基于人工智能的网络通信安全与计算机病毒防护研究

聂良刚
广西财经学院大数据与人工智能学院，广西 南宁 530003

摘要：随着信息技术的不断发展，网络通信逐渐渗透到人们日常生活的方方面面。然而，计算机病毒和恶意软件的快速演变使网络通信安全面临前所未有的挑战。人工智能（AI）因其强大的数据处理和自动学习能力，正在网络安全领域发挥不可替代的作用。为此，探讨基于人工智能的网络通信安全和计算机病毒防护方法，分析这些技术在威胁识别、自动化响应和实时防御中的应用优势，并讨论 AI 技术在病毒防护中的发展前景，具有重要的现实意义。

关键词：人工智能；网络通信安全；计算机病毒

Research on Network Communication Security and Computer Virus Protection Based on Artificial Intelligence

Nie,Lianggang

Faculty of DB and AI, Guangxi University of Finance and Economics, Nanning, Guangxi, 530003, China

Abstract: With the continuous development of information technology, network communication has gradually penetrated into all aspects of people's daily life. However, the rapid evolution of computer viruses and malicious software makes network communication security face unprecedented challenges. Artificial intelligence (AI) is playing an irreplaceable role in the field of network security because of its powerful data processing and automatic learning ability. Therefore, it is of great practical significance to explore the methods of network communication security and computer virus protection based on artificial intelligence, analyze the application advantages of these technologies in threat identification, automatic response and real-time defense, and discuss the development prospect of AI technology in virus protection.

Keywords: Artificial intelligence; Network communication security; Computer virus

DOI: 10.62639/sspis07.20250201

网络通信安全和计算机病毒防护已成为信息时代不可忽视的课题，在传统的网络安全框架中，防火墙、入侵检测系统（IDS）和防病毒软件是常见的防护手段，但它们的被动式防御难以应对日益复杂的高级持续性威胁（APT）和零日攻击[1]。人工智能技术凭借其数据处理和自适应特性，逐渐被应用于网络安全领域，能够识别复杂威胁，提供自适应的防护策略，并在病毒防护中展现出极大潜力。本文将基于相关研究，探讨 AI 在网络通信安全与病毒防护中的应用及其未来发展方向。

一、人工智能在网络通信安全中的应用

（一）威胁识别和异常检测

在网络通信安全领域，实时威胁识别是核心。人工智能特别是基于机器学习的算法，能够从海量网络流量数据中识别异常模式，以此检测潜在威胁。AI 在这方面的应用主要依赖于深度学习、机器学习和异常检测算法，这些算法通过训练大量正常流量的数据，建立一个网络“基线”，任何偏离这个基线的流量模式都会被标记为异常，从而形成威胁预警。

1. 数据采集和特征提取

实时采集网络流量：AI 模型通常在数据采集层实时提取网络流量数据，包括 IP 地址、端口、协议类型、数据包大小、传输频率等关键信息。这些流量特征参数能够反映网络中的基本通信行为[2]。

特征提取与归一化处理：从数据包中提取特征，如连接时长、数据包间隔时间、请求频率等。此外，通过归一化处理，算法可以更有效地分析和比较不同来源的数据。

2. 基线建立

深度学习算法在初始训练阶段分析大量的正常流量数据，形成该网络的“正常行为”模型。例如，一些企业的特定时间段内的流量较大，算法需要识别出这种规律，避免误报。

自编码器是一种常用的神经网络结构，在训练时主要学习输入数据的主要特征，并通过还原输出检测异常[3]。在威胁识别中，自编码器的输出与实际流量特征对比，当重构误差超过阈值时即判定为异常。

在银行等金融机构，AI 威胁识别系统能够检测到可疑的银行交易流量，AI 系统可根据网络访问频率或交易金额异常变化的检查结果，迅速识别潜在的欺诈交易，并及时通知安全人员采取行动。

