计算机应用
Journal of Computer Applications
ISSN 1001-9081,CN 51-1307/TP

《计算机应用》网络首发论文

题目：基于深度学习的网络入侵检测系统综述
作者：邓淼磊，阚雨培，孙川川，徐海航，樊少珺，周鑫
收稿日期：2024-03-06
网络首发日期：2024-07-24
引用格式：邓淼磊，阚雨培，孙川川，徐海航，樊少珺，周鑫．基于深度学习的网络入侵检测系统综述[J/OL]．计算机应用．
https://link.cnki.net/urlid/51.1307.TP.20240723.1515.004

Journal of Computer Applications
计算机应用
ISSN 1001-9081
CODEN JYIIDU
http://www.joca.cn

DOI:10.11772/j.issn.1001-9081.2024020229

基于深度学习的网络入侵检测系统综述

邓淼磊[1,2],阚雨培[1,2*],孙川川[1,2],徐海航[1,2],樊少珺[1,2],周　鑫[1,2]
(1.河南工业大学 信息科学与工程学院,郑州 450001;　2.河南省粮食信息处理国际联合实验室,郑州 450001)
(*通信作者电子邮箱kypei2023@163.com)

摘　要:入侵检测系统等安全机制已被用于保护网络基础设施和网络通信免受网络攻击。随着深度学习技术的不断进步,基于深度学习的入侵检测系统逐渐成为网络安全领域的研究热点。通过对文献的广泛调研,详细介绍了利用深度学习技术进行网络入侵检测的最新研究进展。首先,简要概述了当前几种不同的入侵检测系统;接着,介绍了基于深度学习的入侵检测系统中常用的数据集和评价指标;然后,总结了网络入侵检测系统中常用的深度学习模型以及其应用场景;最后,探讨了当前研究过程中所面临的问题,并提出了未来的发展方向。

关键词:网络安全;入侵检测;深度学习;异常检测;网络入侵检测系统

中图分类号:TP393.08　　**文献标志码:**A

Summary of network intrusion detection systems based on deep learning

DENG Miaolei[1,2], KAN Yupei[1,2*], SUN Chuanchuan[1,2], XU Haihang[1,2], FAN Shaojun[1,2], ZHOU Xin[1,2]
(1. *College of Information Science and Engineering, Henan University of Technology, Zhengzhou Henan* 450001, *China*;
2. *Henan International Joint Laboratory of Grain Information Processing, Zhengzhou Henan* 450001, *China*)

Abstract: Security mechanisms such as intrusion detection systems have been used to protect network infrastructure and communication from network attacks. With the continuous progress of deep learning technology, intrusion detection systems based on deep learning have gradually become a research hotspot in the field of network security. Through extensive literature research, this paper provides a detailed introduction to the latest research progress in using deep learning technology for network intrusion detection. Firstly, a brief overview of several different intrusion detection systems is provided; Next, the commonly used datasets and evaluation metrics in deep learning based intrusion detection systems were introduced; Then, the commonly used deep learning models and their application scenarios in network intrusion detection systems were summarized; Finally, the problems faced in the current research process were discussed, and future development directions were proposed.

Key words: network security; intrusion detection; deep learning; anomaly detection; network intrusion detection system

0　引言

网络在现代生活中扮演着重要的角色,网络安全已成为一个重要的研究领域。网络入侵成为了一种严重威胁,对个人、企业和政府机构的敏感数据和业务运作构成了严重威胁。因此,及时发现和应对网络入侵成为了网络安全的重要任务之一。现有的安全方法大多是被动安全防御[1],包括安全网关、防火墙、代码签名和加密技术,无法主动检测和响应[2]。入侵检测系统[3](Intrusion Detection System,IDS)最早于1980年提出,是一种网络安全防护技术,主要通过捕获和分析网络数据流量记录检测网络攻击或异常行为。当攻击发生时,IDS会及时响应发现攻击。这种方法可以主动发现攻击,适合作为网络的安全预防措施[4]。然而,目前许多入侵检测系统存在较高的误警率,会对威胁性较低的情况会产生大量警报,这不仅增加安全分析人员的负担,而且降低高风险攻击威胁的检测率。因此,许多研究人员致力于开发具有更高检测率和更低误警率的入侵检测系统。现有入侵检测系统的另一个问题是它们缺乏检测未知攻击的能力。由于网络环境瞬息万变,攻击变种和新奇攻击不断涌现。因此,有必要开发能够检测未知攻击的入侵检测系统。

目前,基于异常的网络入侵检测系统成为了一种备受关注的解决方案。相较于传统的基于签名的检测方法,基于异常的方法不依赖于已知攻击的特征,而是通过分析网络流量数据中的异常模式来检测潜在的未知攻击行为。研究人员开始致力于利用机器学习(Machine Learning,ML)方法构建基于异常的入侵检测系统[5],如决策树(Decision Tree, DT)[6]、朴素贝叶斯(Naive Bayes, NB)[7]和支持向量机(Support Vector Machine, SVM)[8]。对比传统的入侵检测系统,ML方法的应用为入侵检测系统提供了更好的实时性和准确性,有助于及时识别和应对不断演变的网络威胁和攻击变种,也为网络

