工程管理
Journal of Project Management
第 4 卷◆第 8 期◆版本 1.0◆2023 年
文章类型：论文| 刊号（ISSN）：2737-4580(P) / 2737-4599(O)

人工智能技术在计算机网络防御中的应用

王学松
辽河油田信息工程公司
DOI：10.12238/jpm.v4i8.6164

[摘　要] 随着我国网络技术的持续发展，威胁计算机网络安全的因素也变得更加丰富，人们常见的黑客入侵以及病毒变得更加隐蔽，危害性也进一步加强。因此，计算机网络安全防御成了计算机领域备受关注的核心话题，人工智能技术作为现代信息技术发展的代表性成果，可以凭借算力、算法等方面的优势，针对计算机网络空间的安全危险因素进行全面检测以及处理。如今，人工智能技术中的神经网络、多 agent 系统以及专家系统等应用在计算机网络空间防御中逐渐得到了普及应用，集中在数据加密、智能化防火墙、智能化入侵检测以及规则产生式专家系统等方面体现其应用价值，使得计算机网络空间安全防御系统变得越发完善。
[关键词] 人工智能技术；计算机网络防御；应用

The Application of artificial intelligence technology in Computer network defense

Xue-song wang
Liaohe Oilfield Information Engineering Company

[Abstract] With the continuous development of network technology in China, the factors that threaten computer network security have become more abundant, the common hackers and viruses have become more hidden, and the harm is further strengthened. Therefore, computer network security defense has become the core topic of attention in the field of computer science. Artificial intelligence technology, as a representative achievement of the development of modern information technology, can comprehensively detect and deal with the security risk factors in computer network space with the advantages of computing power and algorithm. Today, the neural network of artificial intelligence technology, agent system and expert system application in computer network space defense gradually got popular application, focus on data encryption, intelligent firewall, intelligent intrusion detection and rules produce expert system reflects its application value, makes the computer network space security defense system becomes more perfect.
[Key words] Artificial intelligence technology; computer network defense; application

信息数据的采集、分析、处理、整合等方面都与计算机网络技术有着十分密切的联系。目前，计算机网络技术尚未做到完全发展成熟，存在众多安全漏洞，易诱发数据信息盗窃、黑客入侵等问题。随着国内计算机网络体系的持续发展，传统的安全防御工作手段无法满足现阶段网络技术发展的需求。人工智能技术作为当下信息技术的代表性成果，在自主学习、自我完善和数据智能分析处理方面具有十分明显的优势，为其在计算机网络安全防御中的普及应用提供了坚实基础。人工智能技术的智能化和自动化能为计算机网络空间防御提供全新的支持，有效改善网络空间的防御工作水平，最终营造出安全、高质量的网络环境。因此，本文通过研究分析计算机网络空间防御中的人工智能技术应用，为国内计算机网络安全防御工作的优化和调整提供参考。

1　网络安全防御概述

计算机网络空间是一种由信息技术基础设施彼此连接形成的虚拟空间，有互联网、通信网络、计算机系统以及各种嵌入式处理器等组成元素。从人工智能学科的 agent 理论看来，与人工智能的传统环境概念相比，网络空间十分独特，包括对于环境的部分感知、动态离散等内容。计算机网络安全防御是指为了避免信息计算机遭受扰乱或者摧毁行为，采取的监视、检测以及响应各种非法授权的计算机行为。计算机网络安全防御是计算机技术持续发展中的重要内容，能够及时发现并解决存在的黑客、病毒入侵等多种行为，为人们营造良好的网络安全环境，保障信息传输、存储以及贸易交易的安全性。