（稿件编号：IS-25-1-1016）

作者简介：聂良刚（1971-），男，汉族，籍贯：广西藤县，硕士，教授，研究方向：网络，信息化，软件及算法。

基金项目：中国高校产学研创新基金 - 新一代信息技术创新项目：“基于云、本地和 AI 人工智能技术的病毒防护体系研究与应用”（基金号：2021ITA11014）。

（二）自动化入侵检测和响应

在入侵检测和响应中，AI 可依托自动化技术实现更快速、精确的响应，减少人为误操作的风险。在入侵检测系统（IDS）和入侵防御系统（IPS）中，AI 模型可以自动识别威胁并立即采取行动，无需等待人工操作。

1. 多层检测机制

AI 系统可利用多层检测架构，其中决策树和随机森林算法用于初步判断是否存在入侵，这些算法基于对网络流量基本特征的分析，对网络通信进行快速分类，并标记异常的流量类型。

对于被初步检测为可疑的流量，系统可基于更复杂的深度学习模型（如卷积神经网络 CNN 和长短期记忆网络 LSTM）进行进一步分析，从而检测更隐蔽的威胁 [4]。

2. 实时响应

在检测到恶意流量或入侵行为后，AI 系统能够自动执行应急操作，比如阻断可疑 IP 地址、断开感染设备与网络的连接，或隔离特定网络区域。这些自动响应操作可以在毫秒级完成，极大地缩短了响应时间。

AI 系统可以实时调用威胁情报数据库，将流量特征与全球已知威胁库进行比对，并自动判断是否需要采取全网扫描、流量重定向等更高级别的应对措施。比如在公司邮件系统中，AI 可以实时扫描邮件内容，识别出包含恶意链接或钓鱼企图的邮件，再利用 NLP 和图像识别分析邮件附件和正文内容，自动化拦截钓鱼邮件。

（三）自适应安全策略调整

AI 技术在应对新型和多样化威胁方面尤为重要，以自适应调整安全策略实时优化网络防御效果，并依赖于深度学习和强化学习实现对威胁的动态应对。

1. 自适应学习的工作流程

在自适应学习系统中，深度学习模型会定期分析新发现的病毒特征、攻击方式等最新的威胁情报数据，并据此更新判断标准 [5]。

强化学习算法通在不断训练中学习如何最优选择防御策略。例如，当系统识别到网络中存在新的攻击行为时，可以模拟不同防御策略的效果，并作出自我调整，以最佳方式应对新威胁。

2. 实时调整策略参数

在自适应系统中，防火墙的规则设置不再是固定的，而是随着网络环境变化自动调整。系统可以根据网络流量的变化，在某段时间内关闭对某些端口的访问或限制流量带宽。

AI 系统还会根据网络中不同事件的频率、强度等自动调整风险等级，动态提升或降低某些设备的安全优先级。例如，当系统发现某个 IP 访问过于频繁、尝试获取高级权限时，会自动将该 IP 的风险等级提升到“高”，并增加监控力度。

二、基于 AI 的计算机病毒防护策

（一）病毒行为分析与检测

传统防病毒软件主要依赖于病毒特征库，依靠比对文件特征与已知恶意代码的签名来识别病毒。这种方法虽然对已知威胁有效，但面对新型病毒或恶意软件时显得滞后，无法满足实时防护需求。人工智能（AI）防病毒系统则利用行为分析技术，能够识别并检测出异常行为，而无需依赖特征库，因而能够在新型病毒出现的初期即对其进行识别和隔离。

1. 异常行为检测的基础构建

AI 系统可分析大量正常程序行为的数据样本，从而构建一个“正常行为”的基线，具体包括程序的网络请求、系统调用、CPU 及内存使用模式等。这一基线使得 AI 系统能够准确判断程序行为的正常范围，从而识别偏离该基线的异常活动。

常见的行为参数包括网络端口使用情况、访问频率、文件系统的读写行为、权限获取行为等。举例来说，当某个程序在短时间内多次尝试访问高权限资源，或频繁打开异常网络端口，AI 系统会将其标记为异常，进一步分析其潜在的恶意特征。

