网络安全防御中人工智能技术应用分析

何程翔　蒋宗昊*
杭州云鹭科技有限公司　浙江杭州　310000

摘　要：随着信息化社会的快速发展，计算机网络安全威胁日益加剧，传统安全防护手段已难以有效应对日益复杂的攻击模式。人工智能（AI）技术凭借其强大的数据处理能力和自我学习机制，在网络安全防御中展现出巨大潜力。AI能够通过神经网络、Agent系统、专家系统及数据挖掘等技术手段，对网络数据进行实时分析与监测，及时识别潜在威胁，有效提升系统的安全性和防御能力。此外，AI在优化防火墙、垃圾信息拦截以及网络安全监测与风险预测等方面具有显著优势，可以实现更高效的安全防护体系。本文首先分析计算机网络安全防护的现状，并阐述AI技术的基本原理和发展趋势，然后探讨AI在计算机网络安全防护中的应用模式和技术优势，最后总结AI技术在提升网络安全防护效果方面的重要作用，为构建智能化、自动化的网络安全防御体系提供参考。

关键词：计算机网络；网络安全防护；人工智能技术

序言

在大数据、云计算和物联网快速发展的背景下，计算机网络已成为社会经济运行的重要基础设施。然而，网络安全威胁与日俱增，病毒攻击、DDoS攻击、数据泄露等问题层出不穷，严重威胁着用户数据安全与企业信息资产。AI技术结合深度学习、专家系统和数据挖掘等手段，实现了对网络攻击行为的自动识别与快速响应，不仅能够及时发现潜在威胁，还能智能调整防御策略，从而显著提升网络安全防护的效率与准确性，为信息系统提供更全面的安全保障。本文围绕AI技术在计算机网络安全防护中的应用展开深入分析，首先介绍网络安全防护的基本概念与AI技术的原理，然后探讨神经网络系统、Agent系统、专家系统及数据挖掘在网络安全领域的具体应用，最后分析AI在优化防火墙系统、垃圾信息拦截和网络风险监测中的实际效果，以期为构建更完善的网络安全体系提供有益的参考。

一、计算机网络安全防护与人工智能概述

（一）计算机网络安全防护

计算机网络安全防护是指通过一系列技术和管理手段，确保计算机网络系统及其存储、处理和传输的数据免受恶意攻击、未授权访问、信息泄露和破坏等威胁[1]。网络安全防护涵盖多个层面，包括物理安全、通信安全、数据安全和应用安全等，网络攻击手段日益复杂，如DDoS攻击、恶意软件、网络钓鱼、零日漏洞利用等，使得传统安全防护措施（如防火墙、入侵检测系统等）难以满足实际需求[2]。因此，采用更加智能化、自适应性强的安全防御体系成为当前网络安全发展的重要方向。现代网络安全防护体系通常采用多层防御策略，包括基于访问控制的身份认证、加密技术保护数据传输、行为分析检测异常流量、沙箱技术隔离恶意软件，以及事件响应系统快速处置安全威胁等[3]。此外，随着云计算、物联网（IoT）和5G技术的发展，网络安全防护的边界日趋模糊，安全风险管理的挑战进一步加大。因此，如何借助先进技术提高网络安全防御能力，特别是人工智能技术的引入，已成为网络安全领域研究和实践的重要方向[4]。

（二）人工智能技术

随着计算能力的提升和数据资源的丰富，人工智能在多个领域得到了广泛应用，如医疗诊断、自动驾驶、金融风控、智能推荐系统等。在网络安全防护领域，人工智能技术的引入极大地提升了威胁检测和响应的智能化水平[5]。传统的安全防御依赖于规则匹配和特征提取，而人工智能可以基于大数据进行模式识别、异常检测和预测分析，从而有效应对未知威胁。例如，深度学习算法可以分析网络流量，识别潜在攻击行为；自然语言处

作者简介：
何程翔（1995.11-），男，汉族，浙江金华人，本科，研究方向为大数据安全、人工智能。
蒋宗昊（1993.2-），男，汉族，浙江杭州人，本科，研究方向为大数据安全、人工智能。

理技术可以用于分析网络钓鱼邮件，提高防御能力。此外，人工智能可以通过不断学习攻击模式，提升安全策略的适应性和自动化水平，使安全防护体系更加智能、高效。人工智能技术自我学习功能运行流程如图1所示。

