 DOI: https://doi.org/10.12349/iser.v6i5.5683

Explore the application of AI technology in computer network monitoring

Jiaqiong Chen

Shimen County Forestry Bureau, Changde, Hunan, 415300, China

Abstract

In the context of rapid development in modern network technology, cyber attack forms have become increasingly complex and diverse, posing serious threats to the secure operation of network systems, and even severely endangering personal privacy and corporate secrets. Therefore, it is essential to strengthen computer network monitoring, particularly by integrating artificial intelligence technologies to achieve real-time monitoring and in-depth analysis of network traffic, data transmission, and user behavior, effectively defending against various cyber attacks, thereby ensuring the secure operation of networks. This article primarily analyzes the key points of applying AI technology in computer network monitoring, aiming to enhance the level of computer network security protection and effectively safeguard the privacy and security of network users.

Keywords

AI technology; computer; network monitoring

探索 AI 技术在计算机网络监测中的相关运用

陈家琼

石门县林业局，中国 · 湖南 常德 415300

摘　要

在现代化网络技术高速发展背景下，网络攻击形式越来越复杂化和多样化，严重危害网络系统的安全运行，甚至对个人隐私、企业机密等造成严重威胁。基于此，需要做好计算机网络监测工作，尤其要对人工智能技术进行融合应用，实现网络流量、数据传输、用户行为的实时监控和深度分析，并有效防御各类网络攻击，进而保障网络安全运行。文章主要对AI技术在计算机网络监测中的应用要点进行分析，从而有效提升计算机网络安全防护水平，有效保护网络用户的隐私安全。

关键词

AI技术；计算机；网络监测

1 引言

在现代化信息技术发展背景下，网络攻击逐渐从以往的病毒、勒索软件等向高级持续性威胁、僵尸网络等方向发展，对用户信息安全造成极大威胁。基于此，要结合实际情况，持续性优化计算机网络监测技术，尤其要对人工智能技术进行联合应用，进而创新网络安全监测策略，尤其要发挥人工智能技术在网络流量分析、入侵检测技术、恶意软件检测、用户行为分析等方面的功能作用，强化数据处理能力和响应能力，有效提升计算机网络安全防护效果。

2 AI 技术在计算机网络监测中的应用价值

AI 技术可以对人类智能进行模拟和扩展，并确保计算机系统能够具备数据处理、学习、决策能力。其中人工智能技术包含机器学习、深度学习、自然语言处理等技术。在计算机网络监测中引入人工智能技术，能够实现网络数据的动态监控、分析、预警和处置，有效提升网络智能化、自动化防御能力[1]。尤其可以分析海量网络数据、日志信息，对异常的网络流量、行为模式等进行精准、快速、自动识别，第一时间发现网络攻击等现象，并发出响应预警，协助网络管理人员及时采取合理措施进行处理，保障网络运行安全。其中，人工智能技术在计算机网络监测中的应用优势体现在：预警能力强，能够精准预测可能存在的安全维修，并第一时间发出预警，确保网络管理人员能够第一时间采取响应的措施；自动化程度高，能够对不同类型的网络攻击进行自动识别、分析和处置，减轻网络安全人员的工作压力；适应性强，能够结合网络环境的变化情况，进行自我学习和调整，使其对各类复杂场景进行良好适应；安全性高，能够对黑客攻击进行高效防御，保障监控系统可靠运行。其中智能化网络监控系统主要在企业网络安全防护、公共网络安全监管、家庭网络安全防护等场景中进行适用。

