人工智能技术在计算机网络安全防护中的应用研究

姜睿涵
西华大学　四川　成都　611744

摘　要：在信息化建设不断发展的当下，计算机网络已然成为了社会运行、企业管理、公共服务的关键支撑力量。网络攻击也朝着隐蔽化、自动化、持续化的方向发展。传统的防护方式在面对未知威胁的发现、海量告警的处置、快速响应这些方面存在着一定的欠缺。人工智能拥有数据挖掘、模式识别、自主学习的能力，能够被运用到入侵检测、恶意代码识别、趋势感知、安全运维等方面。对人工智能在这些方面的应用价值、现实存在的问题、优化的路径展开研究，对于推动网络安全防护模式的智能化建设具有积极意义。

关键词：人工智能；计算机网络安全；入侵检测；恶意代码；安全防护

引　言：

计算机网络在政务、金融、教育、医疗、企业生产等诸多领域有着广泛应用，其所承载的数据规模持续增大，安全风险也相应增加。现阶段网络攻击不再仅仅局限于简单的病毒传播、端口扫描，而是更多地呈现为漏洞利用、身份伪装、钓鱼攻击、恶意代码变种还有持续性渗透。传统的安全防护方式能够对部分已知威胁予以应对，然而在面对未知攻击、复杂行为、海量日志时，容易出现识别滞后、误报较多、响应缓慢等状况。人工智能技术能够从数量众多的安全数据当中发现规律，识别异常行为并且辅助安全决策，这对于提高计算机网络安全防护水平有着重要的意义。

一、计算机网络安全防护面临的新形势

（一）网络攻击方式日益复杂

网络攻击如今已从单点入侵转变为多阶段、持续化渗透。攻击者一般会先去收集目标系统架构、人员信息、开放端口、业务应用等方面的内容，之后借助弱口令、系统漏洞、钓鱼邮件或者第三方组件缺陷进而进入内部网络。在入侵后并不会立刻进行破坏，而是通过权限提高、横向移动、隐蔽通信、数据回传等方式长期潜伏，逐步获取核心信息或者控制关键资源。云计算、物联网、移动办公还有远程接入的不断普及，让网络边界变得越来越模糊，终端和接口数量持续增多，攻击面因而扩大，传统的单点防护难以全面识别攻击链条，网络安全迫切需要具备动态感知和智能分析能力。

（二）传统防护模式存在局限

传统的网络安全防护主要借助防火墙、入侵检测系统、杀毒软件、访问控制、人工巡检来实现，其运行的逻辑大多建立于规则策略、特征库的基础之上。这种方式对已知的攻击能够起到一定的识别作用，然而当面对未知的漏洞利用、恶意代码变种、伪装行为时，却很容易出现漏报的情况，并且存在滞后性。各类安全设备每天都会产生大量的告警信息，其中混杂着重复的内容、低风险的提示、误报的信息，安全人员需要在海量的日志当中筛选出关键事件，而处置效率会受到经验水平的较大影响。另外，不同系统之间的数据格式、管理平台并不统一，致使终端、网络、身份、数据库的安全信息难以进行关联，从而造成安全管理处于碎片化的状态。

（三）智能化防护成为发展方向

人工智能给网络安全防护带来了全新的技术途径。机器学习可以借助对正常行为与异常行为样本展开训练，建立流量识别模型、用户行为分析模型、风险分类模型，深度学习适宜处理高维度、非结构化且复杂关联的数据，能够用于恶意代码检测、异常流量识别、攻击行为分析，自然语言处理能够对漏洞公告解析起到辅助作用，还能参与威胁情报提取、钓鱼邮件识别工作，知识图谱能够将资产、漏洞、攻击工具、威胁组织、防护措施关联起来，助力安全人员了解风险传播的路径。智能化防护并非是要取代人工，而是要负责海量数据的处理工作、进行风险筛选、承担辅助决策的任务。

二、人工智能技术在网络安全防护中的主要应用

（一）在入侵检测与异常流量识别中的应用

入侵检测属于网络安全防护里相当关键的部分。传统的系统大多依靠规则匹配，对于已知的攻击能够有比较好的识别效果，然而在面对新型攻击、低频异常、隐蔽渗透的情况时，往往容易出现滞后的状况。人工智能能够收集连接次数、数据包大小、访问时间、协议类型、流量方向、会话时长等各类数据，进而建立起正常网络行为的模型。当终端出现异常外联、大规模扫描、非工作时间高频访问或者异常上传等情况时，系统能够依据行为偏离的程度来进行风险判断。就好比普通办公终端在短时间内频繁连接数据库，并且伴随着多次失败登录，模型可以结合用户角色、历史行为、访问时段来识别潜在的入侵风险，以此提高异常发现的效率。