收稿日期:2024-03-06;**修回日期:**2024-05-15;**录用日期:**2024-05-20。
基金项目:国家自然科学基金资助项目(62276091);河南省科技攻关项目(232102210132)
作者简介:邓淼磊(1977—),男,河南南阳人,教授,博士,CCF杰出会员,主要研究方向:信息安全、物联网;　阚雨培(2000—),男,河南南阳人,硕士研究生,CCF会员,主要研究方向:信息安全、入侵检测;　孙川川(1998—),男,河南郑州人,硕士研究生,CCF会员,主要研究方向:深度学习、信息安全;　徐海航(1999—),河南周口人,男,硕士研究生,CCF会员,主要研究方向:深度学习、入侵检测;　樊少珺(2001—),女,河南南阳人,硕士研究生,CCF会员,主要研究方向:深度学习、入侵检测;　周鑫(1999—),男,河南郑州人,硕士研究生,CCF会员,主要研究方向:深度学习、信息安全。

安全领域带来了新的可能性。然而，当处理大规模或高维网络数据时，它们的检测性能将显著下降，检测所需时间将显著增加。因此，由于流量和带宽的增加，ML方法在现代互联网环境中可能显得效果不佳。另一方面，深度学习（Deep learning，DL）技术在处理互联网日益复杂的入侵检测问题方面更有效。与传统的机器学习技术相比，深度学习方法更擅长处理大数据，以其多层次的神经网络结构能够自动从原始数据中提取抽象和高级别的特征。此外，深度学习方法可以从原始数据中自动学习特征表示，使得模型更具适应性和泛化能力。随着深度学习技术的发展，将深度学习应用在入侵检测系统中逐渐成为一种趋势[9]，如自编码器（AutoEncoder，AE）[10]、生成对抗性网络（Generative Adversarial Network，GAN）[11]、卷积神经网络（Convolutional Neural Network，CNN）[12]、长短时记忆（Long Short Term Memory，LSTM）网络[13]等深度学习模型，已在入侵检测领域展现出卓越的性能和潜力。

1 入侵检测系统的分类

入侵检测系统（IDS）是计算机安全领域中的重要应用程序，旨在监视和识别各种安全违规行为[14]。对于入侵检测系统来说，入侵行为是指试图以非法或未经授权的方式访问有关计算机系统的信息或破坏系统操作。入侵检测系统根据所检测数据来源的不同，可以分为基于主机的入侵检测系统和基于网络的入侵检测系统。由于互联网的发展，研究人员对网络入侵检测系统的研究也越来越重视，为此研究人员将深度学习算法应用于网络入侵检测，以进一步提高其性能，因此本文主要针对网络入侵检测进行研究调查。另外，根据其检测技术，入侵检测方法又分为基于误用的检测方法和基于异常的检测方法[9, 15]。其中误用检测方法通过将事件和流量与已知攻击标志数据库相匹配，从而判断是否存在攻击行为，但是这种方法无法检测未知的攻击。另一方面，异常检测方法试图学习正常行为规律并将其他一切识别为异常或入侵。但这种方法还存在着较高的误报率，因此研究人员将深度学习技术应用于异常入侵检测的研究中，从而降低入侵检测误报率。具体分类框架如图1所示。

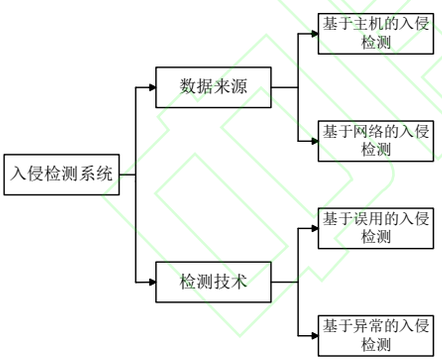

图1 入侵检测系统的分类框架

Fig. 1 Classification framework for intrusion detection systems

本文主要针对网络入侵检测进行研究调查，根据基于网络的入侵检测系统提供的功能，其组成部分如图2所示。通过监控网络，从网络数据包中收集信息。攻击者通过注入恶意代码或分析网络数据包获取信息来实施网络攻击。攻击既可能发生在处理所有网络事务的服务器上，也可能发生在实际执行网络活动的系统主机上。也可以利用系统中存在的漏洞进行攻击。事实上，深度学习等技术可以让基于网络的入侵检测系统更智能地检测网络威胁[16]。

