基于深度学习的网络入侵检测系统研究

荣志文　付　蓉
金盾检测技术股份有限公司　江苏南京　210000

摘　要：随着网络攻击的日益复杂和频繁，传统的网络入侵检测技术面临着较大的挑战。深度学习作为一种高效的自动化学习方法，已广泛应用于各种数据分析领域，特别是在网络安全领域。基于深度学习的网络入侵检测系统通过利用大规模网络数据训练深度神经网络模型，能够有效地识别多种网络攻击模式。本文旨在研究基于深度学习的网络入侵检测系统的设计与实现，分析其在入侵检测中的应用优势，基于深度学习的入侵检测系统表现出了较高的准确率和较强的泛化能力。

关键词：网络入侵检测；深度学习；卷积神经网络；循环神经网络；生成对抗网络

引言

随着信息技术的迅猛发展，网络安全问题逐渐成为全球关注的焦点。网络入侵检测系统（IDS）作为保护网络安全的核心技术之一，承担着实时监控网络流量、检测异常行为和防范恶意攻击的重要任务。传统的入侵检测方法通常依赖于规则匹配或特征提取，但这些方法在面对复杂的攻击模式时，难以保持高效性与准确性。近年来，深度学习技术的快速发展为网络入侵检测提供了新的解决方案。深度学习模型能够通过对大量网络数据的自动学习，提取出更为深刻的特征信息，有效提高入侵检测的性能和准确性。

一、网络入侵检测系统概述

（一）网络入侵检测的定义与背景

网络入侵检测系统（IDS）是通过监控和分析网络流量及活动，自动检测并响应网络安全威胁的系统。随着互联网的快速发展和信息技术的普及，网络安全威胁愈加严重。各种网络攻击手段层出不穷，从传统的病毒传播、木马攻击到近年来的DDoS攻击、零日漏洞等多种形式，给网络安全带来极大挑战。入侵检测技术作为网络安全防护的核心手段之一，起到了监控、识别、分析和响应入侵行为的重要作用。通过实时监测网络流量，IDS可以识别出潜在的攻击模式并及时报警，帮助安全管理员迅速采取措施进行防范。随着网络环境的日益复杂化，传统的入侵检测方法在处理大规模数据和复杂攻击时的有效性逐渐减弱，促使研究人员探索新的、更高效的入侵检测技术。

（二）网络入侵检测技术的分类

网络入侵检测技术主要分为两类：基于签名的检测和基于异常的检测。基于签名的检测方法通过与已知攻击特征数据库进行比对，检测网络流量中的恶意活动。该方法优点是准确率较高，能够快速识别出已知的攻击类型。然而，其缺点在于无法识别新型的、未知的攻击模式，限制了其在面对多变的网络威胁时的适应性。另一类方法是基于异常的检测技术，该方法通过建立正常网络行为模型，检测偏离该模型的异常活动。该方法能够检测到未知攻击，但其准确率较低，容易发生误报和漏报。因此，近年来的研究更多地集中于结合两者优势，开发综合性更强、能够自动学习新攻击特征的入侵检测方法。

（三）深度学习在网络安全中的应用前景

深度学习技术凭借其强大的特征自动提取能力，已成为提升网络入侵检测系统性能的重要技术之一。与传统的规则匹配和特征提取方法不同，深度学习能够通过大规模数据的训练，自动发现网络数据中的潜在规律和攻击模式。因此，深度学习不仅能提高系统在面对复杂网络攻击时的识别能力，还能减少人工干预，提升检测效率。随着网络攻击的多样化和智能化，深度学习在网络安全领域的应用前景广阔。通过使用卷积神经网络（CNN）、循环神经网络（RNN）等深度学习模型，网络入侵检测系统能够更加精准地识别各种已知和未知的攻击行为。同时，深度学习技术的不断进步，特别是在模型优化和计算能力的提升，进一步增强了其在大规模网络环境中的应用能力。因此，深度学习在网络入侵检测

领域将继续发挥重要作用，推动网络安全防护技术的持续发展[1]。

二、深度学习技术基础

（一）深度学习的基本概念与发展历程

深度学习是一种基于人工神经网络的机器学习技术，它通过构建多层次的神经网络模型来进行数据特征的自动学习与表达。深度学习的核心思想源自于神经科学，旨在模拟人脑神经元之间的连接方式。最早的神经网络模型可追溯至20世纪40年代，但深度学习真正的发展始于21世纪。2006年，Geoffrey Hinton等学者提出了深度置信网络（DBN）及其训练方法，使得深度学习技术迎来了突破性进展。2012年，深度卷积神经网络（CNN）在图像识别领域获得了重大成功，标志着深度学习进入了一个快速发展的新时代。随着大数据技术的不断发展和计算能力的提升，深度学习在多个领域取得了显著成果，并广泛应用于语音识别、图像处理、自然语言处理等领域。特别是在网络安全和入侵检测领域，深度学习展现出了巨大的应用潜力，能够有效处理复杂的网络数据，并识别各种攻击模式。