2　人工智能技术在计算机网络防御的应用优势

2.1 神经网络

神经网络是由简单处理元形成的大规模并行分布处理器。人工智能技术中的神经网络不仅可以实现信息的分布储存，还有着一定的容错能力，可以凭借自身较强的学习能力，进行知识的自我组织，有效满足不同层面的信息处理需求。组成神经网络的神经元计算工作有明显的独立性特征，在并行处理数据的同时，可以维护数据处理执行速度。神经网络的优势使其在计算机网络安全防御工作中进行模式识别、分类以及有效选择应对攻击事件的手段。从目前我国人工智能的神经网络技术发展来看，网络空间防御工作中的入侵检测领域呈现出优秀的使用价值，可以分为蠕虫检测、垃圾邮件检测和僵尸检测等。相关人员以计算机行为测量为出发点，综合使用神经网络技术对常见的蠕虫病毒进行检测。与决策树分类检测技术相比，神经网络的入侵检测技术在检测效率方面具有明显优势，能够识别出蠕虫病毒变种。因为部分神经网络系统中图形处理器或者硬件为基础组成，使得数据处理速度提升十分明显，可以逐渐在网络空间安全防范领域中普及。

2.2 多 agent 系统

在我国分布式人工智能技术持续发展的过程中，agent 作为代表性技术成果，某种程度上可以被视为自动执行的实体，利用现代传感器对外界环境进行感知，利用效应器对环境施加作用。在人工智能的多 agent 系统持续发展过程中，计算机网络空间安全防御工作也开始引入这一技术，考虑到该项技术在环境感知和规划能力方面的优势十分明显，一般会在网络安全防御工作中的网络态势感知、入侵检测等环节应用。虽然全球范围内的互联网技术正在逐渐发展成熟，但是依旧存在明显的系统漏洞，是分布式网络攻击频繁出现的主要原因，即利用各种自动化方法同时攻击多个网络服务系统，因为此系统并非由独立的机构或者个人管理，对于攻击信息进行鉴别的系统会在多个系统中分散分布。对于单独系统的安全管理人员而言，要想有效处理分布式网络攻击，需要与其他系统的管理人员保持全方位的沟通，来获得网络安全的全部状态信息，但实现难度较大。

2.3 专家系统

在人工智能技术持续发展的过程中，专家系统是发展时间最早、发展最为成熟的技术成果，具体组成部分为知识库和推理机构。专家系统是由不同领域专家提供特殊领域知识，经过计算机系统自主推理后，模拟专家思维形成决策，提出解决方案的系统。不同领域专家的知识都是以规则作为出发点形成的，要想提高专家系统的处理效率，还需要专家为系统提供高质量的行业知识。由网络安全专家提供的知识和经验建立的专家系统，可以在计算机网络安全防御决策中发挥重要作用，或为相关人员开发自动化的网络防御系统提供支持。

2.4 智能算法

在计算机网络安全防御工作中，人工智能技术的明显优势之一就是智能算法的高效优势，主要体现在非具体信息的处理以及智能学习、推理能力方面。模糊信息算法是人工智能技术应用较为普遍的算法，在非具体定义、非安全路径数据信息分析中有着明显的应用价值，不仅能够规避之前计算机网络在数据格式方面的固定要求，也能有效缓解单一化网络来源分析问题带来的数据错误处理现象。在网络系统的使用过程中，计算机用户通常会遭遇各种来历不明的病毒或者入侵行为的干扰，普通用户因为专业知识有限，导致无法及时察觉到网络病毒入侵行为。人工智能中的模糊信息算法可以有效区分网络信息的来源途径，对于未知来源的恶意网络入侵能够进行全方位模糊信息推理，对其内容进行详细分析，以精确分析结果选择网络安全防御工作手段。

3 计算机网络防御中的人工智能技术应用分析

3.1 数据加密

相较于传统网络安全防御技术，人工智能有着明显的特异性特征，可以通过持续的学习，积累、记忆网络安全数据。技术人员针对不同路径和来源的数据设立对应的人工智能网络参数，保证人工智能技术全面发挥其记忆和学习能力，储存具备较高威胁性的网络病毒及其攻击特征。计算机网络安全防御系统可以不断积累各种经验，持续提高防御能力。在面对相同的入侵攻击行为或病毒入侵行为时，能够根据工作经验及时作出反应，使用数据库中积累的处理手段第一时间进行处理。在人工智能技术的模糊算法加持下，计算机网络空间安全防御系统能够针对多种数据持续简化处理流程，使得人工智能技术和计算机网络安全能够做到完美兼容。