（二）在恶意代码识别与病毒防护中的应用

恶意代码呈现出变种速度快、伪装能力强、传播范围广等特性，常常借助加壳、混淆、动态加载、重编译等手段来避开传统的查杀机制。人工智能能够从程序结构、函数调用、系统权限、文件操作、进程行为、注册表修改、网络通信等多个维度去提取特征，进而针对可疑程序展开综合评判。静态分析能够在程序尚未运行之时识别出异常代码片段、危险函数调用、可疑指令，而动态分析则可以在沙箱环境里观察加密文件、注入进程、连接异常服务器等实际行为。经过正常样本与恶意样本的训练，模型能够对未知文件进行风险分类，有效辅助安全人员提前察觉勒索软件、木马、挖矿程序等恶意活动迹象，实现对新型威胁的主动识别与预警，提升安全防御的前瞻性。

（三）在安全态势感知与风险预警中的应用

安全趋势感知注重从整体方面去把控网络安全状况，防止孤立地处理单个告警。人工智能能够对终端日志、网络流量、身份认证记录、漏洞扫描结果、数据库访问日志、外部威胁情报加以整合，进而建立起多维安全分析模型。该系统借助分析资产重要性、漏洞危险程度、攻击活跃度、业务影响范围，来为不同事件划分处置的优先级。比如说，若某服务器存在高危漏洞，并且同时出现异常地址访问、异常进程启动的情况，系统就能将其识别为高风险事件并及时发出预警。知识图谱还能够关联攻击工具、漏洞编号、资产位置、攻击路径、防护措施，以此帮助管理人员理解风险的传播关系。

三、人工智能提升网络安全防护效能的作用机制

（一）提高威胁识别的准确性

人工智能能够提高安全防护效果，这主要依赖于其对海量数据具备的学习、比较、识别能力。网络攻击形式繁杂多样，然而在行为方面常常会留下异常痕迹，像是访问频率突然增加、权限请求出现异常、数据传输量出现异常、通信对象出现异常或者操作时间出现异常等情况。智能模型借助学习历史日志、正常业务行为，能够建立行为基线，并且在新数据进入之时迅速判断偏离的程度。相比于人工逐一对日志进行排查，人工智能能够更快速地发现那些细微、连续且关联性较强的风险变化。面对未知攻击，模型也能够依据行为相似性、风险特征做出判断，从而减少漏报的情况，面对重复告警，则能够通过关联分析、风险评分来进行筛选，进而降低误报所带来的干扰。

（二）增强安全运维的自动化能力

网络安全运维包括资产管理、漏洞修复、日志审计、告警处置、权限检查、应急响应等方面的内容，其任务繁杂且具有较强的重复性。人工智能能够承担一部分高频、数据密集型工作，进而提高运维效率。系统可以自动识别新增资产、异常开放端口、未经授权的服务，及时向管理人员发出提醒，以便他们进行核查，在漏洞管理方面，能够依据漏洞等级、资产暴露程度、业务重要性、攻击利用情况，生成修复优先顺序，避免平均使用力量。在告警处置环节，模型可合并同源、同类、连续事件，减少重复提示。结合自动化响应技术，可执行封禁地址、隔离终端、阻断连接、生成报告等操作，提升处置效率。但关键业务处置仍需人工审核，确保决策的准确性与安全性，实现人机协同的高效告警管理。

（三）推动防护体系协同联动

网络安全防护这项工作不是靠单一设备就能完成的，它需要终端、网络、应用、数据、身份等多个方面协同运转才行。人工智能凭借数据融合、关联分析，能够打通不同安全设备间的信息壁垒，把分散的告警转化为完整的安全事件。在传统环境里，防火墙、终端防护、数据库审计、身份认证、入侵检测系统都会各自生成日志，这使得安全人员很难迅速判断事件的全貌。智能平台能够对多源数据进行清洗、标注与关联，发现独立现象背后隐藏的共同风险。比如说，账号异地登录后访问敏感文件，同时终端出现异常进程并向外部传输数据，经关联分析可判定账号被盗、数据泄露风险。系统据此触发封禁账号、隔离终端等响应措施，推动从威胁检测