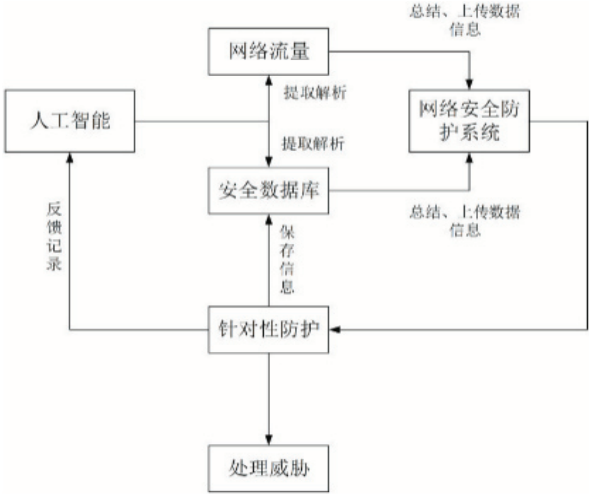

图1　人工智能技术自我学习功能运行流程

二、计算机网络安全防护中人工智能技术的应用

（一）神经网络系统应用

神经网络是一种模拟人脑神经元结构的计算模型，广泛应用于模式识别、分类和预测分析等任务。在计算机网络安全防护领域，神经网络技术主要用于异常检测、恶意代码分析和入侵检测等方面。传统的入侵检测系统（IDS）通常依赖特征匹配规则，难以有效检测未知攻击，相比传统方法，神经网络系统的优势在于自适应学习能力强，能够持续优化检测模型，提高网络安全防御的智能化水平。然而，神经网络技术在网络安全应用中也面临挑战，如训练数据的质量影响检测效果，神经网络模型容易受到对抗样本攻击等。因此，结合多种人工智能技术，提高神经网络系统的安全性和稳定性，是当前研究的重要方向。

（二）Agent系统应用

Agent系统是一种基于自主智能体（Agent）的分布式计算技术，适用于复杂环境下的智能决策与任务执行。在网络安全防护中，Agent系统可以用于实时监测、攻击溯源和自动化安全响应。Agent系统的特点是自主性、交互性和适应性，能够根据环境变化做出决策，并协调多个Agent协同工作。例如，在分布式入侵检测系统（DIDS）中，不同Agent可以分别负责不同类型的安全监测任务，如网络流量分析、文件完整性检查、用户行为分析等，然后将分析结果汇总进行综合评估。Agent技术还可以用于自动化应急响应，在检测到安全威胁后，迅速采取相应措施，如封锁可疑IP地址、隔离受感染主机等。此外，Agent系统可以结合机器学习技术，提高攻击模式识别能力，优化防御策略。当前，Agent系统在网络安全防护中的应用仍处于不断优化阶段，如何提升系统的协同工作效率、降低计算开销，是未来研究的关键方向。Agent系统运行模式如图2所示。

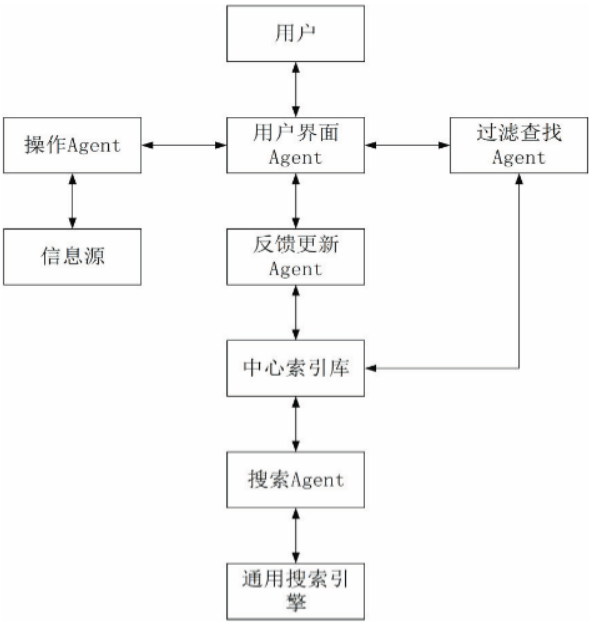

图2　Agent系统运行模式

（三）专家系统应用

专家系统（Expert System）是一种模拟人类专家决策过程的人工智能系统，通过知识库和推理引擎来分析问题并给出决策建议。在网络安全防护领域，专家系统可用于安全策略制定、威胁分析和事件响应等方面。传统安全管理依赖于人工经验，而专家系统可以自动化安全分析过程，提高响应速度。例如，在入侵检测方面，专家系统可以结合历史攻击数据和安全规则，对可疑事件进行自动诊断，判断其是否为攻击行为，并提供相应的应对措施。专家系统还可用于安全配置管理，自动推荐最佳安全策略，减少人为错误。此外，结合机器学习和大数据分析，专家系统可以不断优化自身规则，提高检测准确率。然而，专家系统的主要挑战在于知识库的构建和维护，需要持续更新以适应不断变化的网络威胁。

（四）数据挖掘技术应用

数据挖掘（Data Mining）是一种从大量数据中提取隐藏模式和有价值信息的技术，在网络安全防护中主要用于威胁检测、异常行为分析和安全预测等方面。网络安全环境中每天产生海量数据，如日志信息、流量数据、用户行为记录等，传统安全分析方法难以高效处理这些