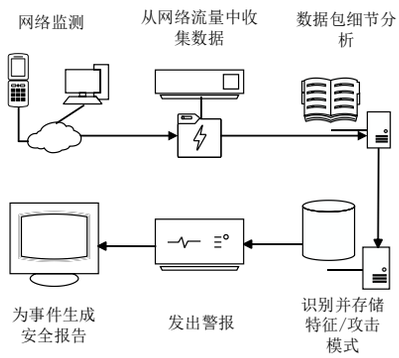

图2 网络入侵检测系统的工作流程

Fig. 2 The workflow of a network intrusion detection system

IDS的组成部分如下：

1）网络检测：需要对网络进行监控，以收集包含网络相关信息的必要数据包。网络数据包由数据包头和数据包有效载荷组成。包头和有效载荷都可用于提取进行攻击所需的信息。即使对网络流进行分析，也是为了找到可用于实施攻击的数据模式。因此，为入侵检测建立的数据集具有数据包级和流量级特征，可对攻击进行分类。2）数据收集：它指的是收集要进行攻击的目标系统的详细信息。这可以通过使用网络命令或工具进行查询来实现。例如，使用"Wireshark"嗅探流经网络的数据包，或使用"nslookup"等网络命令获取域名等与服务器和主机相关的详细信息，就能获得数据包级的详细信息。3）分析数据包细节：这可称为扫描网络数据包以窃取机密信息。例如，R2L（Remote to Local）攻击可通过入侵系统和未经授权访问系统来实施。为获取访问权而实施的一些攻击包括嗅探数据包并窃取凭据，或注入木马等恶意软件，以获取系统的远程访问权。通常情况下，这些类型的漏洞只有在目标系统有只有当目标系统开放的端口很少时，这些类型的漏洞才能被利用。4）识别和存储签名/攻击模式：分析数据包详细信息后的下一步是识别已知攻击和新型攻击的攻击模式，或识别可用于发起内部攻击的某些已知漏洞的签名。这些签名和模式会存储在数据库中，供今后参考；因此，如果发现异常，安全管理员可以轻松报告入侵行为。5）生成警报：识别攻击模式后，将生成警报并报告给安全管理员。警报根据签名/模式的匹配情况触发。

1.1 基于数据来源的分类

入侵检测系统根据所检测数据来源的不同，可以分为基于主机的入侵检测系统和基于网络的入侵检测系统。基于主机的入侵检测（Host-based Intrusion Detection System，HIDS）[17]通过检查防火墙、服务器或数据库日志来检查、分析、收集和监视网络和主机网络内的数据动作，以识别任何异常或可疑的行为。与基于网络的入侵检测系统相比，HIDS更加专注于监视主机内部的行为，能够提供更加细粒度和精确的检测。基于网络的入侵检测（Network-based Intrusion Detection System，NIDS）[18]通过检测网络数据包，解析数据包的内容来判断网络中是否有攻击行为。NIDS使用软件或硬件监视和分析网络通信，它可以监视整个网络中的数据流量，并且与跨网络和外部防火墙的多台主机协同工作，以提高入侵检测的覆盖范围和准确性。相较于基于主机的入侵检测系统，NIDS能够更全面地监视整个网络环境，对网络中的异常行为进行及时发现和防范。

表1 基于主机和基于网络的入侵检测系统的区别

Tab. 1 Differences between host based and network based IDS

特点	数据来源	部署方式	检测效率	适用性	局限性
基于主机的IDS	操作系统或应用程序的日志	每台主机；依赖于操作系统；难以部署	低，必须处理大量日志	适用于监测主机本地活动	无法分析网络行为
基于网络的IDS	网络流量	关键网络节点；易于部署	高，可真实的实时检测攻击	适用于监测网络流量和通信	仅监控通过特定网段的流量

1.2 基于检测技术的分类

基于误用的入侵检测(Misuse-based Intrusion Detection System, MIDS)[19],通过将网络流量与已有的攻击特征库匹配来判断入侵行为。它维护一个签名数据库,以记录各种攻击和恶意活动,然后对实时数据进行监视和比对,以识别是否存在与已知攻击模式相匹配的行为。基于异常的入侵检测(Anomaly-based Intrusion Detection System, AIDS)[20],通过分析系统中的正常活动以创建行为档案,确定这些活动的特征,并进行定量描述,当用户行为偏离正常记录时,就将这些行为活动定义为攻击。它包括两个主要阶段,即训练阶段和检测阶段。在训练阶段,特征构建模块从主机或网络中收集数据,并对其进行预处理以构建特征。训练模块使用这些特征来生成行为模型。该模型将数据分类为正常或异常(入侵)行为。这种技术可以检测新的攻击,但需要更多的计算能力。误用检测和异常检测之间的主要区别在表2中列出。

表2 基于误用和基于异常的入侵检测系统的区别

Tab. 2 Differences between IDS based on misuse and anomaly

特点	检测性能	检测效率	数据要求	可解释性	未知攻击
基于误用的IDS	误警率低;漏警率高	高;随着特征数据库规模的扩大而降低	几乎所有的检测都依赖于已知的攻击数据	基于领域知识的设计,解释能力强	仅检测已知攻击
基于异常的IDS	低漏警率;高误报率	取决于模型复杂性	低,只有特征设计依赖于攻击数据	仅输出检测结果,解释能力弱	检测已知和未知攻击

