，让系统在处理路径、异常识别等方面具备主动分析的能力。两类技术的结合能够推动网络从静态响应机制转向动态分析体系，在保证数据吞吐的基础上提升系统运行的稳定性。

1 大数据与人工智能技术在计算机网络系统中的应用意义

1.1 提升网络数据处理能力

大数据技术能够为系统提供高容量、快处理的数据支持，让网络在多任务并发的状态下维持稳定运行。信息传输密度不断上升，数据之间的关联关系日益复杂，传统依赖静态逻辑的处理方式难以满足当前系统的即时性要求。引入人工智能可使网络在处理过程中具备动态识别的能力，能够根据数据特征及时调整运行策略，提升处理过程的精准性[1]。不同类型的数据可被有效分类，减少系统的计算压力，提升整体运行效率。增强信息处理能力也意味着系统在面对异常或突发请求时能够更快做出判断，保障通信过程的流畅性。资源分配更为合理，数据调度更加有序，能够让网络架构具备持续优化的内生动力，在实际应用中表现出更高的技术适应性。

1.2 提高信息智能识别效率

大数据技术能汇聚多维度信息资源，为系统识别提供丰富的特征支持，让数据在进入处理流程前就具备初步筛选的基础条件。人工智能技术能借助算法识别规则或提取特征模式，在复杂数据中迅速定位有效信息，减少误判。系统经过多轮训练形成识别路径，让识别过程贴合实际需求，对异常数据或噪声信息的快速剔除，能减轻系统负担，让通信链路保持稳定流畅[2]。提升识别效率也意味着安全机制响应更及时，能够缩短系统反应时间，增强整体控制能力。精准的识别能力还能辅助网络资源的合理调配，让高频数据获取优先通道，提升服务响应的实时性。多个识别过程的并行处理还能拓宽系统处理范围，让网络对复杂场景具备持续适应能力。

1.3 增强系统协同运行能力

计算机网络系统内部包含多个功能模块，如果彼此之间缺乏有效协同，容易导致资源浪费。大数据技术能为各模块提供统一的数据依据，让操作在同一信息背景下进行，降低因信息偏差带来的运行误差[3]。人工智能技术则能借助算法优化任务分配流程，让系统中的各节点根据当前状态灵活应对任务变动，形成清晰有序的协作机制。节点之间能利用智能判断实现资源共享，减少因重复处理引发的性能负担。调度策略经过动态调整，能够自动协调各部分在运行过程中的任务负载，让高频处理区域保持稳定，低频区域具备扩展空间。不同模块间的配合效率提升后，数据传输路径变得更短，响应速度也更快。多模块之间的信息同步性增强，还能提升故障检测的及时性，避免扩散问题。持续增强协同能力能让系统具备面向复杂应用场景的稳定承载力，为网络长期高效运行提供结构保障。

ISSN: 2661-3719(Print); 2661-3727(Online)

1.4 推动网络架构智能升级

传统网络架构大多依赖静态配置或规则驱动，难以适应当下多任务的复杂通信需求。大数据技术能够为调整网络结构提供丰富的决策依据，全面分析流量分布、用户行为或资源利用状况，让架构设计更贴合实际应用。引入人工智能技术能让网络具备根据实时运行状态自动调整参数的能力，实现结构功能的动态适配。网络节点之间可实现任务自动分发，通信路径能够按需重构，系统整体具备更强的灵活性。在架构层面，智能算法优化传输逻辑、路由策略或负载平衡机制能让资源分配更加精准，避免局部拥堵影响整体性能。同时，系统对于异常状态的感知能力明显增强，能够快速做出调整，保持通信稳定。升级后的架构还能够支持更多复杂业务，具备良好的拓展性，为持续技术演进奠定坚实基础。

2 大数据与人工智能技术在计算机网络系统中的应用策略

2.1 构建智能采集系统，提升数据获取效率

引入人工智能算法与大数据处理能力，系统能够在多源异构环境下识别有效信息并实时提取特征。数据采集过程由静态规则驱动转向动态条件控制，能让采集节点具备适应场景变化的能力。物联网终端在采集任务中不再局限于简单上传，而能根据设定阈值判断采集时机，过滤冗余内容，提高系统带宽利用率。网络结构中各采集模块利用算法协同，能缩短响应时间，减少重复访问，提升整体链路通畅度。数据质量得到保障，系统负载更加可控，为后续分析与决策奠定可靠基础。

