 DOI: https://doi.org/10.12349/iser.v5i5.2511

Application and Challenge of Artificial Intelligence in the Field of Network Security

Zhaoyang Zhu

International Institute of Engineering Psychology, Colorado, America

Abstract

With the rapid development of science and technology and the wide application of information technology, artificial intelligence (AI) has gradually emerged and become an indispensable tool in the field of network security. The rise of AI technology has not only changed the protection mode of traditional network security, but also significantly improved the protection capability of network security. AI technology is widely and deeply applied in the field of network security. However, with the widespread application of AI in network security, there are also many challenges. In order to address these challenges, this article will take an in-depth look at the application of AI in the field of cybersecurity and the challenges it faces, analyze existing technologies, assess their strengths and weaknesses, and look at future trends. Through continuous research and practice, we will further play the role of AI technology in the field of network security.

Keywords

AI; network security; apply; challenge

人工智能在网络安全领域的应用与挑战

朱朝阳

国际工程心理学研究所，美国 · 科罗拉多州

摘　要

随着科技的飞速发展和信息技术的广泛应用，人工智能（AI）逐渐崭露头角，成为网络安全领域不可或缺的重要工具。AI技术的崛起不仅改变了传统网络安全的防护模式，而且显著提高了网络安全的防护能力。AI技术在网络安全领域的应用广泛而深入。然而，随着AI在网络安全中的广泛应用，也面临着诸多挑战。为了应对这些挑战，论文对AI在网络安全领域的应用及其面临的挑战进行深入探讨，分析现有技术，评估其优缺点，并展望未来发展趋势。通过不断的研究和实践，进一步发挥AI技术在网络安全领域的作用。

关键词

人工智能；网络安全；应用；挑战

1 引言

网络安全作为保障信息社会健康发展的重要基石，一直是全球关注的焦点。随着网络技术的飞速发展和攻击手段的不断演变，传统的网络安全技术已难以满足日益复杂的安全需求。而人工智能（AI）作为一项前沿技术，为网络安全领域带来了新的机遇和挑战。AI 技术以其强大的数据处理能力和自学习能力，在网络安全领域展现出巨大的应用潜力。

2 人工智能技术的特点和优势

2.1 计算成本低

传统的网络安全技术运算程序确实复杂，导致能源消耗巨大，超出常规想象。相对而言，人工智能技术采用的控制算法为网络安全领域带来了革命性的改变。这种算法简洁高效，通过预先寻找最优解，一次性完成运算任务，不仅大幅减少了人工参与和资源消耗，还极大地提高了任务完成的速度和效率。

2.2 具有一定的学习能力

工智能技术在网络安全领域的应用，除了具备学习能力和计算成本低的优势外，还有处理模糊信息的能力。随着互联网的高速发展，出现了许多未知问题，这些问题往往具有模糊不确定的特点，给人们带来各种风险。人们有时会对这些问题或信息感到反感，因为处理它们很困难，稍有不慎就可能陷入风险中。人工智能技术的出现有效地应对了这些挑战。与传统网络安全技术相比，人工智能采用了模糊逻辑的推理方式，能够感知网络中存在的风险，并对未知问题进行筛选、整理，从而提高网络安全维护工作的效率 [1]。

【作者简介】朱朝阳（1995–），男，中国河南驻马店人，博士，研究员，从事人工智能研究。

2.3 具有处理模糊信息的能力

人工智能技术除了具备学习能力和计算成本低的优势外，还拥有处理模糊信息的能力。在互联网高速发展的今天，出现了很多人们不确定或者是不知道的问题，即未知问题。这些模糊又不确定的网络信息具有相当多的可能性，这一点也就表明了这些问题的出现将会带给人们各种各样的风险。当人们看到这些问题或者是信息时，心里有时候是非常反感的，因为这些信息或数据处理起来是非常困难的，稍有不慎，就会陷入风险之中。模糊信息的大量涌现，对于网络风险的预防，将会是非常大的一项挑战 [2]。

3 人工智能在网络安全领域的应用

3.1 身份认证识别

人工智能在网络安全领域中的身份认证识别方面有着广泛的应用。随着技术的发展，人们对身份验证的安全性要求越来越高，推动了身份验证技术的不断创新。在这一背景下，人工智能发挥了重要的作用。

人工智能可以通过多种方式进行身份认证识别，如面部识别、虹膜识别、声纹识别等。这些技术都是基于生物特征识别，通过对人体生理和行为特征进行检测和识别，实现身份验证的功能。例如，面部识别技术可以通过深度学习对面部图像进行学习和训练，从面部轮廓、亮度、角度等方面对人脸进行准确识别，并与系统中保存的人脸信息进行比对，从而实现身份验证。虹膜识别技术则通过分析虹膜纹理来进行身份验证，具有高度准确性。声纹识别技术则是通过语音信号中鲜明的个体差异对个人身份进行识别。