2 数据集与评价指标

入侵检测系统需要通过网络流量数据集与特定评价指标对系统性能进行评估。本节对基于深度学习的网络入侵检测系统中常用的数据集与评价指标进行介绍。

2.1 数据集

随着入侵检测技术的不断发展,越来越多的相关数据集出现供研究人员使用。常用的主要有KDD99,NSL-KDD, UNSW-NB15, CIC-IDS-2017等。大多数基于深度学习的网络入侵检测系统使用上述数据集进行测试。

KDD99[21]主要包括4类网络攻击,分别为拒绝服务(Denial-of-Service, DoS)攻击、远程到本地(R2L)攻击、端口扫描(Probe)攻击和用户提权(User to Root, U2R)攻击.该数据集包含490万个单个连接向量,以及它的41个特征,可以将其描述为攻击或正常。KDD99是最早用于入侵检测模型训练与测试的公共数据集之一,也是最广泛用于入侵检测领域使用的数据集之一。然而该数据集存在许多缺陷,如部分记录重复、严重的类别不平衡等,因此KDD99不能完全反映出当前网络攻击的特征。

NSL-KDD[22]它是为了解决KDD Cup1999数据集中的缺点而开发的。此外,该数据集由于冗余记录很少而受到青睐。这也有助于减少由冗余数据记录引起的分类步骤中的偏差,从而有助于提高性能。虽然NSL-KDD有很多方面的改进,但该数据集仍然具有一定的局限性,无法反映真实世界网络环境中的流量数据。

为了解决KDD99与NSL-KDD不能反映真实网络流量数据和攻击这一问题,有学者设计了UNSW-NB15[23]该数据集由基于数据包格式的网络流量组成,包括超过250万条记录与49个特征,2218761个良性流(87.35%)和321283个攻击流(12.65%)。其中包含模糊攻击、后门攻击、拒绝服务攻击、蠕虫攻击等9种攻击类型,适合用于训练和测试。

CIC-IDS-2017[24]是加拿大网络安全研究所(Canadian Institute for Cybersecurity, CIC)提出的一个网络数据集,在模拟环境中使用CicFlowmeter对每个流提取80个特征到PCAP和CSV文件中5天。其中包含7种网络攻击,分别为DoS(Denial of Service)攻击、SSH(Secure Shell)暴力攻击、僵尸网络攻击、DDoS(Distributed Denial of Service)攻击、Web攻击、心血漏洞及渗透攻击。

2.2 评价指标

基于深度学习的网络入侵检测系统主要采用以下指标评价系统性能,例如,Accuracy、Precision、Recall和混淆矩阵等来执行评估。与其他分类问题一样,IDS的混淆矩阵包括真阳性(True Positive, TP)、假阳性(True Positive, FP)、真阴性(True Negative, TN)和假阴性(False Negative, FN)等术语。在IDS分类任务中,TP、FP、TN和FN通常分别指正确分类为攻击的攻击数据、错误分类为攻击的正常数据、正确分类为正常的正常数据和错误分类为正常的攻击数据[15]。误报率和漏报率是衡量入侵检测系统效率的两个重要指标。以下是IDS研究中常用的评价标准和计算公式。

1)准确率(Accuracy):正确分类的样本所占的比率。

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

2)精确率(Precision):被预测正确的良性样本所占的比率。

$$\text{Precision} = \frac{TP}{TP + FP}$$

3)召回率(Recall):被正确预测为良性样本的数据与所有良性样本数据的比率。

$$\text{Recall} = \frac{TP}{TP + FN}$$

4)误报率(False Positive Rate,FPR):被错误判断为攻击样本的数据与所有实际良性样本数据的比率。

$$\text{FPR} = \frac{FP}{FP + TN}$$

5)漏报率(False Negative Rate,FNR):被错误判断为良性样本的数据与所有实际攻击样本数据的比率。

$$\text{FNR} = \frac{FN}{FN + TP}$$

3 基于深度学习的入侵检测技术

深度学习是机器学习的一种演变,源于人工神经网络(Artificial Neural Networks, ANN)。它由不同的层构成深度神经网络(Deep Neural Networks, DNN)。深度学习是一种拥有两层以上神经网络的机器学习算法,适用于复杂概念和关系的建模。目前,深度学习正被应用于不同的研究领域,如图像识别、语音识别、自然语言处理、社交网络过滤等。深度学习算法的不同之处在于,除了能同时完成特征学习和分类或聚类任务外,还能找到不同来源的大规模数据之间的相关性[25]。深度学习架构主要分为三类:生成式架构、判别式架构和混合式架构[26]。在基于深度学习的IDS中,深度神经网络可以自动降低网络流量的复杂度来发现数据之间的相关性,而无需人工干预。因此,可以利用大量历史数据对深度学习模型进行训练,建立异常检测模型。基于深度学习的网络入侵检测系统的结构如图3所示。根据不同的深度学习方法,本节将对基于深度学习的入侵检测技术进行介绍。

3.1 生成式架构

生成式(或无监督)深度学习架构可以从无标签的原始数据中自动学习,以完成不同的任务。还能够捕捉数据之间的内在联系和结构,因此它们能够检测到与已知分布不一致的样本,从而识别出潜在的异常行为。总之,生成式方法在入侵检测系统中具有广泛的应用前景,能够帮助提高检测的准确性和鲁棒性,对于应对复杂多变的网络安全威胁具有重要意义。以下是这一类别中最常见的深度学习方法。

