

基于人工智能的校园网络安全威胁检测与防御技术

安宁刚 成永刚 李 丹
西安交通大学 陕西 西安 710049

摘 要：校园网络具备开放接入、终端类型繁杂、业务场景多元、用户规模庞大等特征，长期面临多样化、隐蔽化、复合型网络安全风险，传统基于规则匹配的静态防护方案存在识别滞后、泛化能力不足、未知攻击无法识别等缺陷，难以应对动态演化的网络威胁。本文结合高校校园网络运行架构、用户业务特征与典型安全风险传播规律，构建完整的 AI 网络安全技术体系，系统阐述数据采集预处理、特征工程、机器学习与深度学习四类智能检测底层技术；分别从流量异常、非法访问、恶意攻击、多源联动四个维度梳理人工智能威胁检测实现路径；围绕动态防御架构、边界智能管控、风险主动阻断、体系迭代优化提出分层智能防御策略。研究成果可为高校智慧校园网络安全运维提供智能化解决方案，全面提升校园网络防护精准度、实时性与主动处置能力。

关键词：校园网络；人工智能；威胁检测；智能防御；网络安全

引言：数字化校园建设持续深化，线上教学、科研数据交互、智慧教务、学生宿舍宽带、物联网教学设备等多业务承载于统一校园网络，网络覆盖范围、接入终端数量、数据传输规模同步快速扩张。校园网络面向全体师生开放，接入管控门槛较低，设备来源混杂、用户安全意识参差不齐，致使病毒入侵、越权访问、流量攻击、数据窃取、内网横向渗透等安全事件频发。传统防火墙、入侵检测系统多采用固定特征库匹配机制，仅能拦截已知攻击，面对变种恶意代码、零日漏洞、隐蔽隧道流量、社工类非法访问等新型威胁识别效果较差，存在防护滞后、误报漏报率高、无法自主适配网络变化等短板。人工智能凭借自主特征学习、非线性拟合、动态迭代优化能力，能够脱离静态规则约束，从海量网络原始数据中挖掘潜在异常行为，实现已知与未知威胁的同步识别。本文依托校园网络实际运维场景，梳理 AI 驱动的威胁检测技术框架，并配套分层、闭环、可动态调整的智能防御体系，保障教学、科研、行政办公业务安全稳定运行。

1 校园网络环境与安全威胁特征

1.1 校园网络架构与运行特点

校园网络是校园数字化建设的核心基础载体，架构层级分明，全面覆盖教学、办公、宿舍及公共活动等校园场景。网络体系采用核心交换层、汇聚层、接入层三级部署，多设备协同构建全域局域网系统。校园网络接入节点数量多、分布零散，终端端口长期开放运行。网络流量随时段波动显著，教学高峰期与课余时段的数据传输负荷差异明显^[1]。同时，校园网络服务类型多元，兼顾教学科研、日常办公、线上学习与休闲娱乐等各类业

务需求。

1.2 校园网络用户与业务场景属性

校园网络用户群体庞大，涵盖师生、行政工作人员等，人员结构复杂，网络操作水平与使用习惯差异较大。接入终端类型丰富，包含手机、电脑、平板及各类智能教学设备，终端接入场景灵活多样。网络承载业务具备极强的公共性，教学直播、科研数据传输、办公系统运行、学生线上浏览等多类业务同步并行，整体运行场景繁杂且动态性强。

1.3 校园网络常见安全威胁类型

校园网络的复杂运行环境催生了常态化、多元化的安全威胁，风险贯穿网络运行全过程。异常流量入侵、非法网络访问、恶意代码植入是校园网络最主要的安全威胁。外部网络攻击常试图突破校园网络边界，窃取内网数据、干扰网络正常运行。此外，终端设备携带的风险程序接入内网后，会直接破坏局域网运行环境；用户访问、下载非正规网络资源的行为，也会带来隐性网络安全风险。

1.4 校园网络威胁传播与演化特征

校园网络终端密集、内网互联性强，安全威胁具备传播速度快、扩散范围广的显著特征，单一终端风险可通过内网链路快速蔓延至全网。随着网络防护体系的迭代，网络攻击从传统单一模式逐步演变为复合型攻击。同时，网络威胁隐蔽性持续提升，多数攻击不会在接入初期爆发破坏，而是长期潜伏于网络链路终端设备中，逐步侵蚀网络运行环境，提升网络故障爆发概率，大幅增加安全防护难度。