3.2 恶意域名检测

不法分子经常利用恶意域名进行非法活动，如诈骗、色情传播、网络钓鱼或非法网站运营等。以往，人们主要依赖基于特征的黑名单技术来识别这些恶意域名。但随着技术的不断发展和犯罪手法的日益复杂，尤其是恶意软件的出现，使得这种方法变得越来越无效。因为恶意软件能自动生成大量的域名，使得恶意域名的数量持续激增，并且不断变化和进化。为了应对这一挑战，深度学习中的循环神经网络（RNN）技术应运而生。这种网络能够区分由人类手工编写的正常域名和由恶意软件生成的域名。因为恶意软件生成的域名在结构上往往呈现出一些特定的模式，如元音和辅音字母的比例可能不太自然，或者频繁出现大小写字母与数字的混合组合。这些特征使得 RNN 可以相对容易地识别和区分这些域名 [3]。

3.3 流量攻击检测

人工智能在网络安全领域的流量攻击检测方面有着广泛的应用。传统的网络安全系统主要依赖于规则和模式匹配来检测网络攻击，但这种方法在面对新型攻击行为时往往显得力不从心。而人工智能技术，特别是机器学习，能够学习并理解网络的正常行为模式，使其能够更快速地检测到异常的网络流量。

具体来说，基于机器学习的流量攻击检测可以通过分析网络流量的统计特征，建立模型来检测异常行为。例如，通过对网络流量的实时监测，机器学习算法可以识别出与正常流量模式不符的异常流量，如突然增加的流量、来自未知源的流量或者具有特定特征的流量等。这些异常流量可能预示着潜在的网络攻击，如 DDoS 攻击、网络钓鱼等。此外，人工智能技术还可以应用于威胁情报分析。网络攻击往往具有高度变异性和复杂性，传统的威胁情报分析方法往往难以从庞大的数据中识别出有用的信息。而基于人工智能的威胁情报分析可以自动对大量的网络流量数据进行筛选和关联分析，从而提取出潜在的威胁情报。

3.4 恶意软件识别

恶意软件的出现，给国家、企业和个人带来了严重的经济损失。尽管常规的防御措施能起到一定的遏制作用，但其自身的变异与演化却使传统的防御措施很难有效地应对。与此形成鲜明对比的是，有指导的学习方法可以从海量样本中挖掘出恶意代码与恶意代码的特性，从而更加高效地对恶意代码进行识别与防御。该方法既能对已知的恶意程序进行检测，又能通过对其行为模式的分析，对其可能的变化进行预测，进而对新的攻击进行预防。马尔可夫模型、长短期记忆网络 LSTM、自动编码器 AE、生成对抗网络 GANs 以及大规模语言模型 LLMs 等人工智能技术可以作为自动生成邮件的有效工具。对于 Transformer、BERT、GPT 生成式大模型来说，制造钓鱼邮件和垃圾邮件的成本很低，只需给出关键提示词，这些模型就可以在秒级内生成大量逼真、切题的鱼叉式钓鱼邮件和垃圾邮件，继而成为钓鱼攻击和拒绝服务攻击的跳板。该技术可以在最短的时间内将受病毒计算机与整个网络隔离开来，并有效地阻断了病毒的扩散，极大地减少了病毒对网络的危害。

3.5 垃圾邮件检测

随着互联网的迅速发展与智慧型通讯设备的广泛使用，电邮已经逐渐成为人们生活中不可缺少的一种工具。但同时，这也成为了垃圾信息泛滥的温床。传统的垃圾信息检测技术以文字串匹配、地址黑名单等为手段，无法有效应对新的垃圾信息。与恶意程序识别相似，大量样本库可为深层神经网络的训练提供充足的资源。随着用户和服务商的持续报道，这两个数据库也在不断地增加。深层神经网路不但可以侦测到讯息的源头，更可以对其中有无价值或恶意的讯息进行分析与判断，将卷积神经网络与循环神经网络相结合，能够大幅提升识别精度，为更高效地处理垃圾信息提供理论支撑。

3.6 异常检测

网络防护系统的优化，关键是它是否能够及时识别和及时处理异常状况。网络状态是一个不断变化的动态过程，其呈现方式也是多种多样的。该方法不仅可以有效地识别外

界的攻击，还可以探测到内部的违规行为，对网络安全具有重要的意义。异常行为通常包含了大量的数据流，并且包含了大量的操作，如文件存取的频繁、数据的异常转移等，如何对其进行有效的提取与表示，是图像识别中的一个重要难题。近几年，非监督学习被广泛用于异常检测。其中，降维可以有效地对数据进行降维处理，去除冗余，提升辨识精度，更好地挖掘数据的本质特性 [4]。