【作者简介】陈家琼（1993–），女，土家族，中国湖南常德人，本科，助理工程师，从事电子计算机研究。

3 AI 技术在计算机网络监测中的应用要点

3.1 网络流量分析

在计算机网络监测工作中，网络流量分析是重要的监测技术之一。在具体监测工作中，通过 AI 技术中的机器学习功能对网络流量的正常行为进行自动学习，同时监测和抓取网络中传输的数据包，对其展开全面分析，进而第一时间发现异常数据、流量分布、网络使用情况等，并及时发现报警信号，及时定位潜在危险。其中常见的网络流量分析工具有 Wireshark、NetFlow 和 sFlow 等。其中，基于机器学习的网络流量数据安全可视化监测系统如图 1 所示。如利用 AI 系统能够对传输数据包的大小、流量频率、访问路径等特征，对可能存在的分布式拒绝服务攻击、数据泄露等网络攻击行为进行精准识别[2]。而且机械学习模式可以即时发现不正常的行为模式，且误报率较少，能够有效提高计算机网络安全监测和防护的准确性。随着计算机网络技术的高速发展，网络攻击形式越来越复杂，以往预定义规则和特征库的网络流量分析方法已经不适用，需要充分利用 AI 技术的机器学习和深度学习算法功能，对海量的网络数据进行自动学习和智能分析，并抓取有价值的信息特征，并对其中存在的异常流量、可能存在的威胁进行精准识别。尤其可以利用人工智能对网络流量开展动态监测和分析，确保能够自动识别网络中的异常流量模式，并自动生成分析报告，协助网络管理员第一时间确定异常问题，并提出针对性的处理策略。

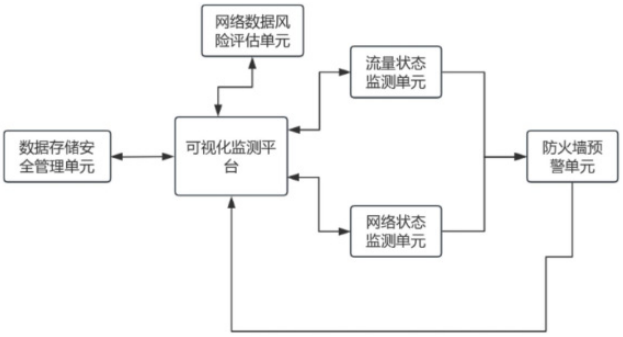

图 1 基于机器学习的网络流量数据安全可视化监测系统

3.2 入侵检测系统

入侵检测系统就是对网络、系统活动进行监测的重要手段，可以对网络中可能存在的恶意活动、政策违规等现象进行精准识别，并第一时间做出响应。这是计算机网络安全防护的关键方法之一。面对当前日益复杂的网络攻击，需要在入侵检测系统中引入 AI 技术，这样可以有效提升网络威胁检测效率和响应能力。其中入侵网络系统包含 HIDS 和 NIDS 等类型[3]。利用 AI 技术的机器学习和深度学习算法功能，对海量网络数据展开全方位、多角度、深层次学习和分析，并及时识别网络数据中的异常行为模式，并明确其中可能存在的威胁。此外，要结合网络日益出现的新型攻击手段，对模型进行不断更新，确保人工智能入侵检测系统可以对新型攻击手段进行良好适应，保障入侵检测工作的高效性、准确性进行。尤其可以利用实时监测、日志分析等方式，尤其可以利用深度学习功能动态分析网络攻击行为模式，挖掘入侵行为的潜在特征，精准识别新型网络攻击，如高级持久性威胁等，并及时发出警报信号，协助管理人员高效采取防御措施。例如，为了保障林业内网安全运行，需要对人工智能技术进行优化应用，保障网站维护工作的高效开展。如可以通过机器学习、深度学习算法等技术，精准识别黑客攻击、病毒入侵、软件恶意攻击等问题，并第一时间采取紧急措施，保障林业内网安全，为林业资源的优化处理创建良好条件。

3.3 用户行为分析

在计算机网络监测工作中，通过用户行为分析功能需要对用户的网络行为进行动态监测和智能分析，精准识别异常行为，并深入分析可能存在的安全威胁。在人工智能技术支持下开展用户身份认证工作，尤其需要利用面部识别、指纹识别、虹膜识别等生物识别技术，对网络用户的身份进行验证；此外还能够通过分析用户键盘敲击节奏、鼠标移动轨迹等行为模式对用户身份进行持续验证，进而保障计算机网络安全防护。在用户行为分析工作中引入人工智能技术，可以构建用户行为模型，对正常用户的行为模式进行智能学习和记录，精准识别用户的异常行为，如异常登录、数据泄露、内部攻击等，并第一时间发出警报信号，这时候系统就能够自动制定应对措施[4]。其中，常见的网络安全防护措施有身份验证步骤、限制访问权限、发出警报等。通过人工智能技术的优化应用，能够更加精准地分析用户行为，不需要人为干预，保障网络安全防护效果的提升。

