电子技术支撑下人工智能助力通信安全防护体系构建

胡国清
江西诚科建设咨询监理有限公司　江西　南昌　330025

摘　要：电子技术为人工智能应用于通信安全防护筑牢根基，高性能计算与边缘计算提升AI训练与响应效率，传感器网络和多源数据融合丰富AI决策信息，5G/6G通信保障数据安全传输与隔离。而人工智能通过智能威胁检测、动态加密、自适应访问控制等关键技术，增强了通信安全能力。基于此，可通过设计分层防御架构、实施全生命周期安全管理、推动合规与标准化建设、建立产学研协同机制等，构建通信安全防护体系。

关键词：电子技术；人工智能；通信安全防护；体系构建

引言：在数字化浪潮席卷的当下，通信网络已成为社会运转的关键基础设施，其安全稳定关乎国家安全、经济发展与社会民生。然而，随着网络攻击手段日益复杂多样，传统通信安全防护体系面临巨大挑战。电子技术的蓬勃发展，为人工智能在通信安全领域的应用提供了强大支撑，高性能芯片、先进传感器、高速通信网络等技术不断突破。在此背景下，探索电子技术支撑下人工智能助力通信安全防护体系的构建，具有重要的现实意义与战略价值。

1 电子技术对人工智能的支撑作用

1.1 高性能计算与AI模型训练

（1）在人工智能模型训练，特别是深度学习模型训练过程中，数据处理量巨大，传统计算设备难以满足高效运算需求。而GPU（图形处理器）和TPU（张量处理器）凭借其强大的并行计算能力，能够大幅提升数据运算速度，有效加速深度学习模型的训练进程。在网络安全领域，这一优势尤为明显，可显著缩短威胁特征提取周期，让AI能更快识别新型网络威胁，为后续的安全防护争取宝贵时间。（2）边缘计算技术的兴起，进一步完善了人工智能的计算体系。它将计算任务下沉至靠近数据源头的边缘设备，有效降低了数据传输过程中的时延，从而支持实时威胁响应。例如，在AI防火墙中引入本地学习模块，借助边缘计算，防火墙可在本地快速处理网络数据，实时分析潜在威胁并及时做出防护响应，避免因数据传输至远程服务器而产生的延迟导致安全风险。

1.2 传感器网络与多源数据融合

（1）随着物联网技术的普及，大量物联网设备如5G基站、终端传感器等广泛分布于各个场景，这些设备构成了庞大的传感器网络。它们能够实时采集网络流量数据、用户行为数据以及周边环境数据等多类型信息，为人工智能提供了丰富且多维的特征输入。这些多样化的数据是AI进行精准分析和决策的基础，使得AI能够更全面地了解所监测对象的状态，提升其判断的准确性。（2）中国电信“星辰·见微”安全大模型便是传感器网络与多源数据融合应用的典型案例。该大模型通过整合来自传感器网络的网络日志数据和设备状态数据，对这些多源数据进行深度融合与分析，能够更精准地识别提示注入攻击行为，大幅提升了提示注入攻击检测精度，为网络安全防护提供了有力的技术支持，充分体现了传感器网络与多源数据融合对人工智能在安全领域应用的推动作用[1]。

1.3 5G/6G通信与安全信息传输

（1）5G和正在研发的6G通信技术，具备低时延、高带宽的显著特性，这为人工智能应用中加密数据的高速传输提供了可靠保障。在联邦学习场景中，各参与方需要交换模型参数以实现共同训练，而这些模型参数往往涉及敏感信息，需要进行加密处理。5G/6G的高带宽特性能够确保加密后的模型参数快速传输，低时延则保证了联邦学习过程的高效推进，避免因数据传输问题影响模型训练进度。（2）此外，5G/6G通信技术中的网络切片技术，能够将物理网络划分为多个逻辑上相互隔离的虚拟网络切片。不同的人工智能应用可根据自身需求使用专属的网络切片，实现安全隔离。这种隔离方式能够有效防止不同应用之间的干扰，同时保障关键通信链路免受外部攻击，确保人工智能应用在数据传输过程中的安全性和稳定性，为人工智能技术的广泛应用奠定了坚实的通信基础。