4 人工智能技术在网络安全管理中的挑战与对策

4.1 数据质量和隐私保护

4.1.1 数据质量

人工智能技术对海量、海量、高质量的数据需求。但是，如何获得高质量的有标签的数据，一直是网络安全研究中的一个难题。这是由于来自网络的攻击与威胁的资料往往是有限的，而且还会含有诸如错误标记或离群的噪音。这些噪音会使模型的性能变差。针对这一问题，可以通过对样本进行异常检测，并对其进行预处理。另外，网络中还经常出现信息缺失和不完全等问题。这会造成训练模型不精确或者不能有效地处理新的威胁。为了解决这个问题，可以利用数据清洗技术，以及填充缺失值的技术，来完善数据集，从而提高模型的性能。

4.1.2 隐私保护

在网络安全管理的过程中，由于会涉及许多敏感数据，如用户的身份信息、IP 地址、网络流量数据等，因此在利用人工智能技术进行数据分析和处理时，用户的隐私保护显得尤为重要。为了确保用户的隐私权益，需要采取一系列的策略和措施。一方面，数据脱敏。数据脱敏可以通过修改原始数据的方式来保护用户的隐私，使得未经授权的人员无法获取到真实的信息。另一方面，加密匿名化也是一种常用的手段，通过将数据进行加密和匿名化处理，可以有效防止数据泄露和滥用。

4.2 对抗性攻击和对抗性学习

在对抗性攻击中，攻击者可以通过改变输入数据或者增加噪音等方式，使模型产生错误的结果。针对这一问题，研究者们正致力于建立一种新的对抗样本产生方法，并设计相应的防御措施。然而，攻击者可以使用微小的，不易察觉的攻击来躲避已有的侦测与防御。为此，可以通过提高算法的鲁棒性，并将行为分析与异常检测相结合，以更好地处理对抗性攻击。由于对抗攻击中所使用的样本数量较少，导致在训练过程中存在大量对抗样本不足的问题。针对这一难题，研究者们开始研究如何利用人工数据产生与迁移学习来提高对抗样本的种类与数量。本项目的研究成果将有助于提升模型的健壮性，增强对抗攻击的能力。

4.3 可解释性和可信度问题

可解释性是指人工智能算法在做决策时，其决策逻辑和依据能够被人类所理解和解释。在网络安全领域，这些算法通常基于大量数据学习和决策，但其内部逻辑和过程常常像是一个“黑盒子”，让人难以捉摸，这就给网络安全管理带来了挑战，因为安全专家需要明白算法是如何得出结论的，这样才能验证其决策的准确性和可靠性。同时，可信度也是人工智能算法在网络安全管理中需要考虑的重要因素。这意味着算法的决策结果应该是值得信赖的。但在实际应用中，由于历史数据可能存在噪声、偏差，甚至可能受到恶意攻击的影响，这些都可能降低算法的决策准确性，从而影响其可信度。

为了应对这些挑战，可以考虑以下几种策略：①选择那些解释性较好的算法，如决策树或规则集等。这类算法可以为提供关于其决策过程的更多信息，使得可以更清楚地了解它们是如何得出结论的。②可以通过构建可解释性模型来优化算法的输出。这意味着将算法的决策结果转化为更直观、更易于理解的形式，如规则或图形。这样一来，安全专家就能更容易地理解并验证算法的决策过程。③开发一种能够评估算法决策结果的可信度评估方法也至关重要。这种评估方法将为提供关于算法决策结果准确性的反馈，从而确保算法在实际应用中的可信度。

5 结语

综上所述，人工智能为网络安全领域带来了巨大的机遇与挑战。其广泛的应用，如入侵检测、恶意软件分析、数据泄露预防、风险评估和自动化响应等，不仅提高了安全性的实时性和准确性，还降低了人为错误的风险。此外，随着技术的发展，新型的攻击方式和漏洞也在不断地出现，这对于人工智能模型的适应性和更新速度提出了更高的要求。如何在不断变化的威胁环境下保持技术的先进性和实时性，是我们必须克服的难题。

参考文献

[1] 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.

[2] 茹素岩.网络社会安全视角下人工智能活动特征、风险及公共政策选择[J].广州社会主义学院学报,2024(1):110-116.

[3] 苏德悦.“人工智能+”时代开启,怎么守护安全?[N].人民邮电,2024-03-18(003).

[4] 李乔宇.借助AI加速网络安全技术创新[N].证券日报,2024-03-09(A04).