文章类型：论文|刊号（ISSN）：2972-4236(P) / 2972-4244(O)

人工智能下网络安全威胁智能识别与防御技术

杨天胜
DOI:10.12238/acair.v2i2.7363

[摘　要] 随着互联网的发展,网络安全威胁的类型和复杂性不断增加,这就需要网络安全防御技术具有更高的智能性,以应对当前不断变化的网络安全威胁。因此,基于人工智能的网络安全威胁智能识别与防御技术是当前网络安全领域的一个研究热点。本文首先概述了人工智能在网络安全领域的应用,然后详细分析了基于人工智能的威胁智能识别技术,包括其基本原理和各种方法。接着,介绍了基于人工智能的网络安全防御技术,包括入侵检测与防御系统、恶意软件分析与处置技术以及漏洞挖掘与修复技术。
[关键词] 人工智能；网络安全；威胁识别；防御技术
中图分类号：TN915.08　文献标识码：A

Intelligent Identification and Defense Technology of Network Security Threats under Artificial Intelligence

Tiansheng Yang

[Abstract] With the development of the Internet, the types and complexity of network security threats are increasing, which requires higher intelligence of network security defense technology to cope with the changing network security threats. Therefore, the intelligent identification and defense technology of network security threat based on artificial intelligence is a hot research topic in the field of network security. In this paper, the application of artificial intelligence in the field of network security is summarized, and then the threat identification technology based on artificial intelligence is analyzed in detail. Then, it introduces the network security defense technology based on artificial intelligence, including intrusion detection and defense system, malware analysis and disposal technology, and vulnerability mining and repair technology.
[Key words] artificial intelligence; network security; threat identification; defense technology

引言

随着互联网的发展,网络安全已成为影响国家安全的重要因素之一,同时也是一个国家网络基础设施建设中的核心问题。随着信息技术在经济和社会生活中的广泛应用,网络安全威胁也越来越多样化、复杂化,同时也日益呈现出新的趋势。目前,国内外大部分学者都在致力于网络安全技术的研究,如信息获取、恶意代码检测、入侵检测和漏洞挖掘与修复等。传统的网络安全技术主要是基于网络攻击的分析和防护,通过对入侵行为进行检测和阻断来达到防护目的,随着人工智能技术的不断发展,基于人工智能的威胁智能识别与防御技术也在不断发展和完善。

1 人工智能在网络安全中的应用概述

人工智能(AI)是指通过计算机算法模拟人类智能行为的一种技术。它涵盖了多个学科领域,如机器学习、深度学习、自然语言处理、专家系统等。AI的主要特点包括自我学习、自我适应、自我优化和决策能力等,这些特点使得AI在网络安全领域具有广阔的应用前景。

2 基于人工智能的威胁智能识别技术

2.1威胁智能识别技术的基本原理

威胁智能识别技术是基于AI技术的一种网络安全防护方法。它通过对网络流量、日志文件、系统行为等数据进行分析,利用机器学习算法构建威胁模型,实现对网络威胁的智能识别。威胁智能识别技术主要分为三个模块,分别是威胁识别模块、威胁分析模块和威胁防御模块。其中,威胁识别模块将收集到的网络数据进行特征提取、数据预处理,将数据进行分类和聚类处理,形成可用于分析的特征向量；威胁分析模块对提取到的特征向量进行威胁分析,利用机器学习算法构建模型,输出结果；威胁防御模块通过对模型输出结果的分析,构建网络安全防护体系,从而实现对网络安全威胁的智能识别和防御。在整个过程中,机器学习算法是整个体系的核心内容。在构建模型时,一般采用机器学习算法,常见的机器学习算法有支持向量机(SVM)、决策树和神经网络等。

2.2基于深度学习的威胁智能识别方法

基于深度学习的威胁智能识别方法是近年来研究的热点之

一。深度学习是机器学习的一个分支,它利用神经网络模型模拟人脑神经元的工作方式,通过对大量数据进行学习,实现对复杂数据的特征提取和分类。在网络安全领域,深度学习模型可以通过对网络流量、恶意软件、漏洞等数据的训练,学习到威胁的特征和模式,从而实现对网络安全威胁的智能识别。

具体而言,基于深度学习的威胁智能识别方法可以分为以下几个步骤：首先,收集大量的网络安全数据,包括网络流量、日志文件、恶意软件样本等；然后,利用深度学习算法构建威胁识别模型,对收集的数据进行训练,使模型能够学习到威胁的特征和模式；最后,将训练好的模型应用于实际网络环境中,对网络流量进行实时监测和分析,实现对网络安全威胁的智能识别。