3.2 智能化防火墙

目前威胁计算机网络安全的核心问题之一就是高级威胁攻击，之所以攻击威胁带有高级性，是因为不法分子对于攻击技术的掌控能力逐渐提高，预算相对充足，攻击人员一般会使用多种方式、技术生成针对性的攻击工具，在计算机网络攻击过程中，可对各项工具方式和技术的组合不断进行调整。在高级威胁攻击的影响下，在计算机网络安全防御中应用人工智能技术可以针对 APT 攻击的各个环节进行突破，在任意一个环节识别出风险因素之后可以切断整个攻击链条。以人工智能技术为基础形成的层次化防御解决方案是利用多种层次流量管控以及威胁防护手段封堵连续攻击环节中的关键节点。层次化安全防御体系不仅拥有最为传统的被动检测能力，还能够使用各种高级技术方法检测未知恶意软件以及加密变形。人工智能技术能够全方位收集木马病毒、恶意软件和隐藏风险文件夹等网络风险因素，与特征库中储存的数据进行对比和记忆，持续对病毒特征库进行更新。在传统的防火墙检测技术无法检测异常文件的前提下，智能化防火墙技术可以进行深层次的检查，保障进入计算机网络系统内部的各项文件完全安全。

3.3 规则生产式专家系统

专家系统是目前计算机网络安全防御系统中应用较为普遍的人工智能技术，该系统是以各专业领域人士提供的工作经验作为前提条件建立的，能在使用的过程中有效防御外界的非法入侵行为。系统管理人员可以根据已有的外来信息和数据特

征编码进行总结，根据入侵计算机网络的内部信息以及频率分析入侵规律，针对系统的安全网络防御工作建立智能化系统。系统根据专家提供的相关建议针对可疑入侵行为进行全方位检测，按照数据库中的相关方法做出应对。随着人工智能技术的引入和应用，专业人员只需要经过一次编程工作便能够形成完善的计算机网络安全防御系统，人力资源投入量明显下降，规则产生式专家系统的建设能够在持续应用中由系统针对信息和可疑病毒全方位进行检测，保障系统运行。

3.4 智能化入侵检测

目前计算机网络的使用人员都会安装专业的网络防御软件，在经济社会持续发展的影响下，人工智能技术在网络防御软件中基本普及。从技术层面看来，入侵检测技术能够持续拓宽人工智能技术的适用范围，在人工智能技术和入侵检测技术有效融合的情况下，可以针对网络信息进行全方位检测，由系统自主进行网络信息分析，抵御外来不良信息的干扰，同时对各种病毒实时监控，强化系统的防护工作力度，有效规避外来入侵事件以及计算机病毒。入侵检测技术和人工智能技术的融合发展是在全方位发挥人工智能技术算力、算法优势前提下，减少网络空间安全防御中的人力资源投入，提高防御工作的质量和效率。

4 总结

综上所述，随着计算机技术和网络技术的不断发展，计算机网络已经遍布各个领域，并在人们的生活中发挥着重要作用，但因计算机系统发展不够完善，会频繁出现一些网络安全问题，在此背景下，人们更加关注计算机的网络安全防御措施，而以人工智能为代表的现代技术成果，也得以广泛应用在计算机网络防御中。基于此，本文首先对计算机网络安全防御进行简单介绍，然后对人工智能技术在计算机网络防御中的应用优势进行了研究。最后结合数据加密、智能化防火墙、规则生产式专家系统以及智能化入侵检测等手段，分析人工智能技术在计算机网络防御中的应用。

[参考文献]

[1]张力影.人工智能技术在计算机网络运维中的应用[J].无线互联科技,2023,20(06):26-28.

[2]刘婉婉.人工智能在计算机网络技术中的应用探究[J].网络安全技术与应用,2022(03):23-24.

[3]耿杨.人工智能技术在大数据网络安全防御机制中的应用研究[J].数据,2022(01):48-50.

[4]张智.人工智能技术在大数据网络安全防御中的应用[J].无线互联科技,2021,18(11):95-96.