人工智能在计算机网络技术中的应用研究

柴桦

西部战区陆军参谋部，甘肃兰州，730000；

摘要：随着计算机网络技术向规模化、复杂化方向发展，传统网络管理与安全防护模式逐渐难以应对海量数据处理、动态风险防控等需求，而人工智能凭借自主学习、智能决策与高效运算的特性，为计算机网络技术的升级提供了新路径。本文先明确人工智能与计算机网络技术融合的核心价值，再从网络管理、安全防护、资源调度三个关键领域，分析人工智能的具体应用方向，最后梳理两者融合过程中需关注的要点，旨在为推动人工智能与计算机网络技术深度结合、提升网络运行效能提供思路。

关键词：人工智能；计算机网络技术；网络管理；网络安全；资源调度

DOI：10.64216/3080-1508.26.01.052

引言

现在全球数字化转型越来越快，计算机网络已经不只是传统的通信工具，而是变成了连接各种智能设备、传输大量不同类型数据、保证各种业务正常运行的核心基础设施。随着数字化应用场景越来越多，计算机网络的覆盖范围不断扩大，从企业内部网络、城市网络，延伸到全国甚至全球网络、物联网，网络里的设备节点和数据交换次数越来越多，运行结构更复杂，处理的数据量也更大。这一变化，对计算机网络的稳定性、安全性和高效性，提出了比以前高得多的要求。传统计算机网络技术，主要靠人工提前定规则、手动操作管理，一开始设计时没考虑到要处理海量数据和应对随时变化的风险，所以在三个关键场景里明显不够用：一是要实时处理大量数据时，人工分析速度慢，没法马上看懂数据、挖出有用信息；二是遇到没见过的安全威胁时，靠人工定的威胁规则只能挡已知威胁，对新的、变了样的威胁识别不出来；三是要调整网络资源分配时，固定的规则跟不上业务需求的变化，最后反应慢、效率低、判断不准，满足不了现在数字化场景的需求。人工智能技术是新一代信息技术的核心，核心逻辑是靠数据驱动，用深度学习、机器学习等算法，自己学数据、智能分析数据、准确判断情况。它有两个优势：一是能快速找出数据里藏的规律，从大量杂乱的原始数据中提取有价值的特点和关联；二是能随时调整运行策略，根据分析结果自己优化决策，不用人工管就能适应场景变化。这些优势正好补上传统网络技术的短板，把人工智能融入计算机网络，不是简单加功能，而是让技术特点相互配合，升级网络能力：既提高网络管理和维护的自动化程度与效率，又让安全防护从“等威胁来再应对”变成“主动找威胁、提前防”，还能让资源分配更精准合理，最终推动网络技术向智能、自动、高效发展，为政府、金融、工业等场景的网络应用，提供更扎实可靠的支持。

1 人工智能与计算机网络技术融合的核心价值

1.1 提升网络运行效率，降低运维成本与故障影响

网络正常运行时，会一直产生三类数据：一是设备运行数据，包括路由器、交换机、服务器的负载、温度、端口状态等；二是数据传输数据，包括传输速度、数据包丢失比例、延迟时间等；三是业务数据，包括视频传输、文件下载等业务的访问量、数据总量等。传统模式下，处理这些数据全靠人工：要专业维护人员定期收数据、手动分析，判断网络是否正常，还要逐个查设备、测线路找故障。这种方式一是费人力，网络越大要的人越多；二是反应慢，数据处理和故障排查久，容易错过最佳处理时间，导致网络卡顿、业务中断。融入人工智能后，一方面能实时收数据，靠算法几秒内处理完海量数据，自己分辨正常和异常，快速监测网络状态；另一方面发现故障后，能靠历史数据训练的模型，快速定位故障设备、位置和类型，还能自动给建议，简单故障甚至能自动修复，大幅缩短处理时间，提升运行和运维效率。

1.2 增强网络安全防护能力，实现从“被动防护”到“主动防控”的转变

网络开放方便了信息交换，却也打破了安全边界，面临各种变化的威胁，既有病毒、黑客攻击等老威胁，也有新的变异病毒、智能定向攻击，防护难度越来越大。传统防护靠人工提前定规则，用防火墙等设备拦已知威胁，只能挡规则内的威胁，新威胁出现后要等人工更新

规则，这段时间网络很危险，防护范围小、反应慢。人工智能融入后，一方面能不断收安全数据，自己学新威胁的特点，更新威胁库，不用人工管就能识别新威胁；另一方面能实时监测数据传输和设备访问，发现陌生 IP 高频访问、超权限读数据等异常，立刻启动防护，切断攻击、冻结权限，挡住威胁扩散，防护更准、更快。

