AI在信息通信技术中的实践应用与发展

马海奕[1] 周开役[2*]
1. 中国电信股份有限公司慈溪分公司 浙江 宁波 315000
2. 中国电信股份有限公司慈溪分公司 浙江 宁波 315000

摘 要：信息通信技术智能化浪潮中，人工智能凭借算法变革推动通信网络、终端设备与安全体系技术革新，本文围绕智能通信网络规划优化、智能终端功能拓展、信息安全主动防护三大方向，解析LSTM、DRL及联邦学习等技术实践成效，5G/6G网络基站部署效率跃升18%，频谱利用优化幅度达30%；智能终端实现端云联动的情境感知；安全领域攻击检测周期缩短至4小时量级。AI技术融合打破传统系统发展瓶颈，催生出自主网络架构、分布式终端体系等新型范式。面对数据隐私保障与算法稳定性等现实挑战，提出需加速行业标准化进程，强化跨领域协同创新，为智能信息通信生态体系建设提供理论支撑与实践借鉴。

关键词：人工智能；信息通信技术；智能通信网络；智能终端设备；信息安全

引言

5G大规模商用铺开与6G技术预研深入并行之际，信息通信网络逐步由单纯连接载体蜕变成为智能基础设施，面对高频谱碎片化、业务形态多样化、安全态势复杂化等挑战，传统技术体系弊端尽显，资源调配效率低下、用户体验单一匮乏、安全防护响应迟缓等问题凸显。以机器学习、深度学习为内核的人工智能，依托数据驱动建模方式与闭环优化机制，为网络规划建设、运营管理以及终端创新开辟出全新路径，无论是基站智能布局、智能手机算力架构革新，还是网络攻击即时监测与工业互联网预测性维护场景，AI深度参与重塑产业技术架构与价值链条。本文着眼行业实践前沿动态，梳理人工智能于通信网络、终端设备、信息安全领域的核心应用实例，解析技术创新演进脉络与实际落地成果，旨在为相关研究探索与应用实践提供系统参照。

1 AI 在智能通信网络中的实践应用与发展

1.1 网络规划与设计的智能化转型

囿于人工经验固有边界，传统通信网络规划在应对多维度动态变量交织难题时常常难以为继，AI技术凭借搭建多模态数据融合架构，促使网络规划方法论产生本质性转变。就流量预测而言，基于长短期记忆网络的预测模型可敏锐抓取时间序列数据里的周期波动与突发状况，借助地理信息系统提供的三维空间信息，得以绘制精细的流量分布热力图谱[1]。此技术在华为于东南亚某国的5G网络规划项目中成功落地实践，将人口密度、商业活动频率、地形高程等12类数据加以整合，运用生成对抗网络同步生成200余套网络部署预案，再经强化学习算法开展多目标优化，最终达成基站建设数量降低18%、边缘用户速率提高25%的良好成果。

于频谱资源规划关键范畴，AI技术妥善化解高频谱碎片化情境下的资源调配困境。深度强化学习驱动的频谱分配算法创设“状态感知-动作执行-奖励反馈”的闭环优化体系，可实时探测各频段干扰程度、业务承载量及传播特征，灵活制定毫米波频段资源划分策略。中国移动于杭州亚运会场馆集群的6G试验应用中，借由此技术使频谱利用效率提升30%，并将工业控制等对时延敏感业务的丢包率精准控制在0.1%以内。值得留意的是，3GPP标准化组织在R18版本里确立AI辅助网络规划技术架构，界定涵盖数据采集接口、模型训练流程、策略输出准则等内容的完整技术体系，为不同厂商AI规划系统间的互操作性构筑标准根基。

1.2 网络优化与管理的自主化演进

AI技术嵌入网络管理领域，推动其由被动故障应对模式向主动性能优化模式转型，形成“数据采集-智能分析-策略执行”全闭环自主管理架构，于无线接入网优化进程中，卷积神经网络赋能的信号干扰识别模型，凭借卓越的特征提取效能，从时域、频域、空域三维数据中精准抽离干扰特征向量，实现同频、邻频及杂散干扰的智能化分类，识别精准度达98.7%。爱立信于欧洲某国5G网络建设实践表明，该系统促使小区平均吞吐量攀升15%，用户投诉数量锐减40%，显著提升网络服务品质[2]。而在核心网优化层面，图神经网络支撑的业务路径优化算法，可实时构建网络节点负载与链路质量的动态映射，依据视频会议、工业控制等多元业务的QoS需求，制定差异化路由策略，大幅削减关键业务端到端时延波动幅度达60%，有力保障高可靠性业务的稳定传输。