2 人工智能网络检测技术基础体系

2.1 网络数据采集与预处理技术

人工智能网络检测的核心基础是全网数据采集,可实时抓取校园网络链路流量报文、终端访问记录、设备交互数据等原始信息,为安全分析提供数据支撑。网络运行产生的原始数据体量庞大,存在大量冗余、重复、无效内容,无法直接用于模型分析运算^[2]。数据预处理技术可对原始数据进行清洗、去重、纠错、格式统一等标准化处理,补齐缺失字段、规整数据结构,剔除干扰性无效数据。规范化后的数据集可适配人工智能模型运算标准,保障后续特征分析与风险识别的精准性与高效性。

2.2 人工智能特征提取与筛选方法

网络数据维度丰富、信息繁杂,精准提取有效特征是识别网络安全威胁的核心关键。人工智能技术可从流量波动、访问频次、传输时长、协议调用状态等多维度,深度挖掘网络数据中的隐藏行为特征。初始提取的特征数量繁杂,存在大量低关联、低区分度的无效特征。智能算法可通过分层筛选机制,剔除无效特征、保留核心关键特征,有效区分网络正常操作与异常攻击行为,压缩特征维度。该方式可降低模型运算负荷,聚焦风险识别核心指标,构建精准、高效的网络特征体系。

2.3 机器学习异常识别技术原理

机器学习是当前网络异常检测的核心技术,依托海量标准化网络样本数据完成自主迭代学习。模型通过持续训练,总结正常网络行为的运行规律,划定合规的参数波动区间,同时积累各类异常网络行为的特征数据,形成完善的风险识别逻辑。在实时检测场景中,训练成熟的模型可比对实时网络数据与历史学习样本,精准判断数据偏离与行为异常状态。模型通过持续迭代优化识别逻辑,不断提升对未知异常行为的分辨能力,适配网络风险动态演化的场景需求。

2.4 深度学习网络行为分析机制

深度学习基于多层神经网络架构,可实现复杂网络行为的精细化研判,弥补传统检测技术的短板,精准捕捉浅层算法无法识别的隐性风险与复合型网络异常。多层神经网络可对海量网络数据进行分层解析,挖掘各类网络行为的潜在关联,梳理隐蔽的异常数据规律。针对校园网络多变的访问模式、复杂的流量传输状态,深度学习可实现全方位精细化研判,精准识别隐蔽攻击、变异异常流量等高危行为,构建全面精细的网络行为分析体系,为校园网络智能安全检测筑牢技术根基。

3 基于人工智能的校园网络安全威胁检测技术

3.1 网络流量异常智能检测技术

校园网络流量状态随时变化,数据构成种类繁多,传统检测手段很难发现细节性的流量异常问题。人工智

能技术可以对全网流量数据进行深度拆解与分析,总结日常流量传输的稳定状态与变化规律。算法能够精准捕捉带宽占用突然升高、数据包传输秩序混乱、大量无效请求频繁出现等异常状态。可以清晰地区分正常业务产生的流量和攻击行为产生的异常流量,能够识别低频波动、形态变异等隐蔽性极高的异常流量类型^[3]。这类技术不再局限于固定的匹配规则,依靠自主数据学习能力适配校园网络复杂多变的流量场景,有效提升流量异常的识别精准度,从数据传输层面夯实校园网络的安全防护基础。

3.2 非法访问行为智能识别技术

校园网络面向全体师生开放接入端口,宽松的接入环境容易滋生各类网络访问风险,越权操作、陌生设备接入的问题时有发生。智能识别技术可以针对全网访问行为搭建完整的分析逻辑,梳理合法用户常规的访问路径、登录时段以及资源访问范围。系统会对各类非常规访问操作进行深度判断,及时发现跨权限操作、陌生终端接入、非工作时段异常登录等违规行为。算法长期积累用户日常访问习惯,主动识别和标记脱离常态的异常访问行为。可以弥补传统检测方式的不足,精准捕捉隐性越权操作,拦截各类非法访问行为,降低校园内部资源被违规读取和篡改的风险。

3.3 恶意代码与攻击行为智能甄别技术

网络攻击方式处于持续更新的状态,不断出现形态变异的恶意程序和新型攻击手段,持续增加校园网络防护的工作难度。智能甄别技术依托成熟的深度学习算法,对网络传输文件、终端运行程序以及后台进程开展全方位排查。精准挖掘程序运行过程中的异常特征,准确区分正常程序与恶意脚本、植入病毒等危险内容。针对端口扫描、数据嗅探、漏洞试探等常见攻击方式,搭建针对性的识别模型完成专项检测。模型通过海量攻击样本积累识别经验,对各类新式、变异攻击行为具备良好的分辨能力,减少新型攻击绕过防护体系的可能性,主动完成各类网络恶意攻击的甄别排查工作。

