DOI:10.12361/2705-0866-05-09-140601

# 深度学习在网络安全领域的应用研究综述

陈青梅　任明春　彭志珍

贵州省疾病预防控制中心，中国·贵州　贵阳　550003

【摘　要】近年来，深度学习由于其能够更全面地捕捉网络数据的特征，在与各种网络异常检测方法结合后能获得更好的检测结果等特点，逐渐引起网络安全领域的关注。为进一步理清深度学习在网络安全应用相关工作的研究脉络，首先对神经网络表示学习进行简要介绍；其次梳理常用的三类基于深度学习的网络安全检测方法，并对这三类方法进行分析对比；接着简要介绍公开的网络入侵检测数据集；最后对本文进行总结并探讨目前研究的局限性及将来的研究方向。

【关键词】深度学习；神经网络；网络异常检测；网络安全；入侵检测数据集

# A Review of the Application of Deep Learning in Network Security

Qingmei Chen, Mingchun Ren, Zhizhen Peng

Guizhou Provincial Center For Disease Control And Prevention, Guiyang 550003, Guizhou China

[Abstract] In recent years, deep learning has gradually attracted attention in the field of network security, because it can capture the characteristics of network data more comprehensively, and obtain better detection results after combining with various network anomaly detection methods. In order to clarify the research context of the application of deep learning in network security, the neural network representation learning is briefly introduced. Secondly, three kinds of network security detection methods based on deep learning are summarized, and these three methods are analyzed and compared. Then, the open network intrusion detection datasets are briefly introduced. Finally, this paper summarizes and discusses the limitations of the current research and the future research direction.

[Keywords] Deep learning; Neural network; Network anomaly detection; Network security; Intrusion detection dataset

## 1　引言

神经网络是深度学习的实现模型，它模仿人脑的神经元网络来处理信息。神经网络由输入层、隐含层和输出层组成，每层有许多神经元构成。神经元之间通过权重相连，神经网络通过学习调整权重来处理输入信息并生成输出结果。深度学习则是使用多层神经网络来进行机器学习的方法，这些多层神经网络被称为深度神经网络。而卷积神经网络（Convolutional Neural Network, CNN）、循环神经网络(Recurrent Neural Network, RNN)和图神经网络（(Graph Neural Networks, GNN）则是深度神经网络的不同实现形式。基于深度学习的网络安全检测方法可以通过对网络流量、设备活动等数据进行分析，自动识别和学习网络攻击的特征，从而快速发现潜在的攻击，使网络管理人员能够采取相应的安全防护措施以预防网络攻击的发生。

## 2　基于深度学习的网络安全检测方法

### 2.1基于卷积神经网络的网络安全检测方法

卷积神经网络是一种常用于图像和视频数据处理的深度学习模型。通常包含卷积层、池化层及全连接层等结构。将采集的历史数据传入输入层，并经过正向传播到各网络层处理后输出，当输出结果不满足期望值的情况下执行反向传播过程。在网络安全检测过程中，需将网络数据转化为灰度图的表现形式，然后在输入卷积神经网络中提取空间特征信息进行学习，最终输出结果。

卷积神经网络在网络和信息安全领域也取得了不错的表现效果。如在网络异常事件检测方面，Nasr等[1]设计了一种基于CNN的流关联检测系统-DeepCorr。它利用改进后的CNN算法学习复杂流关联函数，能捕捉到动态变化下噪声的复杂性质，与传统入侵检测算法相比，在检测准确率上有了显著的提升。此外，Andresini等[2]也提出了一种结合CNN的入侵检测模型，克服了传统机器学习算法不能有效检测未知网络攻击的问题。

2.2基于循环神经网络的网络安全检测方法

循环神经网络是一种针对时间序列数据问题的神经网络，它利用序列间的循环连接实现对序列的表征学习与理解，能够处理变长序列，被广泛应用于序列数据问题的处理。相比传统的神经网络，它能够保留历史信息并利用历史信息来影响当前时刻的输出和隐藏状态，有效解决了序列数据中一般神经网络无法解决的问题。

由于循环神经网络善于处理任意长的数据，它在数据预测和恶意软件检测方面有较广泛的应用。如Ramakrishnan等[3]提出了几种递归神经网络架构(标准RNN，长短期记忆网络LSTM和GRU)来解决网络流量预测问题，通过对历史网络流量的观察来预测未来网络流量的特征。Hagos等使用基于LSTM的递归神经网络建立了传输控制协议(TCP)关联特征的通用预测模型等。

2.3基于图神经网络的网络安全检测方法

图神经网络是对现有神经网络的扩展，能够处理以图结构表示的数据。这类网络结构在一定程度上受到卷积神经网络和图嵌入的推动。将图神经网络应用在网络安全领域解决问题的一般框架为：首先将采集到网络数据进行预处理后构建成图结构，接着根据下游任务需求，将图结构中的高维数据在不影响其性质的前提下转换成低维嵌入向量表示，并提取其数据特征和数据间的依赖关系，最后经图神经网络训练后输出结果。