数据。而数据挖掘技术可以基于关联分析、聚类分析和分类模型，从复杂数据中发现异常模式。例如，利用关联规则挖掘技术，可以识别攻击者的惯用手法，提前预警可能发生的攻击行为；聚类分析可以用于检测异常流量，发现潜在的安全威胁；分类模型（如决策树、随机森林等）可以自动识别恶意流量，提高检测效率。此外，数据挖掘技术可以与机器学习结合，建立智能化威胁检测系统，提高安全防护的精准度和实时性。未来，如何优化数据挖掘算法，提高其在大规模网络数据环境下的应用性能，是研究的重点方向。

三、人工智能在计算机网络安全防护中的具体应用

（一）优化防火墙系统

人工智能（AI）技术在防火墙系统的优化中发挥着关键作用，通过自学习算法和数据分析提升防火墙的检测效率和精确性。传统防火墙通常采用静态规则匹配的方式，一旦遇到未知威胁或新型攻击模式，往往难以应对，导致防御效果受限。引入AI后，防火墙可通过深度学习（Deep Learning）和支持向量机（SVM）等技术，自动学习历史攻击数据，提取攻击特征，生成动态防御策略。AI赋能的防火墙可以实时识别潜在威胁，并对异常流量进行自适应分析与过滤。结合行为分析、特征提取和异常检测机制，AI防火墙能够自动更新规则库，有效防御DDoS、SQL注入、恶意脚本等复杂攻击。此外，通过强化学习（Reinforcement Learning），防火墙系统在不断自我优化过程中，能够根据网络流量特征自动调整策略，实现更高的检测精度和防护能力，从而大幅降低网络安全风险。

（二）垃圾信息与邮件拦截

AI技术在垃圾信息和邮件拦截方面极大地提升了识别准确性和拦截效率。传统的反垃圾邮件系统主要依赖关键字匹配、黑名单和白名单机制，但面对复杂多样的新型垃圾邮件和钓鱼邮件，其过滤效果有限。通过引入自然语言处理（NLP）、深度学习（Deep Learning）和贝叶斯分类器等AI技术，系统能够自动分析邮件内容、发送者行为模式以及附件特征，准确识别垃圾信息。同时，AI模型可以通过大数据训练构建多层分类机制，有效区分正常邮件与钓鱼邮件、垃圾邮件和恶意邮件，降低误判率。AI的自学习能力还能够根据用户的反馈数据不断优化模型，提高识别精度和拦截效果。此外，AI技术结合图像识别，可以检测邮件中的隐性恶意代码或伪装链接，从而进一步增强邮件安全性。这种智能邮件过滤系统不仅能够有效阻止垃圾邮件的侵入，还能避免用户因误点钓鱼邮件导致的信息泄露和财产损失。

（三）网络安全监测与风险预测

AI技术为网络安全监测和风险预测提供了强大的支持。传统的安全监测系统主要依赖基于特征的匹配和静态规则检测，无法及时发现潜在的安全威胁。AI通过深度学习、行为分析和异常检测等技术手段，可以对海量网络流量进行实时监测，识别异常行为并预警潜在威胁。例如，基于神经网络的入侵检测系统（IDS）可以在数据流中快速识别异常模式，并通过自学习机制更新特征库，提高检测准确性。此外，AI结合大数据分析技术，通过回归分析、聚类分析和关联分析，可以深入挖掘网络日志数据，预测未来可能发生的网络攻击和潜在风险。AI还能够根据历史攻击数据、用户行为习惯以及系统漏洞分析，提前预警可能发生的威胁，并生成相应的防护策略。这种智能化的安全监测体系，极大地提升了网络安全的预防能力，帮助企业及时发现并处置安全威胁，降低网络攻击造成的损失。

结语

综上所述，人工智能技术的引入为计算机网络安全防护带来了革命性的变革。通过AI优化防火墙系统，可以实现对复杂威胁的动态防护，提高检测效率和准确率；AI赋能的垃圾信息与邮件拦截技术，极大地提升了邮件安全性，减少了信息泄露的风险；AI在网络安全监测与风险预测中，通过大数据分析和异常行为检测，有效防范了潜在攻击，提升了网络安全的防御能力。尽管AI在网络安全防护中发挥了巨大作用，但仍需面对数据隐私、算法漏洞和模型对抗攻击等挑战。因此，未来需要不断完善AI算法，强化数据治理，建立更安全、更智能的网络安全防护体系，以应对不断变化的网络安全威胁。

参考文献

[1] 边艳妮.人工智能技术运用于网络安全防护的探究[J].华东科技，2022（10）：63-65.

[2] 高义升.基于人工智能技术的计算机网络安全防护系统设计[J].网络安全和信息化，2024（4）：127-128.

[3] 高林娥.计算机网络安全管理中人工智能技术的运用[J].电子技术与软件工程，2021（1）：239-240.

[4] 刘准.计算机网络安全管理中人工智能技术的运用分析[J].电脑知识与技术，2020，16（30）：34-35.

[5] 程帅超，张冬冬.信息化时代计算机网络安全防护技术分析[J].软件，2023，44（10）：89-91.