3.4 多维度网络威胁联动检测机制

单一的检测角度存在明显识别盲区,很难应对当下结构复杂、隐蔽性强的校园网络安全威胁。多维度联动检测机制融合流量分析、行为研判、代码甄别等多种检测手段,搭建覆盖范围更广的智能化检测体系。分别从网络传输链路、终端操作行为、程序运行状态等多个角度采集数据,综合判断网络整体安全运行情况。有效突破单一检测技术的功能局限,弥补传统识别模式存在的漏洞和短板。多维度数据相互交叉验证,能够精准筛查

隐蔽性强、特征不明显的复合型网络威胁,扩大校园网络安全筛查的覆盖范围,提升检测深度,打造稳定性和全面性更强的智能检测体系。

4 校园网络安全智能防御技术与优化策略

4.1 动态智能防御部署架构

传统校园网络防御模式多为静态固化部署,防护策略长期保持不变,难以适配持续迭代的网络攻击手段。动态智能防御架构依托人工智能技术完成整体搭建,能够根据校园网络运行状态自主调整防护模式。架构整合网络监测、风险分析、防御响应等多个功能模块,形成一体化的闭环防御体系^[4]。可以根据全网流量变化、终端接入数量、风险出现频次等数据,自主调整防护强度与策略规则。灵活适配教学、办公、课余休闲等不同场景的网络运行需求,打破传统防御模式僵化滞后的弊端,让校园网络防御工作更具灵活性与针对性。

4.2 网络边界智能防护技术

网络边界是校园内网与外网数据交互的关键通道,也是各类网络攻击的主要突破点位。边界智能防护技术针对网络出入口开展全方位安全管控,细化数据传输的审核标准。依托智能算法筛查进出网络的各类数据报文,拦截携带风险特征的传输内容。技术可以自主识别可信访问来源与高危访问渠道,对陌生外网接入、异常数据传输进行严格管控。针对端口非法外联、跨网渗透等常见边界风险建立专属防护机制,牢牢守住校园网络进出口通道,减少外部风险渗透入侵的可能性,筑牢校园内网的边界安全屏障。

4.3 校园网络风险主动阻断技术

被动防御模式只能在风险爆发后开展处置工作,无法提前规避网络安全隐患。风险主动阻断技术依托智能检测能力,实现网络风险的前置化处置。系统可以实时监测全网运行动态,提前捕捉异常流量、违规访问、恶意程序运行等潜在风险苗头。在高危行为尚未对网络系统造成破坏前,自动触发隔离、拦截、断联等防护操作。精准限制风险终端的网络接入权限,阻断恶意程序的传播路径,弱化风险扩散带来的负面影响。从源头遏制各类网络隐患发酵,大幅提升校园网络安全防护的主动性与时效性。

4.4 网络安全防御体系优化思路

校园网络环境与攻击手段始终处于动态变化状态,防御体系需要持续迭代完善,适配全新的安全场景。优化工作可以从技术、管理、运行三个层面同步推进,补齐现有防御体系的短板。持续更新智能算法模型,吸纳新型威胁特征,提升系统对未知攻击的识别能力。细化校园网络分层防护机制,针对核心业务区域、普通终端区域划分差异化防护等级。定期梳理防御运行漏洞,调整防护策略细节,适配校园网络业务的更新迭代^[5]。逐步构建适配校园场景、响应速度快、容错能力强的智能防御体系,持续提升校园网络整体安全运行水平。

结束语

校园网络用户开放、终端混杂、业务多元,传统静态安全防护手段已无法应对持续演化的复合型、隐蔽化网络威胁。人工智能技术通过多源数据预处理、自动化特征挖掘、机器学习与深度学习模型,可实现流量异常、非法访问、恶意攻击全类型威胁精准识别,解决传统检测漏报、滞后、泛化性差等痛点。依托动态闭环防御架构、边界智能管控、风险自动阻断、体系持续优化策略,能够构建主动式校园网络安全防护体系,从被动告警转向前置拦截,全方位降低入侵、数据泄露、网络瘫痪等安全事件发生概率。后续可结合联邦学习、大模型安全分析技术进一步优化检测精度,持续升级智慧校园网络安全底座,为数字化教学、科研、办公业务提供稳定可靠的安全支撑。

参考文献

- [1]王欠欠.基于人工智能的校园网络安全威胁检测与防御技术[J].信息记录材料,2026,27(6):127-129.
- [2]步扬坚.人工智能驱动的校园网络安全防御体系设计与实现[J].信息记录材料,2026,27(8):39-41.
- [3]李世楠,陈灿.网络安全防御中的人工智能技术研究[J].信息记录材料,2026,27(3):129-132.
- [4]刘平.人工智能的高校校园网络信息安全防护方法[J].信息记录材料,2025,26(1):163-165.
- [5]杨位林,李杰.人工智能驱动的入侵检测技术在网络安全防护中的应用研究[J].中文信息,2025(9):15-16.