到处置的防护闭环形成，有效提升安全防御能力。

四、人工智能应用中的问题与优化路径

（一）加强数据治理，提升模型可靠性

人工智能模型能否发挥功效，首要取决于数据质量。网络安全数据来源繁杂，涵盖流量日志资产漏洞、用户行为数据，还有外部威胁情报。要是数据有缺失重复格式混乱标注错误或者样本失衡的情况，模型训练结果就有可能偏离真实场景，出现误报漏报或者判断不稳定的状况。所以要建立统一的数据采集清洗脱敏标注、存储机制，确保数据来源可信格式规范且更新及时。模型训练不能仅依靠公开数据集，还得结合本单位业务特点和真实网络行为加以优化。系统上线后要持续监测准确率召回率误报率、处置效果，并依据业务变化调整参数。对于重要安全判断还需设置人工复核结果追溯、解释说明机制，让模型输出更可靠可控。

（二）完善管理机制，避免技术与业务脱节

人工智能安全应用不能仅仅局限于平台建设、功能展示方面，还需要融入安全管理制度、业务流程、岗位责任当中。在实际情况里，部分单位尽管部署了智能安全系统，但是却并未形成清晰的告警分级、处置流程、责任分工，以至于系统发现异常之后无人进行跟进，风险还是难、时消除。另外，有一些安全人员并不了解模型判断逻辑，对于智能告警要么过度依赖，要么完全排斥，从而影响事件研判质量。智能系统在采集、分析网络行为数据的时候，还会涉及隐私保护、权限边界、合规管理等问题。所以，应当明确数据使用范围、模型维护责任、告警处置标准、应急响应流程，把技术应用纳入整体网络安全治理模式。单位还应当加强复合型人才培养，让安全人员既掌握网络攻防知识，又能够理解数据分析、人工智能基本原理。

（三）构建人机协同的智能防护模式

人工智能于网络安全防护而言有着重要价值，不过绝不能将其视作无所不能的工具。网络攻击具备较强的对抗性，攻击者会持续钻研防护规则，还会借助对抗样本、数据投毒、行为伪装等手段来干扰模型判断。智能系统也有可能因训练样本不够充足、业务场景发生变化或者算法存在局限而出现误判。所以未来网络安全防护要秉持人机协同的思路，让人工智能去承担海量数据处理、异常识别、风险排序、处置建议等任务，由安全人员负责复杂事件研判、攻击溯源、策略制定、关键决策。对于常见的低风险事件，可以通过自动化流程迅速处理，对于涉及核心业务、重要数据、产生重大影响的事件，应当保留人工确认环节。系统要拥有较强的解释能力，能够说明告警原因、数据依据、处置建议，在提高效率的同时确保安全可控。

结　语：

人工智能技术促使计算机网络安全防护模式发生转变。通过机器学习、深度学习、自然语言处理、知识图谱等方式，安全系统能够更为精准地辨认异常流量、检测恶意代码、剖析安全趋势，进而为运维决策给予支持，使得网络安全防护从被动响应逐渐朝着主动预警转变。不过人工智能的应用仍旧受到数据质量、模型可靠性、管理配套、对抗攻击等因素的限制，无法用技术工具取代完整治理。未来要强化数据治理，完善安全流程，培育复合型人才，建立人机协同且动态优化的智能防护模式，推动人工智能在网络安全领域发挥更为稳定的作用。

参考文献：

[1] 肖玉文 . 人工智能在计算机应用软件开发中的实践 [J]. 无人机 ,2025,(11):73-75.

[2] 刘莉 . 人工智能技术在计算机网络安全课程教学中的应用研究 [J]. 信息与电脑 ,2025,37(18):212-214.

[3] 李瑞莹 , 余山林 . 人工智能技术在计算机软件安全防护中的应用 [J]. 软件 ,2025,46(08):68-70.

[4] 张成挺 , 程超 , 王宏铝 , 等 . 人工智能技术在计算机网络安全防护中的应用 [J]. 电脑知识与技术 ,2025,21(01):102-104+107.

[5] 曹越 . 人工智能技术在计算机网络安全中的应用研究 [J]. 中国新通信 ,2023,25(17):119-121.