基于深度学习的网络安全威胁智能识别与防御研究

王永建　武世杰
河北方维网络技术有限公司　河北　石家庄　050000

摘　要：在信息技术飞速发展的今天，网络安全威胁智能化、隐蔽化给传统防护手段提出了挑战。文章就深度学习技术应用于网络安全领域进行讨论，目的在于为智能识别和防御提供一种全新的方案。首先对深度学习技术产生的背景，基本原理以及其在网络安全方面的应用状况进行综述，并对其优势和面临的挑战进行剖析。然后对基于深度学习的网络安全威胁识别技术进行了系统的研究，主要包括恶意软件识别，网络入侵识别以及网络钓鱼识别等。进一步提出基于深度学习的网络安全威胁防御策略主要包括态势感知，预警和响应技术。最后总结研究成果并展望未来研究方向，同时指出深度学习技术应用于网络安全领域中的潜力与挑战。

关键词：深度学习；网络安全；威胁识别；威胁防御；智能技术

引言

信息技术的快速发展导致网络环境复杂性加大，随之而来的是网络安全威胁越来越严重。网络攻击手段智能化、隐蔽化使传统安全防护措施受到了空前挑战。基于这一背景，深度学习技术以其在图像识别和自然语言处理方面的优异性能为智能识别和防御网络安全威胁提供了一种全新的角度与解决方案。文章将对深度学习技术应用于网络安全领域进行深入探究，分析该技术在网络安全威胁智能识别及防御方面所具有的优势及面临的挑战，进而提出相关研究思路及方法。

1 深度学习技术概述

1.1 深度学习技术的发展背景与基本原理

深度学习技术最早可以追溯到上世纪40年代，但是一直到本世纪初随着计算能力不断增强以及大数据不断累积，深度学习才能迎来迅猛发展。深度学习以构造一个多层结构神经网络为核心，模拟人脑进行信息处理的模式，从而达到高效学习数据并提取特征的目的。该技术的开发为复杂问题的解决提供了一种全新的思路。[1]

深度学习技术产生有很多背景。一是随着互联网普及、信息技术发展，数据量呈爆炸式上升，给深度学习带来大量训练数据。二是计算硬件和软件的改进特别是GPU的大量使用大大提高深度学习模型训练效率。另外，开源框架与算法的推广也降低了深度学习的使用门槛并推动了科技的迅猛发展。

深度学习基本原理是建立在人工神经网络基础之上。典型深度学习模型包括输入层、若干隐藏层、输出层。输入层对原始数据进行接收，隐藏层对数据进行非线性变换进行特征提取，输出层基于任务需求产生预测结果。深度学习模型训练过程分为正向传播与反向传播两大阶段。前向传播阶段通过网络层层传输数据产生预测结果；在反向传播环节，依据预测结果和真实标签的不同，采用梯度下降算法对网络参数进行调整，使预测误差达到最小。

1.2 深度学习在网络安全领域的应用现状

深度学习技术从产生至今已在很多领域特别是图像识别，语音识别以及自然语言处理领域获得显着成果。近年来，网络技术飞速发展，网络安全问题日趋严重，常规安全防护手段已很难应对越来越复杂的网络威胁。将深度学习技术应用于网络安全领域，重点研究了如下问题：识别恶意软件：恶意软件对网络安全构成了重大威胁。基于深度学习的恶意软件识别方法能够通过对恶意软件行为特征，代码结构以及其他信息进行分析，从而快速地对恶意软件进行识别与分类；网络入侵检测：网络入侵检测在网络安全中占有重要地位。深度学习技术能够通过对网络流量，系统日志及其他数据进行分析来发现潜在入侵行为并提高检测精度与实时性；网络钓鱼鉴定：网络钓鱼属于网络诈骗的常见方式。该方法以深度学习为基础，通过对钓鱼网站页面布局，域名特征及其他信息进行分析，能够快速地识别并截获钓鱼网站；网络安全态势感知：即对网络安全状况进行综合感知与评价。深度学习技术能够通过对网络流量，用户行为等多源数据进行分析，从而实现网络安全态势实时监控与预警；网络安全预警与应对：网络安全事件出现时，及时预警与应对对减少损失具有重要意义。深度学习技术能够通过对历史数据进行分析来预测网络安全事件发生的概率以及制定出相关应对策略。