1)循环神经网络(Recurrent Neural Network,RNN)。

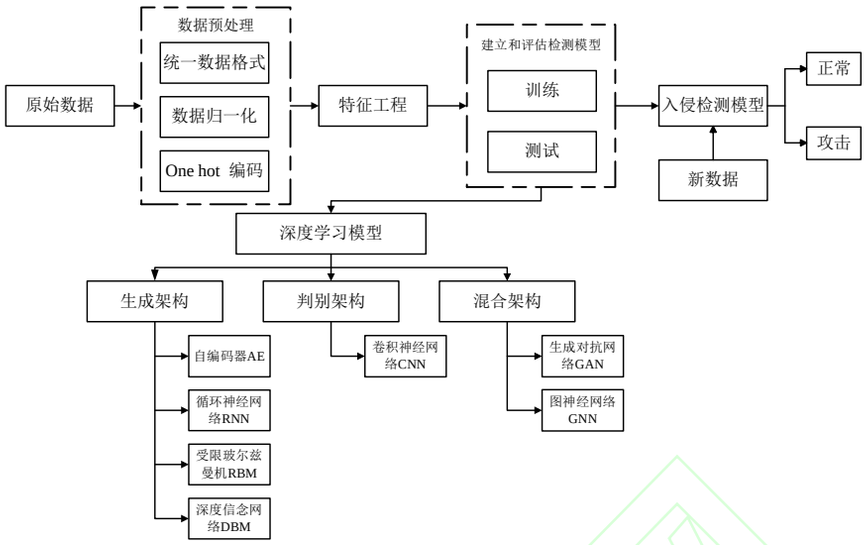

图3 基于深度学习的IDS的总体架构

Fig. 3 Overall architecture of IDS based on deep learning

循环神经网络是于1982年提出的一种动态前馈神经网络。RNN之所以被称为递归，是因为它们对序列的每个元素执行相同的任务，其输出取决于先前的计算，循环神经网络（RNN）可以利用数据的序列信息，提取时序特征，非常适合应用于与序列相关的入侵检测问题。长短期记忆（LSTM）网络和门控循环单元（Gated Recurrent Unit，GRU）是为了克服传统RNN在反向传播过程中所面临的“梯度消失或爆炸”问题而设计的。长短期记忆网络对时间序列中间隔和延迟长的事件有较强的处理能力。门控循环单元是LSTM的轻量级版本，进一步简化了结构，较少的参数也让训练更容易。

Sharafaldin等[27]提出了一种IDS框架该框架，使用不同类型的RNN，即LSTM）网络，门控循环单元（GRU）和简单RNN。在这项研究中，使用基于XGBoost的特征选择算法，以减少每个数据集的特征空间。结果表明，对于使用NSL-KDD的二分类任务，XGBoost-LSTM实现了最佳性能，测试准确率（Test Accuracy，TAC）为88.13%，验证准确率（Validation Accuracy，VAC）为99.49%。对于UNSW-NB15，XGBoost-Simple-RNN是最有效的模型，TAC为87.07%。对于多类分类方案，XGBoost-LSTM在NSL-KDD上实现了86.93%的TAC，XGBoost-GRU在UNSW-NB15数据集上获得了78.40%的TAC。为了提高检测少数攻击类的性能，Wei等[28]利用SMOTE（Synthetic Minority Oversampling Technique）方法生成少数类的代表性样本，缓解了网络流量的不平衡问题，然后采用双向长期记忆网络（Bidirectional Long-Short Term Memory，BiLSTM）进行初步特征提取，多头注意（Multi-Head Attention，MHA）进一步捕获网络流量的特征和全局信息，全连接层（Full-Connected Layer，FCL）模块进行最终分类。为了解决在训练过程中的梯度消失问题，Donkol等[29]提出了利用似然点粒子群算法用于特征选择和增强的长短期记忆技术与RNN结合用于分类，构建一个入侵检测模型，该模型解决了梯度消失的问题。由于物联网数据量大，以及深度学习模型的计算需求，导致通信开销过大，阻碍了深度学习模型在检测针对物联网的网络入侵方面的应用。Syed等[30]提出了一种新的基于雾云的物联网入侵检测框架，该框架结合了分布式处理大规模BoT-IoT数据集，根据攻击类别和时间序列的特征选择步骤分割数据集，特征选择步骤减少了90%的数据集大小。随后用SimpleRNN和Bi-LSTM模型进行分类。为了避免不适当和冗余的特征减慢分类过程和导致错误决策来影响IDS的性能，Mushtaq等[31]提出了一种由深度自编码器（AE），LSTM和Bi-LSTM组成的混合入侵检测框架，利用AE获取最优特征，然后LSTM将样本分为正常样本和异常样本。在NSL-KDD数据集上，AE-LSTM分类准确率为89%。然后，相同作者又提出了一种入侵检测系统（AE-GRU）[32]，该系统使用自编码器提取相关的特征和门控循环单元（GRU）进行流量类型分类。实验结果表明，AE-GRU 在NSL-KDD，UNSW-NB15 数据集上分别取得了 89.54%，88.39% 的准确率。Kanna 等[33]提出了基于 MapReduce 的黑寡妇优化卷积-长短期记忆（BWO-CONV-LSTM）网络模型，网络模型是 CNN 和 LSTM 神经网络的组合，结合了两个网络的优点，能以最小的复杂度学习时空特征，模型的超参数通过 BWO 进行优化。实验结果表明，BWO-CONV-LSTM 模型对 NSL-KDD、ISCX-IDS、UNSW-NB15 和 CSE-CIC-IDS2018 数据集具有较高的入侵检测性能，准确率分别为98.67%、97.003%、98.667% 和 98.25%，并且具有更少的假值、更少的计算时间和更好的分类系数。UDAS P B 等[34]提出了一种网络异常检测模型SPIDER。SPIDER模型结合了传统RNN的4个更新版本，即双向长短期记忆网络（Bi-LSTM）、LSTM网络、双向门控循环单元（Bidirectional Gated Recurrent Unit，Bi-GRU）和GRU。混合模型由几个卷积层提取空间流量特征和四个增强的 RNN 层组合而成，这些层中的每一层的数量和位置已被选择以获得最佳可能的结果。