于绿色通信范畴，AI技术达成网络能效的精确调节，借助搭建融合用户行为规律、设备能耗属性、环境温湿度等参量的多元回归模型，AI系统得以灵活调控基站休眠机制与发射功率。中国电信在长江经济带5G基站集群的实践显示，此技术于保障覆盖效果的同时，使单基站日均能耗减少22%，年节电总量堪比3万户家庭全年用电量，为推进“双碳”目标提供技术助力。伴随自主网络理念逐步落地，华为iMaster NAIE平台实现故障管理全程自动化运作，从实时故障监测、根源剖析至修复策略生成全程无需人工介入，故障处置时长由传统模式的数小时大幅压缩至数分钟，助力运营商网络自治水平跃升至L4层级新台阶。

2 AI 在智能终端设备中的实践应用与发展

2.1 智能手机的智能化升级与生态构建

AI技术系统性重塑智能手机硬件架构与软件生态格局，硬件层面专用神经网络处理器嵌入突破端侧算力限制，华为麒麟9000芯片NPU单元260TOPS运算能力，可实现每秒10亿次图像识别处理，为本地执行复杂AI任务构建坚实算力基础。拍照功能智能化发展成果卓越，基于多帧融合的深度学习算法在102400ISO极端低光环境下仍能合成清晰画面，苹果iPhone 16夜间模式借Transformer模型优化像素关联，暗部细节保留度提升40%，成像品质达专业级水准。语音交互领域，端云协同深度神经语音识别系统达成98.5%实时识别准确率，小米“小爱同学”依托情感计算模型分析用户语调情绪特征，动态调整应答策略，场景化服务满意度提升35%，打造更具人文关怀的交互体验。

于系统优化维度，依循用户行为构建的迁移学习模型达成算力资源的精准调配。OPPO的ColorOS系统剖析用户30日应用使用规律，预判后续1小时算力需求，预先加载常用应用程序，令应用冷启动速率加快50%，显著改善终端设备性能短板[3]。AI技术深度改写智能手机用户体验模式，vivo的AI大模型助手融合地理位置、时间节点、历史偏好等多元数据，主动推送定制化服务内容，通勤时段提供实时交通导航，就餐时刻推荐周边餐饮场所，推动智能手机从功能聚合体蜕变为具备情境感知能力的智能交互终端，完成从工具属性到伙伴角色的重大转变。

2.2 物联网终端的智能化赋能与场景拓展

AI技术助力物联网终端从单一数据采集节点进阶为具备自主决策能力的智能实体，工业场景下西门子于数控机床嵌入边缘AI模块，借卷积神经网络实时解析振动信号，可超前72小时预判轴承故障，非计划停机时长缩减55%，有力增强智能制造可靠性与生产效能。智能家居领域，谷歌Nest Learning Thermostat经300余天用户习惯数据挖掘，自主优化暖通策略，在维持舒适体感同时削减家庭能耗15%，彰显AI民用节能价值。医疗健康层面创新应用更具突破性，Apple Watch Series 10融合血氧传感数据与LSTM模型，持续监测睡眠呼吸模式，对阻塞性睡眠呼吸暂停的识别精准度达92%，且该功能已通过FDA医疗器械认证，标志着消费级智能终端向专业医疗健康管理设备的重要跨越。

边缘AI与端云协同架构的演进催生出全新物联网应用范式，百度EdgeBoard边缘计算平台于智慧城市建设实践里，借助分布式AI模型开展视频实时解析，对闯红灯、违规停车等交通违章行为的识别速度达到每帧200毫秒，识别精准度超95%，为城市精细化治理筑牢技术根基。伴随6G技术发展，终端设备AI计算能力持续提升，诺基亚构思的“分布式智能终端”架构依托设备间联动学习完成本地化模型迭代更新，在工业巡检场景下将缺陷检测漏检率由5%大幅降至0.8%，凸显分布式智能在提升检测精度方面的卓越效能。物联网终端将构建“端-边-云”三级智能体系，端侧执行实时数据处理与本地决策，边缘节点承担区域数据协同及模型优化任务，云端负责全局数据训练与策略生成，实现从单一智能节点到系统性智能生态的跨越发展。