威胁识别方法主要是基于深度学习算法的,由于深度学习模型能够在大规模复杂的数据中自动提取特征,并对这些特征进行分类和决策,因此得到了广泛的关注和研究。基于深度学习的威胁智能识别方法可以分为两类,一类是基于卷积神经网络(Convolutional Neural Network,CNN)模型的威胁识别方法,其中 CNN模型包括多个卷积层和池化层,它们通过卷积操作自动提取特征并进行分类；另一类是基于循环神经网络(Recurrent Neural Network,RNN)模型的威胁识别方法,其中RNN模型可以自适应地处理输入序列中的长期依赖关系。

2.3基于自然语言处理的威胁智能识别方法

随着网络攻击的不断演变,攻击者越来越多地利用自然语言进行伪装和欺骗,如钓鱼邮件、恶意网站等。因此,利用NLP技术对网络安全威胁进行智能识别也具有重要意义。基于NLP的威胁智能识别方法主要通过对网络中的文本信息进行语义分析和情感分析,提取出与威胁相关的关键词和特征,从而实现对网络安全威胁的识别。具体而言,NLP技术可以通过对邮件正文、网站内容、社交媒体帖子等文本信息的分析,检测出其中的威胁信息,如恶意链接、钓鱼邮件等,从而提醒用户及时采取防护措施。

对于网络安全威胁,通常情况下,网络攻击者会使用多种方法来伪装自己的身份,如利用假名、英文字母以及数字等进行伪装,并通过网络爬虫、邮件扫描、钓鱼邮件等方式获取用户的邮件和网站地址。为了提高威胁智能识别的准确性,可以通过以下几种方式:一是对网络安全威胁进行语义分析,提取出与威胁相关的关键词;二是利用情感分析技术对文本信息进行情感分析,如利用情感词典计算文本情感倾向；三是利用机器学习算法对文本信息进行分类,从而识别出网络安全威胁类型。

3 基于人工智能的网络安全防御技术

3.1防御技术的基本原理

基于人工智能的网络安全防御技术主要是利用AI技术对网络攻击进行自动检测和防御。其基本原理包括以下几个步骤：

首先,收集并分析网络流量数据。AI系统可以通过对网络流量的实时监控,获取大量的网络数据,包括数据包、IP地址、端口号等信息。然后,利用机器学习算法对这些数据进行分析,识别出异常流量和潜在的网络攻击。

其次,构建网络安全模型。AI系统可以根据历史攻击数据和网络安全知识库,构建出网络安全模型,用于预测和防御未来的网络攻击。这些模型可以通过不断学习和更新,提高自身的防御能力。

最后,自动响应和防御。当AI系统检测到网络攻击时,可以自动触发防御机制,如阻断攻击源、隔离被攻击主机、发送告警信息等,从而实现对网络攻击的快速响应和有效防御。基于人工智能的网络安全防御技术通过对网络攻击进行自动检测和防御,有效减少了传统网络安全防御技术的人力投入和设备维护成本,提高了网络安全防御效率,在未来具有广阔的应用前景。

3.2入侵检测与防御系统

在现代网络安全领域,入侵检测与防御系统(IDS/IPS)扮演着至关重要的角色。然而,随着网络攻击手段的不断演进和复杂化,传统的IDS/IPS系统已经难以满足现代网络安全的需求。因此,基于人工智能(AI)的IDS/IPS逐渐成为了网络安全领域的研究热点。

传统的IDS/IPS主要依赖于规则匹配和签名识别等方法来检测和防御网络攻击。这种方法在过去的一段时间内取得了一定的效果,但随着网络攻击技术的快速发展,攻击者开始采用更加隐蔽、复杂的攻击手段,如零日漏洞、多态攻击等,使得传统的IDS/IPS难以有效应对。

为了应对这一挑战,基于AI的IDS/IPS应运而生。这类系统利用机器学习、深度学习等算法,能够对网络流量进行实时监测和分析,从而实现对网络攻击的自动识别和防御。与传统方法相比,基于AI的IDS/IPS具有更高的灵活性和适应性,能够更有效地应对不断变化的网络攻击手段。

基于AI的IDS/IPS的核心在于其强大的学习和优化能力。通过自适应学习机制,这类系统能够不断学习和优化防御策略,提高防御效率和准确性。例如,基于深度学习的IDS/IPS可以通过分析大量的网络流量数据,自动提取出攻击行为的特征,进而构建出高效的攻击检测模型。同时,这类系统还能够根据攻击行为的变化,不断调整和优化防御策略,从而保持对攻击的持续有效防御。

除了具有更高的防御效率和准确性外,基于AI的IDS/IPS还具有更低的误报率和漏报率。传统的IDS/IPS往往因为规则匹配和签名识别的局限性,导致大量的误报和漏报。而基于AI的IDS/IPS则能够通过自学习和自调整,逐步降低误报率和漏报率,提高系统的整体性能。