2）自编码器（Auto-Encoder，AE）

自编码器通常用于通过产生比原始数据输入更好的数据表示来降维。AE 将编码器和解码器结合在一起，并使用反向传播将它们训练在一起。编码器提取原始特征，并通过将输入转换为低维抽象来学习数据表示。然后，解码器接收低维表示并重建原始特征自编码器主要用于数据的降维。随着入侵检测系统需要处理的复杂数据的迅速增长，对大规模数据的处理成为入侵检测系统面临的挑战之一，自编码器被广泛地用于入侵检测中的降维任务。

Wang等[35]为了针对云计算环境下的网络流量具有大规模、高维度、高冗余的特点，基于堆叠胶囊自编码器和支持向量机分类算法，设计了一种新型的云入侵检测系统SCAE-SVM。使用堆叠胶囊自编码器（Stacked Capsule AutoEncoder，SCAE）从原始网络数据中自动提取基本特征，并将其输入到SVM中，以有效识别攻击。在KDDCup 99和NSL-KDD数据集上，该方法展示了较高的检测性能。MUHAMMAD G等人[36]利用堆叠AE以无监督的方式学习输入网络记录的特征，以减小特征维度。然后用监督的方式训练DNN，以有效检测攻击。该方法在三个公开可用的数据集：KDDCUP99、NSL-KDD和AWID上进行了评估。实验结果表明，该入侵检测系统的多分类准确率分别为94.2%、99.7%和99.9%。BALASUBRAMANIAM S等人[37]为了减少分布式拒绝服务攻击（Distributed Denial of Service，DDos）对云计算造成的破坏和影响。通过结合梯度下降和基于领导者的优化算法（Hierarchical Leader-BASED Optimization，HLBO）提出了一种优化算法GHLBO，该优化算法负责训练一个深度堆叠的自编码器，以有效的检测攻击。训练之前通过具有重叠系数的深度最大输出网络

进行特征提取,并且通过过采样进行数据增强。该方法在BOT-IoT数据集上进行评估,如真阳性率(True Positive Rate, TPR),真阴性率(True Negative Rate, TNR),和测试准确度分别达到90.9%,90.9%和91.7%。Liu等[38]为了解决在真实的工业物联网环境中数据不平衡的问题。考虑引入变分自编码器(Variational Autoencoder, VAE)和条件变分自编码器(Conditional Variational Autoencoders, CVAE)来生成符合原始数据分布的"新"样本,以平衡数据集。分别构建了三种基于数据的研究方案:基于VAE的数据增强方案、基于条件VAE的数据平衡方案以及基于随机欠采样和CVAE的数据平衡方案。通过CSE-CIC-IDS2018数据集构建实验,以验证三种数据处理方案的有效性。经过第三种方案的数据增强后,基于卷积神经网络的IDS模型的宏F1得分提高了3.75%,基于门控循环单元的IDS模型的宏F1得分提高了5.32%。MQTT(Message Queuing Telemetry Transport)是物联网系统中广泛使用的网络协议,为了检测MQTT物联网应用中的未知入侵,Boppana等[39]提出了一种基于生成对抗网络(GAN)和自编码器的无监督入侵检测模型。该模型基于GAN的对抗损失,以更新自编码器的参数和重构损失。在公共MQTT数据集MQTT-IoT-IDS2020上与其他流行的无监督模型比较,即自编码器,单类支持向量机(One-Class SVM, OCSVM),隔离森林(Isolation Forest, IF),GAN-AE的性能优于其他模型,检测准确率达到97%。VAIYAPURI T等人[40]进行了不同AE变体的一类无监督入侵检测的比较评估,研究的AE评估包括堆叠自编码器、稀疏自编码器、降噪自编码器、压缩自编码器和卷积自编码器,5种不同的AE变体。在公共基准数据集NSL-KDD和UNSW-NB15上进行比较的五种AE变体中,压缩自编码器在NSL-KDD和UNSW-NB 15中的ACC、AUC和F1方面产生最佳检测性能。