在复杂通信场景中，数据来源广泛且结构类型多变，采集过程面临实时性及准确性的双重要求。借助在网络系统中集成智能采集模块，设备可基于特定识别规则判断采集目标的重要程度。在通信监控中，智能模块可依据数据包的频率、协议特征或行为模式，快速筛选出可能存在异常的内容，而不对全部数据进行无差别提取。这种按需采集机制能够降低处理量，减少数据冗余，提高系统响应速度。在物联网场景下，传感器能借助边缘算法初步判断数据，只上传具有价值的数据片段，减轻核心服务器的压力。另外，多点分布式采集结构支持任务同步或调度优化，当部分节点出现延迟，其他节点可根据系统策略接管采集任务，保障整体网络连续运行。在数据归集过程中，系统会自动识别格式差异并完成统一结构转化，避免信息在流转中因格式冲突造成丢失。采集行为全过程配合大数据分析平台，能够实时反馈采集质量状态，辅助运维人员调整采集策略。借助完善技术机制，智能采集系统能够提升数据获取效率且增强网络的稳定性，让网络体系更具应对复杂应用场景的能力（如图 1）。

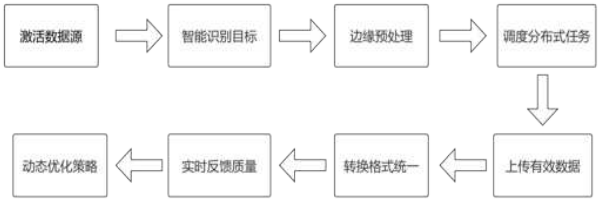

图 1 智能采集系统运行流程图

2.2 应用深度学习技术，优化网络运行逻辑

应用深度学习技术能有效优化计算机网络系统的运行逻辑，提升整体决策效率。深度学习依赖多层神经结构自主提取数据特征，能够从历史运行数据中总结模式，在复杂的网络状态下提供精准的判断依据。系统借助训练生成的模型，能在不同条件下自动调整路由选择、流量控制或资源调配方案，减少人为干预。决策过程能依据数据关联性实现动态修正，让网络在面对高并发请求、节点波动或异常数据时保持响应一致性。深度学习的持续优化能力还能保障系统在长期运行中的适应性，为网络智能演进提供支持。

2.3 强化多源数据融合，增强智能判断能力

强化多源数据融合能够提升计算机网络系统的智能判断能力，在复杂的数据环境中，信息来源存在格式差异、结构分散或传输延迟等问题，单一来源的判断结果容易存在偏差。融合大数据技术与人工智能算法有助于打通数据之间的逻辑隔阂，让系统在横向整合中提取更高质量的综合信息。多源数据在统一逻辑下完成筛选，有利于算法识别模式之间的内在联系，减少误判。智能判断的准确性依赖信息的全面性，借助融合结构化、半结构化及非结构化数据，系统能够从多个维度获取决策参考，增强对复杂网络行为的处理能力。

在网络系统运行中，采集到的数据可能来自路由节点、传感设备或用户操作，各类数据的内容属性与格式规范不尽相同，直接使用可能导致处理逻辑碎片化。借助融合策略，系统能将协议日志或运行状态等信息按照统一标准完成整理，再输入至人工智能模型中进行深层次分析。以网络调度任务为例，判断节点负载状态时只依赖传输速率数据可能无法准确反映实际情况，当将用户请求频率、历史流量趋势及当前处理延迟等数据一并纳入计算时，判断的基础会更加扎实，输出结果更贴近真实需求。在安全防护中，融合多个来

源的访问行为、异常波动或协议特征能提升攻击行为识别的成功率，降低系统暴露风险。人工智能模型借助学习这些复合型数据输入，能够提取出高频关联特征，建立逻辑严密的判断机制。在面向服务的网络环境中，不同服务类型对于带宽、时延或可靠性具有各自标准，融合多源数据能让调度系统精准识别不同服务特性，生成适配性更强的资源分配策略。融合过程中的数据清洗、匹配或标准化环节能降低错误输入的干扰，提升模型训练质量。借助持续的数据融合，系统能从单点响应转向多维协同，在决策效率或准确性方面表现出更高水平，稳步提升网络运行智能化水平（如图 2）。