1.3 优化网络资源利用效率，实现资源“按需分配、动态适配”

网络核心资源有三类：带宽（传数据用）、服务器算力（算数据用）、存储容量（存数据用）。这些资源的需求会变：白天办公、业务多，带宽和算力需求高；晚上需求低；视频直播要多带宽，大数据分析要多算力，文件存储要多容量。传统资源分配靠人工定固定规则，不管需求怎么变都按规则分，容易出现资源浪费（需求降了用不完）或不够用（需求涨了不够分），效率很低。融入人工智能后，一是能分析历史业务需求和实时资源使用情况，精准预判需求变化；二是根据预判调整分配，需求涨了就把闲置资源调过去，需求降了就回收资源分给别人，实现“按需求分配”，既不浪费资源，又能保证业务流畅运行。

2 人工智能在计算机网络技术中的具体应用方向

2.1 人工智能在网络管理中的应用

网络管理的核心需求有三个：一是保证路由器、交换机、服务器等设备正常运行；二是网络或设备出问题时，能快速发现、找准问题并解决；三是不断优化网络参数，让参数符合业务需求和设备状态，提升网络效率。人工智能在这一领域的应用，就是用“自动代替人工、智能提升效果”，重点做三件事：监测网络状态、处理网络故障、优化网络参数，让网络管理从“靠人维护”变成“自动、智能维护”，减少成本，提高精准度和反应速度。

2.1.1 网络状态监测：自动监测，及时发现异常

先在网络里的核心节点、关键设备和传输链路上，装能实时收数据的感知节点，收集设备负载、温度、传输速度等数据；再用算法分析这些数据，建立网络正常运行的模型，明确各项参数的正常范围；之后实时比对新收集的数据和模型，一旦数据超出正常范围，就自动报警，告诉运维人员哪里可能出了问题，不用人一直盯着监控，既省人力，又不容易漏判。

2.1.2 网络故障处理：快速找问题，高效解决

先收集网络历史故障数据，包括故障类型、当时的设备数据、处理方法，再结合实时异常数据，用算法训练出故障诊断模型；故障发生后，把实时异常数据输入模型，很快就能找准故障设备、具体部件甚至对应链路；接着模型会自动给出处理建议，简单故障（比如重启设备就能好的问题）还能自动修复，不用人逐个排查，缩短处理时间，减少对网络的影响。

2.1.3 网络参数优化：跟着需求变，保证业务流畅

先收集业务运行数据（比如访问量、响应时间）和参数配置数据（比如带宽比例、路由策略），用算法找出参数和业务效果之间的关系，明确不同业务适配的最优参数；之后实时监测业务需求，比如视频业务访问量突然增多，就自动提高这类业务的带宽比例，优化传输路径，不用人手动调整，避免业务卡顿，让网络效率最高。

2.2 人工智能在网络安全防护中的应用

网络安全防护的核心需求，是“认出威胁、挡住攻击、保护数据”，具体要做到：不遗漏已知威胁，也能发现未知威胁；攻击发生时，快速挡住，不让影响扩大；保护好敏感数据，不泄露、不被改。人工智能在这一领域的应用，就是用“主动防代替等威胁来、智能认代替人判断”，重点做三件事：识别安全威胁、拦截恶意攻击、保护数据安全，搭建一套全流程、精准的防护体系，弥补传统防护的不足。

2.2.1 安全威胁识别：所有威胁都能认出来

先收集三类数据：已知攻击数据、异常访问数据、正常业务数据，建成数据样本库；再用算法训练识别模型，让模型分清什么是正常行为、什么是威胁行为，还能学会识别新出现的、变了样的威胁；之后实时监测网络里的数据传输和设备访问，把数据输入模型，既能认出常见病毒、黑客攻击，也能发现新型威胁，不会有遗漏。

2.2.2 恶意攻击拦截：精准挡攻击，不影响业务

把人工智能和防火墙、入侵检测系统配合起来，形成智能防护系统；一旦识别出攻击迹象，系统就立刻采取措施，比如阻断攻击 IP、禁止恶意数据包、关闭异常端口，不让攻击扩散；同时根据攻击类型和强度，调整拦截策略，比如攻击和正常业务 IP 有重叠时，只拦攻击数据包，不影响正常业务，做到“挡得住攻击，不耽误干活”。