2. 行为分析模型

Cylance 等 AI 防病毒软件通常采用深度学习模型来识别恶意行为，如卷积神经网络（CNN）可以对程序行为特征进行多层次分析，辨识不同恶意代码的共性模式，而长短期记忆网络（LSTM）可追踪行为序列中的时间相关性，准确地判断行为模式是否异常。

AI 系统以自适应学习不断更新恶意行为的检测能力。例如，Cylance 防病毒软件可以利用行为分析在新型病毒初期即发现其潜在威胁，某恶意程序试图通过特定端口访问敏感信息或尝试获取管理员权限时，AI 系统能够识别这一异常行为并及时警报，在病毒传播前提前采取防护。

（二）基于 AI 的邮件监控与反钓鱼技术

网络钓鱼邮件是计算机病毒传播的常见手段，具有高度的隐蔽性和针对性。传统的反钓鱼手段通常依赖于关键字过滤和黑名单规则，效果有限。而基于 AI 的反钓鱼技术通过自然语言处理（NLP）和图像识别技术，能够对钓鱼邮件的文本和图像内容进行深层次分析，显著提高检测精度。

1. NLP 在钓鱼邮件检测中的应用

NLP 利用词向量化（如 Word2Vec）等技术将邮件内容转化为数值表示，使 AI 系统能够分析内容的语义和上下文。例如，在识别钓鱼邮件时，NLP 技术可以检测到常见的钓鱼模式语句，如“点击以下链接以确认账户信息”等。

NLP 还能分析邮件的情感倾向（如紧迫、恐吓等），判断是否存在社交工程特征。许多钓鱼邮件采用引发恐惧或紧迫感的方式诱使用户点击恶意链接。AI 系统基于情感分析，将会识别这些诱骗特征，并将邮件标记为可疑。

2. 图像识别技术

钓鱼邮件通常伪装成知名公司的官方邮件，利用伪造的 Logo 或图像引导用户点击恶意链接。AI 利用卷积神经网络（CNN）等深度学习模型，

对邮件中嵌入的 Logo、图片等进行识别，判断其真实性。当图像内容和公司官方 Logo 的像素特征存在显著差异时，系统将发出警报。

AI 还可以基于图像识别技术，检测邮件中的嵌入链接，判断链接的潜在风险。例如，识别常见的链接伪装技术，如在 URL 中加入“0”替代“o”等方式误导用户，及时识别、阻止潜在的钓鱼攻击。在金融行业，AI 钓鱼邮件检测系统已广泛应用于识别伪装成银行或信用卡公司邮件的钓鱼邮件，系统可以利用 NLP 分析邮件内容并结合图像识别技术，准确识别出假冒邮件，有效防止客户上当受骗。

（三）恶意程序检测与自愈功能

AI 防病毒系统不仅在检测方面具备优势，还具备自愈功能，可以在感染发生后自动采取修复措施，使被感染系统尽快恢复到健康状态。这种自愈功能在面对病毒传播、数据破坏等情况时尤其有效。

1. 自动隔离和响应

AI 系统能够识别感染源头并实时隔离受感染设备，当系统检测到某一台计算机已被恶意程序感染，AI 自动将该设备与网络隔离，防止病毒在网络中的横向扩散。

AI 依靠行为分析和日志数据追踪恶意程序的传播路径，从而在更广泛的网络环境中进行预防。在对入侵路径进行识别后，即能够阻止其他设备受到相同感染源的侵害。

2. 系统修复与数据恢复

AI 自愈功能的一个关键操作是自动清除恶意代码，系统会利用行为特征库识别恶意文件的位置和依赖，实施自动删除，彻底清除病毒。

AI 系统在实施自愈时通常伴随数据恢复操作，系统可以在清除恶意代码后自动恢复被恶意程序篡改的数据文件。系统还能够基于深度学习模型，从已知的备份文件中提取关键数据，最大限度地恢复数据完整性。例如，在应对勒索病毒的场景下，AI 系统检测到病毒后，立即启动隔离操作，阻断网络连接，防止进一步传播。系统会同时自动扫描文件损坏情况，提取备份文件，恢复原始数据，尽可能不破坏业务的连续性。