3)受限玻尔兹曼机(Restricted Boltzmann Machine, RBM)

RBM是于1986年提出的一种单向模型,旨在解决玻尔兹曼机的复杂性所带来的问题。RBM背后的原理是消除同一层神经元之间的联系。RBM能从原始数据中学习特征的深层次信息,因此在入侵检测任务中被广泛应用。

Coli等[41]开发了一种基于深度高斯-伯努利受限玻尔兹曼机的物联网分布式拒绝服务检测模型。因为该模型能够按照无监督方法从输入中学习高级特征,所以用于NSL-KDD数据集的特征学习,最后用Softmax回归进行攻击检测。模型在NSL-KDD数据集上的二分类,多分类的准确率分别是93.52%,91.69%。ROSA G H D等人[42]使用受限玻尔兹曼机作为自编码器-解码器,将原始特征投影到新的特征空间中,并使用不同的分类器对其进行进一步分类。通过对RBM设置10、20、38、80、100等不同数量隐藏神经元,提取不同的特征。实验结果表明,对于带有径向基函数核的支持向量机(SVM)、决策树(DT)和随机森林(RF)三种不同的分类器,不同数量的投影特征实现了不同的最佳结果。HONGL等人[43]面对海量的非线性数据,传统的入侵检测算法存在特征提取不足、分类模型不准确等问题。为此,提出了一种基于受限玻尔兹曼机(RBM)和延迟决策的入侵检测方法。选择RBM对数据集进行特征提取,对于不能立即分类归类到边界域的行为,在分类决策阶段进行延迟决策,然后对该领域的行为重复特征提取过程,构造不同粒度的特征空间,最后输出分类结果。实验结果表明,该方法在NSL-KDD数据集上的准确率为96.1%。Mayuranathan等[44]针对传统的云平台入侵检测系统对DDoS攻击存在检测精度低、计算复杂度高的问题。使用随机和声搜索优化模型,选择最佳的特征集,使用受限玻尔兹曼机来检测DDoS。在KDD99数据集上进行了测试。实验结果表明,该模型达到准确率99.92%。

4)深度信念网络(Deep Belief Network, DBN)

深度信念网络是一种具有深层架构的神经网络,是由堆叠的RBM组成,它通过无监督算法对每一层RBM进行训练,每个RBM都是在前一个RBM的基础上训练的,其中RBM的每个隐藏层都被认为是下一个RBM的输入。它是一个特征学习的过程,可以解决涉及高维数据的问题,已经被应用于入侵检测领域。

Zhang等[45]提出了一种结合流量计算和深度学习的网络攻击检测方法。该方法由两部分组成:基于流量计算和频繁模式的实时检测算法和基于深度信念网络和支持向量机(DBN-SVM)的分类算法。该方法利用滑动窗口挖掘频繁模式形成模式库,快速检测数据流中是否存在恶意行为,并能方便地增量更新模型。然后,采用基于多层非线性映射的DBN深度学习方法对高维非线性原始数据进行特征降维,以减少特征向量的数量,保留重要数据特征。然后,利用多个SVM分类器对攻击进行分类。其中通过滑动窗口流数据处理使得实时检测,DBN-SVM算法可以提高分类精度。在CICIDS 2017数据集,进行了一系列对比实验。该方法的实时检测效率高于传统的机器学习算法。攻击分类准确率比DBN提高0.7个百分点,比集成算法boost和bagging方法提高2个百分点。Chen等[46]提出了一种基于深度信念网络(DBN)和长短期记忆(LSTM)网络的高效NBAD算法。首先,使用DBN的非线性特征提取方法被应用于自动提取特征,并在保证精度的同时降低原始数据的维数。然后,使用轻结构LSTM网络来获得分类结果。在构建LSTM网络时,将提取的KDD99数据的特征放进LSTM网络中,发现4层LSTM获得最佳性能的结构。Sarkar等[47]研究采用改进松鼠搜索算法和改进的深度信念网络(Modified Deep Belief Network, MDBN)对UNSW-NB15数据集进行异常检测,提出了更好、更快的入侵检测方法。松鼠搜索算法从一组特征中提取相关特征来处理高维网络流量数据。它选择相关和最优的特征子集用于训练过程和测试过程。同时通过MDBN算法对提取的特征进行异常检测,进行二值分类和多类分类。MDBN还有助于处理数据集的不平衡特性。将所提出的IDS模型与现有的其他方法进行了比较,所提出的方法获得了99.79%的最高精度和0.02%的最低FAR。Alissa等[48]采用Jaya优化算法进行特征选择,从而降低了计算复杂度。另外,该文献提出的FSHDBN-CID模型利用HDBN模型进行分类。最后,将鸡群优化技术应用于HDBN方法的超参数优化。实验对比研究表明,FSHDBN-CID模型比其它模型有较大的改进,其精度为99.57%。