（二）常用深度学习算法及其特点

深度学习包括多种算法，其中常用的包括卷积神经网络（CNN）、循环神经网络（RNN）、长短期记忆网络（LSTM）和生成对抗网络（GAN）。CNN广泛应用于图像处理领域，其核心优势在于局部感知和权重共享，使其在处理高维数据时具有较好的性能。RNN及其变种LSTM适用于处理时序数据，能够捕捉到数据中的长期依赖关系，广泛应用于自然语言处理和语音识别等领域。LSTM通过引入门控机制，有效解决了传统RNN在处理长序列数据时的梯度消失问题，使其在入侵检测中具备更强的时序数据处理能力。GAN通过生成器和判别器的对抗训练，能够生成高质量的假数据，并在异常检测和数据增强中发挥重要作用。各个深度学习算法具有不同的特点，适用于不同的数据类型和应用场景，选择合适的算法能够显著提高网络入侵检测系统的性能。

（三）深度学习在数据挖掘中的优势

深度学习在数据挖掘中具有显著的优势，尤其是在处理大规模、复杂的非结构化数据时。传统的机器学习方法依赖于人工提取特征，这需要大量领域知识，并且难以应对复杂的数据模式。而深度学习能够自动从数据中学习出有效的特征表示，避免了人工干预的需要，提高了数据处理效率。在网络入侵检测领域，深度学习能够从大量的网络流量数据中自动提取特征，发现潜在的攻击模式。此外，深度学习能够处理高维数据，适应性强，可以在动态变化的网络环境中持续学习新模式，适应新型攻击[2]。深度学习还具有较强的泛化能力，在面对未知攻击时也能有效识别，减少误报和漏报。随着计算能力的提升和算法的不断优化，深度学习在数据挖掘中的优势将越来越明显，成为大数据时代不可或缺的技术工具。

三、基于深度学习的网络入侵检测系统设计

（一）网络入侵检测系统的架构设计

基于深度学习的网络入侵检测系统通常采用多层次的架构，旨在有效处理复杂的网络流量数据。一般来说，系统架构包括数据采集、数据预处理、特征提取、模型训练和入侵检测等主要模块。在数据采集阶段，系统实时监控网络流量，收集包括IP地址、端口号、协议类型、数据包大小等信息。接下来，数据预处理模块对采集的数据进行清洗、去噪以及标准化，以确保数据质量。特征提取模块则通过深度学习模型自动从网络流量中提取特征，避免了人工设计特征的局限性。经过处理的特征数据将输入到训练模型中进行训练与优化，最终通过模型推理判断是否存在入侵行为。为了提高模型的泛化能力，系统通常采用集成学习或多模型协同工作策略，通过组合不同模型的优势，提高入侵检测的准确率和鲁棒性。整个系统需要具备高效的实时处理能力，以应对高速、大流量的网络数据，确保及时发现潜在威胁。

（二）数据集的选择与预处理

数据集的选择对网络入侵检测系统的效果至关重要。常用的数据集包括KDD Cup 99、NSL-KDD、CICIDS等，这些数据集包含了多种类型的攻击行为和正常流量数据。在选择数据集时，需根据入侵检测的目标选择适当的数据类型和规模。数据预处理是确保深度学习模型能够准确训练和预测的关键步骤。通常，预处理过程包括数据清洗、去重、缺失值填充以及数据标准化等。数据清洗过程中，去除重复记录和异常值有助于减少噪音对模型的干扰。缺失值填充可以采用均值、中位数或众数填充方法，确保数据的完整性。在数据标准化阶段，将所有特征的值转化到统一的量纲范围内，常见的标准化方法包括Z-score标准化和Min-Max缩放。通过这些预处理步骤，可以大大提高模型的收敛速度和精度。此外，为了应对不平衡数据问题，通常采用过采样或欠采样技术，确保模型能够有效学习到各种攻击模式。