2 人工智能在通信安全中的关键技术

2.1 智能威胁检测与分类

（1）在通信流量监测中，机器学习算法成为基础检测工具。随机森林算法通过多棵决策树集成学习，对海量网络流量数据进行特征筛选与异常识别，可精准捕捉

DDoS攻击中的流量突发特征；支持向量机（SVM）则凭借高维空间分类优势，有效区分正常通信与恶意软件传播的流量差异，减少误报率，为通信网络搭建第一道威胁防线。（2）深度学习模型进一步提升威胁检测的深度与前瞻性。长短期记忆网络（LSTM）能挖掘时间序列数据中的隐藏关联，通过分析通信数据的时序规律，预测高级持续性威胁（APT）的攻击路径，提前识别潜伏的攻击行为；卷积神经网络（CNN）可将恶意代码转化为灰度图像，利用图像识别能力提取代码特征，实现对未知恶意程序的快速检测，弥补传统特征码检测的局限性。（3）AI防火墙是智能威胁检测技术的典型应用载体。它通过监督学习利用历史威胁数据训练精准的威胁识别模型，同时结合非监督学习对未知流量进行异常挖掘，在零日攻击（未知漏洞攻击）检测中表现突出，当遇到未记录的威胁行为时，能自主识别并阻断，大幅提升通信网络的主动防护能力。

2.2 动态加密与密钥管理

（1）联邦学习技术为通信加密的密钥管理提供新思路。传统集中式密钥生成模式存在单点泄露风险，而联邦学习支持多节点在本地训练模型、分布式生成密钥，各节点仅交换加密后的参数信息，不泄露原始密钥数据，避免因单一节点被攻破导致整个加密体系失效，保障通信加密的安全性与可靠性。（2）差分隐私技术则聚焦加密数据中的敏感信息保护。在通信数据加密传输过程中，用户位置、通话内容等敏感信息易被泄露，差分隐私通过在数据中添加可控噪声，模糊个体敏感信息，同时保证数据整体的可用性，既满足通信安全防护需求，又保护用户隐私不被侵犯，实现安全性与隐私性的平衡[2]。

2.3 自适应访问控制

（1）基于人工智能的用户行为画像技术，推动访问控制从静态向动态升级。系统通过采集用户登录时间、操作频率、设备信息等多维度数据，构建精准的用户行为模型，当检测到用户行为与画像存在偏差（如非常用设备登录、异常时间段操作）时，自动调整访问权限，如增加身份验证步骤、限制操作范围，有效防范越权访问与账号盗用风险。（2）强化学习算法进一步优化自适应访问控制策略。它通过持续与通信安全环境交互，学习不同场景下的安全防护需求，在保障安全性的同时，兼顾用户体验。例如“星小辰”AI通话助手，利用强化学习分析诈骗电话特征，精准拦截诈骗呼叫，同时避免误拦正常通话，实现安全防护与用户体验的协同优化。

2.4 威胁情报共享与协同防御

（1）区块链与人工智能的融合，为威胁情报共享提供技术保障。区块链凭借去中心化、不可篡改特性，实现跨机构威胁情报的安全存储与追溯，确保情报真实性与完整性；人工智能算法则对海量情报数据进行深度分析，挖掘不同威胁事件间的关联规律，如识别跨国攻击组织的行动模式，为协同防御提供决策支持，提升整体防护效率。（2）亚太地区5G安全联盟的实践的是典型案例。该联盟搭建AI驱动的威胁情报共享平台，整合区域内运营商、企业的威胁数据，通过AI算法实时分析情报并推送防御策略，在应对跨国DDoS攻击时，各成员可快速获取攻击特征与防御方案，协同阻断攻击流量，有效遏制威胁扩散，体现人工智能在跨区域通信安全协同防御中的关键作用。

3 电子技术支撑下人工智能助力通信安全防护体系的构建路径

3.1 分层防御架构设计

（1）终端层作为通信安全的“第一道关口”，依托电子技术的微型化与集成化优势，将AI芯片嵌入手机、物联网终端等设备，实现本地威胁检测与实时防护。例如，智能手机搭载的AI安全芯片，可在本地分析APP的行为特征，识别恶意程序的权限滥用、数据窃取等行为，无需依赖云端算力即可快速阻断风险，避免因数据传输延迟导致的安全隐患，同时降低终端设备的通信带宽消耗。（2）网络层借助软件定义网络（SDN）与人工智能的协同，打造动态防御能力。SDN技术实现网络资源的灵活调度，AI算法则通过实时分析网络流量特征，精准定位攻击源（如DDoS攻击的流量入口）。当检测到异常时，AI可自动向SDN控制器发送指令，调整流量路由策略，将受攻击区域与正常网络隔离，避免威胁扩散，同时保障关键业务的通信链路畅通，实现“检测-决策-响应”的自动化闭环[3]。（3）云层作为通信安全的“中枢指挥中心”，整合电子技术支撑的海量存储与高性能计算资源，构建云安全平台。平台通过AI算法汇总分析终端、网络层上传的全局日志数据（如设备状态、流量异常记录），挖掘跨区域、跨场景的威胁关联，预测区域性攻击趋势（如某一地区即将爆发的勒索病毒传播路径）。基于预测结果，云平台可提前向终端与网络层推送防御策略，实现“全局预警、局部响应”的协同防护。