在网络和信息安全领域，基于图神经网络的网络安全检测方法能够与多种检测思想相结合，识别出网络和信息系统的安全弱点以保护其能正常运行。如在异常事件检测方面，Fan等[4]提出一种同时融合实体属性和二阶结构的深度异构网络表示方法。该方法利用多层感知器和自编码器分别学习属性嵌入和二阶嵌入；然后，使用基于混合嵌入对不同实体的成对交互进行建模，使得实体兼容性小的事件具有较大的异常事件得分。实验表明，提出的方法能够更加全面检测异常事件。此外，Leichtnam等介绍了一种统一而唯一的图表示形式，称为安全对象图。这种图形式混合和链接了不同类型的事件，并允许对要分析的活动进行丰富的描述。为了在图中检测异常行为，该文提出了一种基于自动编码器的无监督学习方法，其在CIC-IDS2017数据集上的表现并不逊于其对比的有监督方法。

## 3 三类网络安全检测方法的对比

卷积神经网络在处理高维数据特征和自动提取局部特征方面占有一定优势。CNN凭借其特有的网络结构与算法，具有良好的泛化能力和鲁棒性且有稳定的输入输出，适用于大规模数据处理和实时应用场景。循环神经网络在处理序列数据时通常具有较好的预测性能，能够学习到序列数据中的规律和特征。但也存在“梯度消失”和“梯度爆炸”现象，导致RNN无法解决长时间的数据依赖问题，为解决此问题出现了LSTM和GRU等RNN变体。如果数据相对稀疏，需要邻域节点做信息的协同建模，那么使用基于图神经网络的检测方式也比较合适，对序列信息的非线性特征学习也占一定优势。三类网络安全检测方法的优劣势对比如表1所示。

表1 三类网络安全检测方法的优劣势对比

| 类别 | 优势 | 劣势 |
|---|---|---|
| 基于CNN类 | 自动识别和学习数据特征，可处理高维数据，具有良好的局部特征提取能力。<br>良好的泛化能力和鲁棒性，具有稳定的输入输出。 | 对于非图像数据的处理能力较弱且对于大规模数据集需要较长的训练时间。<br>小样本数据不太适用和对计算设备要求高。<br>针对复杂的特征训练，容易出现过拟合。 |
| 基于RNN类 | 网络具有记忆性、各网络节点的参数共享且图灵完备。<br>可以处理变长的序列数据。 | 计算复杂度较高，训练时间长。<br>存在“梯度消失”和“梯度爆炸”现象。 |
| 基于GNN类 | 具有强大的非结构化学习能力，数据拟合能力强。<br>能够从非结构化数据中进行学习和推理。 | 模型训练过程中存在大量超参数，且具有非凸形。 |

## 4 网络安全数据集

基于深度学习的网络安全检测方法需使用网络数据集对该方法的性能和效果进行评估。本节主要对网络入侵检测中常用的公开数据集进行简要介绍。

（1）KDD99数据集：该数据集是网络入侵检测领域常用的经典数据集，主要包含四种异常数据类型，分别为DoS攻击、远程到本地、探针攻击和用户提权攻击。然而该数据

集也存在一些缺陷，比如有冗余记录、攻击类别单一等，故不能完全描述网络攻击行为的特征。

（2）NSL-KDD数据集：该数据集是对KDD数据集的改进，数据集中不存在记录冗余和数据缺失，且训练集和测试集数量分配合理，可作为基准数据集直接用于入侵检测的完整实验。

（3）UNSW-NB15数据集：UNSW-NB15数据集包含九种攻击类型数据，对网络流量数据反映较为全面和准确，且数据采集周期长，常用于网络入侵检测实验。

（4）CICIDS-2017数据集：该数据集是基于双向流格式和分组的网络流量数据。包含七种网络攻击类别，且具有流量特征数多和数据多样性的等特点，更接近网络真实环境，适用于检测新网络攻击。

（5）UGR’16数据集：UGR’16也属于单向流网络流量的数据集。该数据集侧重于长时间捕捉周期效应。攻击行为包括DoS、端口扫描和僵尸网络，且大部分流量数据都有标签。

## 5 总结与展望

本文介绍了深度学习在网络和信息安全领域的研究现状和成果，对当前常用的网络安全检测算法进行梳理，分为基于卷积神经网络、基于循环神经网络和基于图神经网络的检测方法，并对这三类方法的优缺点和常用的网络安全数据集进行了分析总结，为同领域的研究者和网络安全管理人员提供网络安全检测的技术方案参考，便于他们对各类网络检测方法的查阅和学习。

深度学习在网络安全异常检测方面取得了不错成绩，但在大部分网络环境下强调入侵检测的实时性，这对检测模型的轻量化处理提出了要求，故研发轻量化的入侵检测模型是未来研究的重点方向之一。此外，单一的深度学习算法在精度、效率和覆盖范围上还存在提升的空间，故可以考虑基于集成学习或其他模型融合的方法来提高入侵检测准确度和效率。

**参考文献：**

[1] Nasr M, Bahramali A, Houmansadr A. Deepcorr: Strongflow correlation attacks on TOR using deep learning[C]//Proc of the 2018 ACM SIGSAC Conf on Computer and Communications Security. New York: ACM, 2018:1962-1976.

[2] Andresini G, Appice A, Malerba D. Nearest cluster-based intrusion detection through convolutional neural networks[J]. Knowledge-Based Systems, 2021, 216:106798.

[3] Ramakrishnan N, Soni T. Network traffic prediction using recurrent neural networks[C]//2018 17th IEEE International Conference on Machine Learning and Applications.Orlando:IEEE, 2018:187-193.

[4] Fan S, Shi C, Wang X. Abnormal event detection via heterogeneous information network embedding[C] // Proceedings of the 27th ACM international conference on information and knowledge management. Italy:ACM, 2018:1483-1486.