（三）深度学习模型的选择与优化

在基于深度学习的网络入侵检测系统中，模型的选择和优化直接影响到系统的检测能力。常见的深度学习模型包括卷积神经网络（CNN）、循环神经网络（RNN）、长短期记忆网络（LSTM）以及自编码器（AutoEncoder）等。不同模型具有不同的特点，适用于不同的数据类型和应用场景。例如，CNN具有强大的特征自动提取能力，特别适用于处理图像和高维数据。在网络入侵检测中，CNN能够从网络流量数据中自动提取有效的特征，避免了人工特征选择的局限性。RNN和LSTM则适用于时序数据，能够捕捉数据中的时间依赖性，适用于分析网络流量的时间序列特征。模型优化方面，常见的优化方法包括调整学习率、使用正则化技术、采用合适的激活函数等。在训练过程中，采用批量梯度下降（SGD）或Adam优化器来更新模型参数，以提高模型的精度和收敛速度。同时，利用交叉验证技术评估模型的泛化能力，避免过拟合现象[3]。

四、基于深度学习的网络入侵检测方法研究

（一）卷积神经网络（CNN）在入侵检测中的应用

卷积神经网络（CNN）广泛应用于图像识别和模式分类任务，也在网络入侵检测中发挥了重要作用。CNN的优势在于其强大的特征提取能力，能够自动从输入数据中提取重要的空间特征。在网络入侵检测中，CNN通常将网络流量数据转化为二维矩阵，类似于图像输入，进行卷积操作，从中提取出流量数据的局部特征。CNN的卷积层通过滤波器对输入数据进行卷积运算，有效地捕捉到数据中的局部模式。这一过程避免了人工特征选择的繁琐，并且提升了特征提取的效率。池化层则有助于降低数据的维度和计算复杂度，同时保留最重要的特征信息。在入侵检测任务中，CNN不仅能识别已知的攻击模式，还能够自动从复杂的流量数据中提取出潜在的攻击行为。例如，在处理DoS攻击、恶意扫描等常见攻击时，CNN通过多层的卷积和池化操作，有效提高了检测的准确性和鲁棒性。通过训练CNN模型，系统能够实现自动化、高效的入侵检测，减少误报率并提高检测速度。

（二）循环神经网络（RNN）与长短期记忆网络（LSTM）的应用

循环神经网络（RNN）和长短期记忆网络（LSTM）在处理时序数据方面具有显著优势，尤其适用于分析网络流量的时间序列特征。与传统的前馈神经网络不同，RNN能够处理和分析具有时序关系的数据，通过自身的循环结构记住前一时刻的信息，从而捕捉到数据中的时序依赖关系。在网络入侵检测中，RNN能够分析网络流量的时间变化趋势，有效识别持续性攻击行为。然而，标准的RNN在处理长时间序列时存在梯度消失和梯度爆炸的问题，这使得其在长序列数据的学习上表现不佳。为了解决这一问题，LSTM作为RNN的一种改进，加入了记忆单元和门控机制，能够有效地捕捉到长时序中的长期依赖关系，从而提升了模型的性能。在网络入侵检测中，LSTM可以用于分析具有长时间间隔的攻击模式，如间歇性DDoS攻击或持续性扫描攻击等。通过LSTM，模型可以更准确地识别出时间序列中潜在的异常行为，提升了检测系统对未知攻击的适应能力。LSTM的引入使得基于深度学习的入侵检测系统在面对复杂、动态变化的网络环境时，能够提供更高的检测准确度和鲁棒性[4]。

结语

基于深度学习的网络入侵检测系统具有显著的优势，尤其在处理复杂、高维和时序数据时展现了强大的性能。通过卷积神经网络（CNN）、循环神经网络（RNN）及长短期记忆网络（LSTM）的应用，系统能够自动从大量网络流量中提取有用特征，识别多种已知和未知的入侵模式。深度学习的引入不仅提高了入侵检测的准确率和效率，还增强了系统在面对新型攻击时的适应能力。尽管当前的深度学习技术在入侵检测中已取得显著成果，但仍面临数据不平衡、计算资源消耗等挑战。未来的研究将进一步优化深度学习模型，提升网络安全防护能力，为应对更加复杂的网络威胁提供技术支持。

参考文献

[1]赵健.基于深度学习算法的网络传输数据智能检测研究[J].现代电子技术，2025，48（23）：118-122.

[2]黎燕.基于深度学习模型的网络流量预测与性能优化方法研究[J].软件，2025，46（11）：25-27.

[3]蓝家运，段晓霞，王丽颖.基于深度学习网络的AI拟声检测系统的设计[J].现代信息科技，2025，9（22）：35-39.

[4]仇丹丹.基于剪枝算法优化的轻量级深度学习网络算法[J].计算机科学，2025，52（S2）：206-212.