3.3恶意软件分析与处置技术

随着信息技术的迅猛发展,网络安全问题日益凸显。其中,恶意软件作为网络攻击的主要工具之一,对个人、企业乃至国家的信息安全构成了严重威胁。为了有效应对这一挑战,基于人工智能的恶意软件分析与处置技术应运而生,成为网络安全领域的研究热点。

恶意软件,通常是指那些未经授权而擅自安装在用户计算机上,并可能损害用户数据、窃取信息、破坏系统或网络服务的

软件。它们通常以伪装成正常软件的形式出现，诱导用户下载并执行，从而实现其非法目的。因此，快速、准确地识别、分析和处置恶意软件，对于维护网络安全至关重要。

基于人工智能的恶意软件分析与处置技术，主要利用深度学习、自然语言处理等技术手段，对恶意软件进行快速识别、分析和处置。这些技术通过对恶意软件的静态和动态特征进行提取和分析，实现对恶意软件的快速检测和分类。静态特征主要包括恶意软件的代码结构、文件属性等，而动态特征则关注恶意软件在运行过程中的行为表现。

具体而言，深度学习技术可以通过构建神经网络模型，对恶意软件的静态和动态特征进行学习和分类。这些模型能够自动提取恶意软件的特征，并将其与已知恶意软件库进行比对，从而实现对恶意软件的快速识别。自然语言处理技术则主要针对恶意软件的文本信息进行分析，如恶意软件的命名、描述等，从而揭示其潜在的行为模式和意图。

除了快速识别恶意软件外，基于人工智能的恶意软件分析与处置技术还能够对恶意软件的行为进行实时监测和阻断。通过行为分析等技术手段，这些技术能够实时监测恶意软件在系统中的活动，并在发现异常行为时及时采取阻断措施，从而有效防止恶意软件对系统的破坏和攻击。

在实际应用中，基于人工智能的恶意软件分析与处置技术已经取得了显著的成效。例如，一些先进的恶意软件检测工具，如人工智能驱动的沙箱技术，能够在隔离环境中模拟恶意软件的运行，从而更准确地评估其潜在风险。此外，一些深度学习模型在恶意软件分类和识别方面表现出了极高的准确率和效率，为网络安全人员提供了有力的支持。

然而，尽管基于人工智能的恶意软件分析与处置技术取得了显著的进展，但仍面临着一些挑战和限制。例如，随着恶意软件技术的不断发展，其隐蔽性和复杂性也在不断提高，给检测和处置工作带来了更大的难度。此外，恶意软件作者可能会利用人工智能技术来生成更难以检测的变种和进化版本，从而增加了网络安全的风险。

3.4漏洞挖掘与修复技术

在数字时代的浪潮中，网络安全问题日益凸显，成为企业和个人关注的焦点。漏洞，作为网络安全中的薄弱环节，是攻击者窥视和入侵的潜在通道。漏洞挖掘与修复技术的核心在于其强大的数据处理和分析能力。通过机器学习技术，系统可以自动地从海量的网络数据中筛选出与漏洞相关的异常信息。深度学习技术则进一步提升了这一过程的精确度和效率，使得系统能够更快速、更准确地识别出潜在的漏洞。这些技术的结合，使得漏洞挖掘不再是一项繁琐而耗时的任务，而是一项高效而精准的工作。

除了快速识别和挖掘漏洞，这些基于人工智能的技术还具备自动化修复机制。一旦发现漏洞，系统可以自动地生成修复方案，并对系统进行加固，从而有效防止攻击者的入侵。这种自动化的修复机制大大提高了系统的安全性和稳定性，减少了人为干预的需要，降低了安全事件的发生概率。

然而，虽然基于人工智能的漏洞挖掘与修复技术具有诸多优势，但我们也应清醒地认识到，它并非万能的解决方案。随着攻击手段的不断进化，我们需要不断更新和完善这些技术，以适应日益复杂多变的网络安全环境。

4 结束语

基于人工智能的网络安全威胁智能识别与防御技术是网络安全领域的重要研究方向。随着人工智能技术的不断发展和完善，这些技术将在网络安全领域发挥越来越重要的作用。未来，技术研发者将需要继续深入研究这些技术，提高网络安全防护能力，为保障国家网络安全做出更大的贡献。

[参考文献]

[1]王明,孙志文,杨海燕.人工智能对网络安全的威胁与应对[J].网络安全技术与应用,2024,(01):163-165.

[2]丁宝星.基于人工智能的网络入侵检测与防御研究[J].中国信息化,2023,(11):76-78.

[3]贾珺.人工智能技术在大数据网络安全防御中的运用研究[J].天津职业院校联合学报,2023,25(09):31-35+54.

[4]张鑫鑫.人工智能在网络安全中的应用[J].无线互联科技,2023,20(06):29-35.

[5]刘静,蔡萌萌,陈晓.人工智能背景下网络安全的攻击威胁和应对策略[J].网络安全技术与应用,2023,(03):155-156.