1.3 深度学习技术的优势与挑战

将深度学习技术应用于网络安全领域，有如下优

点：自动特征提取，传统网络安全分析方法一般要求人工设计特征，并且深度学习技术能够自动地从原始数据中学得有用特征，降低人工干预并提高分析效率与精度；深度学习模型具有出色的数据处理能力，能够处理大量、多维度的数据，这对于分析网络流量、用户行为等复杂数据是非常重要的；高准确性：深度学习模型已在图像识别和自然语言处理中表现出极高的精度，并为网络安全领域提供强大支撑；泛化能力高：深度学习模型泛化能力较好，能够适应各种网络环境及安全威胁，增强其适用性。[2]

将深度学习技术应用到网络安全领域中，同样存在一定的挑战，主要表现在以下几个方面：难以获取数据：训练深度学习模型对标注数据要求较高，并且在网络安全领域中，高质量标注数据比较难获得，制约着模型训练结果；可解释性不强：深度学习模型常被认为是一个“黑箱”，很难给安全专家带来直观分析结果，从而在某种程度上制约了其适用范围；计算资源耗费巨大：深度学习模型对计算资源的要求普遍较高，给网络安全领域在现实中的应用提出了一些挑战；安全性方面：深度学习模型会遭受对抗性攻击，攻击者可通过构建具体输入样本来误导模型判断，从而对网络安全构成新威胁。

2 基于深度学习的网络安全威胁识别技术

2.1 网络安全威胁的分类与特征分析

网络安全威胁有很多种，一是恶意软件对网络安全构成了重大威胁。恶意软件以各种方式混入到系统中，盗用信息、破坏资料。[3]深度学习能够通过对恶意软件行为模式和代码结构进行特征分析来达到识别恶意软件。例如，通过使用卷积神经网络（CNN）来提取恶意软件代码的特征，能够有效地将恶意软件与正常软件进行区分；二是网络入侵，即攻击者利用漏洞和弱口令的形式对系统进行非法的访问。深度学习能够通过对网络流量和登录尝试的数据分析来发现异常行为；三是网络钓鱼，通过伪造网站和邮件来引诱用户暴露敏感信息的攻击方法。深度学习通过对钓鱼网站页面结构和邮件内容进行特征分析来确定钓鱼攻击。比如，用自然语言处理技术来分析邮件内容的语义就能判断其是否含有欺诈信息。

2.2 基于深度学习的恶意软件识别技术

恶意软件识别对于网络安全至关重要，将深度学习应用于恶意软件识别具有如下特点：首先，基于深度学习提取恶意软件特征。传统恶意软件检测方法主要依靠人工提取特征，通常不全面且易受恶意软件变种干扰。深度学习可以对恶意软件二进制代码进行有效特征提取，提升识别精度；其次，根据深度学习对恶意软件家族进行分类。恶意软件通常是家族性的，同家族恶意软件的行为模式和代码结构都有相似之处。深度学习能够通过对这些相似性进行分析来达到恶意软件家族划分的目的；最后基于深度学习提出了一种恶意软件检测模型。传统恶意软件检测模型通常需要大量手工标注数据，深度学习可采用无监督或者半监督方法训练以降低对标注数据依赖性。

2.3 基于深度学习的网络入侵检测技术

网络入侵检测对于网络安全至关重要，将深度学习应用于网络入侵检测主要有以下几点：一是深度学习分析网络流量。在网络入侵过程中经常会伴有网络流量不正常现象，例如海量数据包和流量模式不正常。[4]深度学习能够通过对网络流量进行特征分析来发现潜在入侵行为；二是深度学习对系统日志进行分析。系统日志是对系统运行状态，用户操作行为等信息进行记录。通过对系统日志进行分析，能够检测出异常操作行为，例如频繁登录尝试和异常文件访问。深度学习能够自动提取系统日志的关键信息并实现入侵行为识别；三是深度学习提出一种入侵检测模型。传统入侵检测模型通常需要手动定义规则，深度学习可采用数据驱动方式训练以提升检测精度。

2.4 基于深度学习的网络钓鱼识别技术

网络钓鱼对网络安全构成了巨大威胁，将深度学习运用于网络钓鱼识别有如下几方面内容：一是基于深度学习识别钓鱼网站。钓鱼网站一般都是仿照正规网站外观与内容来引诱用户对敏感信息进行录入。深度学习通过对钓鱼网站进行页面结构和域名相似度分析来识别钓鱼网站；二是基于深度学习识别钓鱼邮件。钓鱼邮件中一般都含有欺诈性链接或者配件来引诱用户进行点击或者下载。深度学习能够通过对邮件内容与结构进行分析来确定钓鱼邮件；三是深度学习对钓鱼行为进行识别。除钓鱼网站及邮件外，钓鱼攻击也可通过社交媒体，即时通讯工具及其他渠道实施。深度学习能够通过对用户行为模式进行分析来发现潜在钓鱼行为。