3.4 恶意软件检测

当前，恶意软件持续变种，如病毒、蠕虫、木马等对网络安全造成极大的威胁。因此，要充分发挥人工智能技术的深度学习模型和算法，对恶意软件的行为模式、代码特征等展开全面训练，及时发现未知的恶意软件。在具体检测过程中，需要利用人工智能技术的静态分析、动态分析等功能，深入分析网络中传输的数据包，并识别恶意代码特征和行为模式，同时检测恶意软件的传播方式、目标行为等；同时还需要对海量的网络数据进行智能学习和训练，精准检测恶意软件，并利用阻止、隔离等措施进行处理[5]。由此可见，人工智能技术与恶意软件检测技术的融合应用，能够对网络活动进行动态监测，及时发现新型威胁，避免恶意软件传播，降低系统攻击。

3.5 自动防御与响应技术

当前，网络威胁越来越复杂化，且威胁形式日益呈现多样化趋势，为了保障计算机网络安全，既要做好网络监测工作，同时要在人工智能技术支持下开展自动化响应和自动化防御，如针对网络攻击，能够利用人工智能技术高效、精准分析攻击源，并通过调整流量路由的方式减轻攻击压

力；针对恶意软件传播需要利用人工智能技术对受到感染的设备进行自动隔离，避免在更大范围内传播；及时停止恶意进程或者关闭受攻击的端口。在人工智能技术支持下，可以结合实时数据第一时间做出动态响应，并形成自动化响应机制，一旦检测到异常流量，就可以及时评估攻击危害程度，同时自动调整防火墙策略，并对入侵检测规则进行灵活性调整，利用自适应响应有效防御潜在威胁。

3.6 威胁情报与安全预测

人工智能技术在网络威胁情报和安全预测中的应用，能够利用自然语言处理技术、机器学习技术，对网络威胁情报源信息进行自动抓取，精准识别和分析潜在威胁，如新的威胁签名和攻击模式等，为后续网络安全防御做好准备工作。其中，基于机器学习的网络安全监测系统如图 2 所示。在安全态势预测工作中，要利用机器学习、大数据分析工作，精准预测网络攻击，尤其可以对历史攻击数据、网络流量模式等进行全方位分析，科学预测潜在的攻击趋势，进而协助企业制定针对性的防护措施和相应方案，保障计算机网络安全。

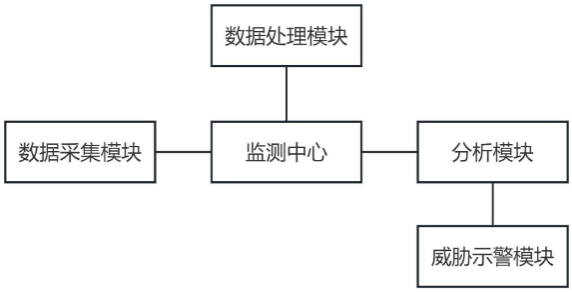

图 2 基于机器学习的网络安全监测系统

3.7 其他方面

①网络性能监测，就是对网络可用性、延迟、带宽等指标进行动态监测，尤其可以利用 SNMP 等监测工具，确保网管人员能够第一时间抓取网络性能数据，并结合数据分析结果，持续性优化调整网络运行方案。②日志管理，在该技术应用中，要对服务器、网络设备、应用程序等日志进行全面收集、存储、分析，帮助网络管理人员对用户活动进行动态追踪，并实时识别异常行为，同时采取针对性的故障排除措施。

4 结语

综上所述，为了进一步提高计算机网络安全，需要做好网络安全监测工作，尤其要对人工智能技术进行融合应用，如网络流量分析、入侵检测系统、恶意软件检测、用户行为分析等方面，实现海量数据的实时监控和分析，及时发现异常数据和异常行为，第一时间发出响应预警，并采取针对性的应对措施，有效提升网络安全防护效率。

参考文献

[1] 徐帅. AI大模型构建智能网络安全防御体系研究 [J]. 安徽电子信息职业技术学院学报, 2024, 23 (04): 17-20.

[2] 吴俭. 人工智能在计算机网络监测中的应用研究 [J]. 智能物联技术, 2024, 56 (05): 111-114.

[3] 周海健. 智能网络的安全检测与预警机制分析 [J]. 电子技术, 2024, 53 (08): 208-209.

[4] 袁超. 基于人工智能技术的高校智能网络安全防护系统设计 [J]. 网络安全和信息化, 2024, (08): 53-55.

[5] 廖璇,何冠锦. 人工智能在国网网络安全监测中的应用[C]// 中国电力设备管理协会. 全国绿色数智电力设备技术创新成果展示会论文集（一）. 国网中卫供电公司, 2024: 230-232.