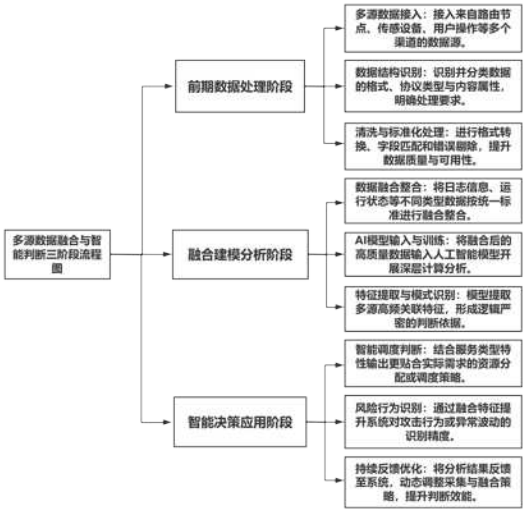

图 2 多源数据融合与智能判断三阶段流程图

2.4 完善智能安全机制，提升网络防护水平

大数据技术能帮助系统在高频交互中发现潜在的异常特征，人工智能则基于训练模型识别风险模式，实现更早、更准的预警。安全机制可利用智能算法实现行为识别或自动响应。系统能够基于历史攻击路径或当前网络状态实时调整防护策略，压缩攻击窗口。增强识别精度能让安全机制具备前置判断能力，在攻击行为尚未扩散前完成处置，保障网络整体的稳定运行。

网络系统面临的安全威胁呈现频率高、传播快的特点，传统以特征码为核心的安全防护方式很难满足现有要求。引入智能分析机制，系统可实时采集终端访问日志、通信状态或协议请求等多维数据，并依托大数据平台实现并行处理。这一基础上，人工智能模型能学习特定行为模式，建立攻击特征数据库，让系统在识别未知威胁时具备模式匹配或深度推理能力。系统能够检测重复访问、高速扫描等显性风险行为，还可分析低频分布、不规则路径及伪装通信等隐性攻击信号。在处理过程中，模型可综合判断行为意图、通信异常或响应延迟，输出风险等级及处置建议。如果系统检测到局部设备出现非预期数据波动，智能机制会根据分析结果自动封锁通信端口或重构路由逻辑，避免威胁进一步扩散。另外，安全机制支持事件数据回溯或规则动态调整，能让系统在经历攻击事件后具备持续优化的能力。数据资源在这个过程中不只作为监测依据，也参与智能规则的更新流程，形成闭环管理体系。构建智能安全机制能够提升网络对已知风险的响应效率，在面对新型攻击手段时做出合理判断，从系统底层建立安全防线，支撑网络在高复杂性通信环境中的可靠运行。

3 结束语

大数据与人工智能技术的深度融合，能够推动计算机网络系统从数据驱动向智能主导的方向不断演化。二者在感知信息或防护风险等多个维度展现出高度协同效应，能够提升网络运行的效率，拓展系统在复杂场景中的适应能力。网络架构借助智能算法获得更高层次的自组织能力，数据资源在融合机制下能释放出更强的决策价值。未来网络系统的演进会以更高精度的数据识别能力以及更完善的安全保障体系为支撑，建立具备学习能力及判断能力的智能基础设施。

参考文献：

[1] 韩璐 . 大数据时代背景下人工智能技术在计算机网络安全中的应用研究 [J]. 科技资讯 ,2025,23(04):44–46.

[2] 施盛江 , 张贵珍 . 大数据时代人工智能在计算机网络技术中的实践研究 [J]. 产业创新研究 ,2024,(18):92–94.

[3] 孟磊 . 大数据时代人工智能在计算机网络技术中的应用分析 [J]. 数字通信世界 ,2024,(05):102–104.

作者简介：王子虎（1988—），男，汉族，安徽利辛人，硕士，讲师，研究方向为人工智能，大数据，物联网通信。