2.5 基于深度学习的网络安全态势感知技术

网络安全态势感知技术对网络安全风险进行评估与预测具有重要意义。将深度学习技术应用于网络安全态势感知具有如下优点：一是深度学习模型能够自动抽取海量网络数据特征并识别潜在安全风险；二是深度学习模型能够实时地对大规模数据进行处理，提升态势感知效率；三是深度学习模型能够综合多个数据源实现多维度安全态势分析。

深度学习技术对网络安全态势的感知同样面临着一定的挑战。如网络安全态势评估与预测需综合考虑诸多因素，深度学习模型对于多因素综合分析仍有欠缺；另外，网络安全态势评估结果需支持安全决策，深度学习模型可解释性差，很难满足决策者要求。所以，今后的研究还需从多因素综合分析和模型可解释性两个方面不断创新与优化。

3 基于深度学习的网络安全威胁防御技术

3.1 基于深度学习的网络安全防御策略

网络安全防御策略，是建设安全防护系统的核心内容。本文提供一种基于深度学习网络的安全防御策略，该策略通过网络流量，用户行为以及其他数据分析来自动识别潜在威胁并进行防御。[5]深度学习模型可以从海量数据中学得复杂的规律与模式，进而提升防御策略制定的精度与效率。比如，训练一个深度神经网络用于网络流量分类就能有效地识别恶意流量并采取适当防御措施。另外，深度学习防御策略可以自适应地进行调整，并依据网络环境变化对防御策略进行动态优化以增强防御效果。

3.2 基于深度学习的网络安全态势感知技术

网络安全态势感知是对网络安全状况进行实时监测与评价的核心技术。以深度学习为基础的网络安全态势认知技术通过对网络流量，系统日志以及其他数据进行分析来实现网络安全态势实时认知与评价。深度学习模型可以对多源数据进行特征提取并构建网络安全态势多维度表达，以全面准确反映网络安全情况。比如训练卷积神经网络提取网络流量特征，就能识别异常流量模式并及时检测潜在安全威胁。另外，基于深度学习态势感知技术也可以实现网络安全态势预测与预警，从而支持网络安全决策。

3.3 基于深度学习的网络安全预警与响应技术

网络安全预警与响应技术对于解决网络安全威胁具有重要意义。以深度学习为核心的网络安全预警和响应技术通过对网络活动进行实时监控，及时发现安全威胁，并做出相应响应。深度学习模型可以通过网络流量，用户行为以及其他数据来学习安全威胁特征，从而达到安全威胁快速辨识与预警的目的。比如，训练一个循环神经网络来分析网络流量的时序，就能预测可能出现的攻击行为和提前报警。同时，基于深度学习响应技术也可以根据预警信息自动引发相关防御措施，例如屏蔽恶意流量和隔离被感染系统以达到有效应对安全威胁。

4 结束语

文章对基于深度学习实现网络安全威胁的智能识别及防御技术进行深入探究，并运用对比分析、逻辑推理等方法揭示出影响网络安全的诸多因素。国内外学者的研究表明，将深度学习技术应用于网络安全领域有着显著优势，特别在恶意软件识别、网络入侵检测以及网络钓鱼识别领域，表现出较强的识别能力。

研究结论显示：基于深度学习网络安全威胁识别和防御技术可以有效地提升网络安全防护智能化程度，并为解决越来越复杂的网络威胁问题提供一种全新解决方案。但也要清醒地看到，深度学习技术应用于网络安全领域还面临着数据隐私保护和模型泛化能力的挑战。这些问题都需要在今后的研究方向上加以关注并加以解决。

参考文献

[1]李大岭,张浩军,王家慧,等.基于深度学习的网络安全命名实体识别方法[J].无线电工程,2024(3):644-652.

[2]乔少华,祝玲,张翠玲.基于深度学习算法的造纸企业工控网络安全管理模型研究[J].造纸科学与技术,2024(1):119-122.

[3]任海娟.基于深度强化学习的智能网络安全防护策略研究[J].无线互联科技,2023(6):19-21.

[4]黄毅,包世洪,马亮,等.基于多重深度学习网络的安全帽检测及工地人员身份识别方法研究[J].建筑安全,2023(4):67-70.

[5]李伟.基于深度学习的网络安全入侵检测与防御技术研究[J].学生电脑,2023(3):0031-0033.