三、基于 AI 的网络安全未来发展方向

（一）构建更安全的 AI 防御系统

当前，AI 防御系统的主要挑战在于对抗样本攻击和数据依赖性问题，特别是在面对复杂攻击时，传统的单一模型容易被对抗样本误导，从而造成识别误判。为增强 AI 系统的安全性，未来的防御系统将采用多模型协作机制，即多个机器学习模型协同工作，利用不同算法视角交叉验证可疑样本，减少误判率。此外，博弈论在此场景下也扮演着关键角色，能够帮助 AI 系统模拟攻击者行为，基于“对抗 – 防御”反复迭代，提升 AI 模型的应对策略。与此同时，保护用户隐私的需求日益增强，未来的 AI 防御系统将进一步采用隐私保护机器学习方法—差分隐私和联邦学习，该方法可对数据进行细微扰动，避免用户信息泄露，而联邦学习允许多个设备协同训练模型而无需共享具体数据，从而在保障数据隐私的同时实现模型的高效训练。

（二）零信任架构与 AI 融合

零信任架构基于“永不信任，始终验证”的理念，不再对网络内任何设备或用户默认授权，而是要求每一次访问都经过严格的身份验证和权限检查。AI 技术在零信任架构中的应用能够极大地提高其实施效率。例如，利用机器学习分析用户的行为模式，AI 系统可以识别出正常的访问行为和异常的访问请求，一旦检测到异常活动，便会自动阻断访问或提升验证级别。AI 还能动态管理用户权限，自动更新安全策略，使用户的权限始终符合安全需求。AI 的实时数据处理和自动化决策能力为零信任架构提供了强大的技术支撑，使得大规模、多节点网络环境中的每个访问请求都得到及时的验证和监控，降低了攻击者从内部渗透网络的可能性。

（三）加强人工智能与网络安全的跨领域合作

AI 防御技术需要整合计算机科学、数据科学、心理学等多个学科的知识，才能在更复杂的网络攻击面前做出准确判断。例如，心理学研究对社交工程攻击的影响有深入了解，将这些洞察融入 AI 防护系统可以有效提升对网络钓鱼等攻击手段的防范能力，不同专业的专家基于学科间的合作，可共同优化防护策略，使 AI 系统在应对新型攻击时具有更高的可靠性。与此同时，建立统一的技术标准和法规规范，也将会成为实现跨学科合作的必要保障。清晰的技术标准可以指导不同领域的协同研发，法规规范用于保障 AI 防护技术在应用时符合法律与伦理要求，推动网络安全 AI 技术的良性发展，增强用户对 AI 防护的信任度。

四、结语

人工智能为网络通信安全和病毒防护带来了新的机遇，凭借其数据分析与自适应学习能力，AI 在威胁识别、网安态势预测、自动化响应和病毒防护等方面表现出色。然而，AI 在网络安全应用中也面临对抗样本攻击、数据质量偏差和算法可解释性等挑战。因此，未来需要持续提升 AI 系统的鲁棒性、构建安全的机器学习算法、应用零信任架构及强化跨领域合作，这样才能在网络通信安全和病毒防护中发挥更大作用，为网络空间的安全提供有力保障。

参考文献：

[1] 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（09）：142-144.
[2] 罗志强．基于人工智能的网络通信安全风险防护探究 [J]．中国宽带，2023，19（06）：13-15.
[3] 胡化猛，马麟．人工智能时代计算机信息安全与防护策略分析 [J]．信息系统工程，2023，（04）：77-79.
[4] 韩艳．基于数据加密技术的计算机网络通信安全防御研究 [J]．信息与电脑（理论版），2022，34（11）：215-217.
[5] 戴训安，申有祥，潘丹．大数据背景下信息通信网络安全管理策略研究 [J]．中国新通信，2022，24（03）：7-9.