3.2 全生命周期安全管理

（1）数据采集阶段聚焦原始数据安全，依托差分隐私与同态加密技术构建防护屏障。在采集用户通信数据、设备状态信息时，差分隐私通过添加可控噪声模糊个体敏感信息（如用户通话记录、位置数据），避免数

据泄露风险；同态加密则允许在加密状态下对数据进行运算，无需解密即可完成AI模型的特征提取，确保数据在采集与传输过程中“可用不可见”，兼顾数据价值挖掘与隐私保护。（2）模型训练阶段通过对抗样本训练提升AI算法的鲁棒性。攻击者常通过构造对抗样本（如篡改网络流量特征、伪装恶意代码）欺骗AI模型，导致检测失效。基于电子技术支撑的高性能计算能力，可生成大量多样化的对抗样本，用于训练AI模型，使其在复杂攻击场景下仍能准确识别威胁，减少因算法漏洞引发的安全风险，保障模型训练结果的可靠性。（3）部署运行阶段依靠AI监控机制实现动态优化。电子技术支撑的实时数据采集与分析能力，让AI可持续监控自身模型的运行性能（如威胁检测准确率、误报率）。当检测到模型性能下降（如因新型攻击出现导致准确率降低）时，系统自动触发模型更新机制，调用云端算力重新训练模型，并将更新后的模型推送至终端与网络层，确保防护体系始终适配最新威胁态势[4]。

3.3 合规性与标准化建设

（1）以法规要求为基础，构建数据分类分级管理体系。在人工智能助力通信安全的过程中，需严格遵循GDPR（《通用数据保护条例》）、等保2.0（《信息安全技术网络安全等级保护基本要求》）等法规，对通信数据按敏感度分级（如公开数据、内部数据、核心数据），针对不同级别数据制定差异化的AI防护策略（如核心数据采用多重加密，公开数据简化检测流程），确保数据处理全流程合规，避免因法规违规引发的法律风险与声誉损失。（2）参考国际与国内标准，建立AI安全评估框架。以ISO/IEC27001（信息安全管理体系标准）、NISTSP800系列（美国国家标准与技术研究院安全指南）为依据，从AI模型的安全性（如抗攻击能力）、可靠性（如检测准确率）、透明度（如决策可解释性）三个维度制定评估指标。通过定期评估与认证，规范AI在通信安全中的应用，提升防护体系的公信力与稳定性。

3.4 产学研协同创新机制

（1）推动企业与高校深度合作，攻克核心技术难题。企业依托丰富的通信场景数据与工程化经验，高校凭借前沿的算法研究能力，双方联合建立实验室（如中国电信与哈尔滨工业大学共建的网络空间对抗实验室），聚焦AI在通信安全中的关键技术（如新型威胁检测算法、动态加密技术）开展攻关，将高校的科研成果转化为实际应用方案，解决企业在防护体系构建中遇到的技术瓶颈，加速技术落地。（2）开放数据集与测试平台，促进AI安全算法迭代。通信安全领域的算法优化需大量高质量数据支撑，企业与科研机构可联合公开稀缺数据集（如提示注入攻击数据集、5G网络异常流量数据集），降低算法研发的数据获取门槛；同时搭建开放的测试平台，模拟多样化的攻击场景（如跨国DDoS攻击、APT攻击），供开发者测试与优化算法。通过共享资源与协同测试，吸引全球开发者参与算法创新，推动AI安全技术快速迭代，为防护体系的持续升级提供技术动力。

结束语

电子技术为人工智能赋能通信安全防护搭建了坚实桥梁，从计算能力提升到数据融合，再到高效通信保障，全方位支撑着人工智能发挥效能。人工智能也凭借智能检测、加密管理等关键技术，为通信安全筑牢防线。未来，随着电子技术与人工智能的持续融合创新，通信安全防护体系将更加智能、高效、可靠。我们需紧跟技术发展趋势，不断完善防护体系，以应对日益复杂的网络安全威胁，为通信行业的稳定发展与社会的信息安全保驾护航。

参考文献

[1]杨嘉.基于人工智能的网络通信信息数据安全加密技术研究[J].信息记录材料,2025,26(03):120-122.

[2]朱杰.基于人工智能的网络通信信息数据安全加密技术研究[J].信息记录材料,2025,26(02):144-146.

[3]姚仕聪.人工智能在移动通信网络安全防护中的应用[J].中国新通信,2024,26(20):13-15.

[4]张利.基于人工智能的网络通信安全风险评估与防护[J].中国宽带,2023,19(9):142-144.