2.2.3 数据安全保护：全程护好敏感数据

先让人工智能学敏感数据的特征（比如身份证号、经营数据的格式和规律），建成特征库；再实时扫描网络里传输和存储的数据，认出敏感数据并做好标记；之后对这些敏感数据加密，传输时变密文，存储时也变密文，别人偷看到也读不懂；同时实时监测敏感数据的访问和传输，一旦发现有人没经过允许碰数据，就立刻阻止并报警，全程保护数据安全。

2.3 人工智能在网络资源调度中的应用

网络资源调度的核心需求是实现资源与需求的精准匹配，提升资源利用效率，人工智能在此领域的应用，围绕“需求预测、动态分配、资源优化”展开，解决资源分配不合理的问题。在资源需求预测方面，人工智能通过分析历史业务运行数据（如不同时段各业务的访问量、数据传输量），结合季节、节假日等影响因素，利用时间序列预测算法，预测未来不同时段、不同业务的资源需求；如预测某一节假日期间，视频业务与购物业务的访问量将大幅增长，进而提前预判这两类业务对带宽与算力的需求，为后续资源分配提供依据，避免资源需求突增导致的业务卡顿。在资源动态分配方面，人工智能根据实时资源需求预测结果与当前资源使用状态，动态调整资源分配策略；当某一业务的资源需求增长时，人工智能可立即将闲置的带宽、算力资源分配至该业务，保障业务运行；当业务需求下降时，再将多余资源回收，分配至其他需求较高的业务，实现资源的“按需分配、动态调整”，避免资源闲置与过载，提升资源利用效率。在资源优化方面，人工智能通过分析长期资源使用数据与业务运行效果数据，挖掘资源分配与业务效果的优化空间，进而调整资源分配的长期策略；如发现某类业务在特定时段对算力需求较高，但当前算力分配未达标，可优化长期资源配置，增加该时段的算力储备；同时，人工智能可识别资源分配中的冗余问题，如删除不必要的资源占用，进一步优化资源配置，提升网络资源的整体利用效率。

3 人工智能与计算机网络技术融合需关注的要点

3.1 保障数据质量

人工智能靠数据工作，在网络里的应用效果，全看网络产生的运行、安全、业务数据好不好。数据缺了、错了，或是有重复没用的，都会让算法学不好、分析不准，进而影响网络管理、安全防护和资源调度的精度。所以，要建“采集+预处理”的机制：采集时，规范感知节点安装、调好采集频率，保证数据全；预处理时，用算法删掉错数据、过滤重复数据、补全缺数据，确保数据准、有用，给人工智能打好数据基础。

3.2 平衡技术成本与效益

用人工智能要花钱，包括研发算法、升级设备（如智能服务器）、日常维护。好处是提高网络效率、降低安全风险、优化资源利用。若盲目买高端技术、花太多钱，却不看自己网络规模、业务需求和现有设备，容易“花得多、赚得少”。所以，要先摸清自己网络情况，再选适配的技术和场景，优先在效果明显的地方花钱，定期算成本和好处，控制开支，让效益最大。

3.3 强化技术兼容性

现在网络里有很多传统设备和软件，人工智能要和它们配合好才能稳定。若不兼容，会导致网络异常、数据传不动。所以，引入前要查传统设备的参数、软件版本，选兼容的人工智能产品；不兼容的地方，可改接口、装插件；上线前，模拟各种场景测试，确保两者能顺畅配合，避免出问题。

4 结语

人工智能为计算机网络技术的升级提供了关键支撑，两者融合不仅能提升网络运行效率、增强安全防护能力、优化资源利用效率，还能推动计算机网络技术向智能化、自动化方向发展，满足当前数字化场景下的网络需求。未来，随着人工智能与计算机网络技术的持续发展，两者的融合将更深入，成为网络的“核心智能大脑”，通过动态路由选择避免拥塞，还能推动运维向“自配置、自修复”的自治模式升级。在安全领域，AI 可实时监测异常流量，识别未知威胁，筑牢防御屏障。这种融合将覆盖智算互联、边缘服务等更多场景，大幅提升网络效率与安全性，为构建智能、可靠的网络环境提供坚实支撑。

参考文献

[1]王于哲.人工智能在计算机网络技术中的应用探讨[J].数字通信世界,2024,(02):126-128.

[2]李兆芃.人工智能技术在计算机网络防御中的应用探索[J].信息记录材料,2024,25(02):223-225+229.

[3]斯马依力江·木萨汗,姜杰,李晴,等.大数据时代人工智能在计算机网络技术中的应用[J].数字技术与应用,2024,42(01):82-84.