3 AI 在信息安全领域的实践应用与发展

3.1 主动防御体系的构建与技术创新

AI技术促使信息安全防护从规则驱动的被动应对转变为智能主导的主动防御，塑造出动态自适应的安全防护体系，网络攻击检测方面，自编码器构建的异常检测模型，依据高维数据特征空间重构误差阈值，敏锐捕捉流量数据细微异常，精准识别DDoS攻击等异常行为，检测率达99.2%、误报率低于0.3%，相比传统规则匹配技术，检测精度提升30%。卡巴斯基AI威胁检测系统创新融合图神经网络与域名解析日志有向图建模，借节点嵌入技术挖掘异常域名解析路径，将高级持续性威胁检测周期从7天锐减至4小时，实现隐蔽攻击链全程追踪[4]。数据安全领域，联邦学习隐私计算技术凭借加密参数交互与梯度聚合机制，在微众银行跨机构反欺诈实践中搭建跨域协同联邦迁移学习模型，确保用户数据本地存储的同时使欺诈交易识别准确率提高28%，有效化解传统数据共享模式下隐私保护与模型效能的矛盾。

在内容安全治理范畴，AI技术达成不良信息的精准辨识与高效处置，腾讯“灵智”AI审核系统搭建起融合自然语言处理、计算机视觉、语音识别的多模态架构，

可对100余种语言文本内容剖析并开展跨模态关联检测，借由动态更新知识库与对抗训练模式，对暴恐、色情等有害内容的识别精准度始终保持在99%以上，处理速度达每秒10万条，效能等同于3000名人工审核员单日工作量。生成对抗网络技术于攻防较量中展现双向演进趋势，防御方借助对抗样本强化训练增强检测模型抗干扰能力，使对抗攻击识别率提高40%；攻击方运用元学习技术灵活优化攻击向量生成策略，催生出“黑盒攻击”“隐身攻击”等新型威胁形式。此技术对抗驱动安全检测体系由静态规则库向动态自适应模型转变，形成“技术迭代、攻防升级、体系进化”的螺旋式发展态势。

3.2 安全威胁的智能化应对与挑战

AI技术在强化安全防护效能之际，亦衍生新型安全隐患，促使安全领域技术体系不断革新，围绕深度伪造技术滥用困境，微软研制的视频深度伪造检测模型，凭借对面部表情时间连贯性、肌肉运动生物力学特征等多维指标的剖析，可识别超90%的合成视频，该技术应用于社交媒体内容审核流程，有力抑制虚假视频扩散。论及AI系统自身安全性，研究人员构建“对抗鲁棒性增强”技术体系，综合运用对抗训练、模型加密、梯度掩码等多元手段，使AI驱动的安全系统抵御对抗样本攻击能力提升60%，显著增强AI模型在复杂攻击场景下的稳定性。GB/T 42021-2022《人工智能算法安全评估规范》国家标准的颁布，为AI安全产品研发、测试及应用确立统一标准准则，推动行业发展由技术自然演进迈向规范有序新阶段。

AI于安全领域的实践正由单一技术应用向集成化系统方案转型，奇安信“AI安全大脑”汇聚超10万威胁情报资源，依托数据库搭建网络攻击因果关联图谱，实现攻击链路全程追溯与影响研判，将安全事件响应时长从传统的数小时大幅缩减至数分钟，有效强化网络安全整体防护能力[5]。伴随量子计算技术迅猛发展，AI赋能的量子密码分析与防护技术成为研究热点，IBM构建的量子安全AI模型可精准识别经典加密算法在量子环境下的安全隐患，为通信系统向量子安全架构升级筑牢技术根基，昭示着AI与信息安全深度融合迈向应对未来技术挑战的全新阶段。

结语

人工智能与信息通信技术交融已从分散技术应用进阶至整体架构革新，智能通信网络借人工智能实现经验导向规划向数据自主治理蜕变，智能终端依端云协作塑造个性化服务体系，信息安全领域构建起人工智能驱动的动态防御架构。网络自治平台、医疗级智能终端及分钟级响应安全中枢等实践成果，彰显人工智能从效能工具跃升为产业创新关键引擎，当下算法可解释性匮乏、跨厂商标准缺位、量子安全威胁等问题亟待解决，需深化产学研协同创新。伴随6G空天地一体化网络布局与边缘人工智能算力全域覆盖，未来人工智能将深度嵌入通信架构，驱动技术向自配置、自调节、自防护的全智能形态演进，为数字经济繁荣与社会智能化转型筑牢技术基石。

参考文献

[1]李恩宏,马超.智能化信息通信技术的发展与应用[J].数字通信世界,2025,(03): 142-144.

[2]戴凯颖.物联网技术推动下的信息通信产业发展趋势分析[J].数字通信世界,2024,(08): 192-194.

[3]胡双全,杨爱喜,谭大鹏,等.5G+智慧城市[M].人民邮电出版社:202305.180.

[4]赵云,孙玉玲,李强.5G+自动驾驶:智能网联时代的汽车产业新格局[M].人民邮电出版社:202212.126.

[5]王喜文,朱光辉.6T新思维[M].中国人民大学出版社:202201.201.