3.2 判别式架构

判别式(或监督)架构主要应用于标记数据以区分预测任务的模式。其通过学习从输入数据到标签的映射关系,即学习如何根据输入数据的特征对其进行分类。在入侵检测系统中,判别式方法能够从已知的数据样本中学习到正常和异常行为之间的差异,从而实现对未知数据的分类和判别。与生成式方法相比,判别式方法更加专注于学习数据的类别信息,不关注数据的潜在分布,因此在训练过程中更加高效,并且能够提供更加精确和可靠的分类结果。在应对入侵检测的任务中,判别式方法通常表现出较好的性能,尤其适用于处理大规模和高维度的网络数据,能够快速准确地识别出潜在的安全威胁。

卷积神经网络(CNN)是典型的判别式有监督方法,它由输入层、卷积层、池化层、完全连接层和输出层组成,不同结构的CNN具有不同数量的卷积层和池化层。近年来,由于CNN具有处理复杂数据的能力,它们也被用作入侵检测的特征提取器和分类器。

Kanumalli等[49]利用CNN和双向LSTM的优点,建立了一个深度学习系统来学习数据的时空属性。通过CNN发现数据集的结构或高级属性,而BiLSTM用于训练数据长期,短期的时间属性,然后集成它们来预测攻击。Chen等[50]提出了一种用于入侵检测系统的多目标进化卷积神经网络,称为MECNN。该方法将CNN作为入侵检测的分类器。首先提出了一种新的编码方案,将CNN的拓扑结构转化为MOEA/D染色体,然后利用MOEA/D对CNN模型的检测性能和模型复杂度同时进行优化。然后,将最合适的MECNN模型部署在雾计算的不同雾节点,为物联网提供低时延、高精度的入侵检测。Wu等[51]提出了一种基于模糊粗糙集、生成对抗网络(GAN)和卷积神经网络(CNN)的智能入侵检测算法。首先提出了一种基于模糊粗糙集的算法来选择最优特征子集。然后,设计了一种基于CNN的入侵检测方法,并对其进行了初步训练。GAN利用生成器对网络数据进行扩展,并将生成的数据与实际数据相结合,对鉴别器进行训练。此外,将训练好的CNN和GAN相结合,构造DCGAN,该DCGAN在扩展训练数据的同时,还具有高效的特征提取能力。最后,将该方法与现有的方法进行了比较。实验结果表明,比现有的方法提升了高达4%的准确

率。Ullah等[52]提出了一种基于Transformer的迁移学习的网络流量不平衡入侵检测系统。该系统使用基于Transformer的迁移学习来学习网络特征表示和不平衡数据中的特征交互。采用合成少数过采样技术(SMOTE)来平衡异常流量,检测少数攻击。通过卷积神经网络(CNN)模型从均衡的网络流量中提取深层特征。最后,提出了卷积神经网络-长短时记忆网络混合模型(CNN-LSTM)来从深层特征检测不同类型的攻击。此外,利用CNN-RNN和CNN-GRU进行基线实验,IDS-INT以99%的准确率、100%的召回率、99%的F1评分和99.21%的准确率优于基线方法。Ren等[53]提出了一种新的分层CNN-Attention网络—CANET。在CANET中,CNN和Attention机制相结合,形成一个CA块,专注于局部时空特征提取。多层CA块组合能够充分学习网络攻击数据的多层次时空特征,更适合现代大规模网络入侵检测系统。大量的实验表明,CANET在准确率、检测率和误报率方面都优于目前最先进的方法。有效地提高了少数群体的检出率。EL-GHAMRY A等人[54]提出了一种基于CNN模型的农业物联网网络入侵检测系统。该方法首先对NSL KDD数据集进行几个预处理步骤。采用递归特征消除法(Recursive Feature Elimination,RFE)选取重要特征,然后将其转换成方形彩色图像。输入图像通过不同的CNN模型来学习,例如VGG16、Inception和Xception模型。利用精确度、F1分数、查全率和精确度指标对CNN模型与经典机器学习算法的性能进行了比较。最后,选择性能最好的CNN模型进行超参数优化,以实现数据集与模型之间的最优拟合。CHEN C等人[55]针对现有入侵检测模型特征提取过程复杂,信息提取不足的缺点,提出了一种入侵检测模型FCNN-SE。利用融合卷积神经网络(FCNN)提取数据集的多维特征并构造新的数据集,采用基于叠加的集成学习方法进行入侵检测。PINGALE S V等人[56],首先,在预处理阶段,使用缺失值估算方法创建完整的数据集。然后,利用全熵方法(Holoentropy)对预处理后的数据进行维数变换。接着从变换后的数据中提取CNN特征,然后基于堪培拉距离(Canberra distance)进行特征选择。最后将选择的特征送到入侵检测阶段,以识别网络入侵。检测是使用一个深度MAXOUT网络进行的,该网络的权值和训练参数是用REMORA优化算法修改的。所提出的模型提供了更好的结果,其测试AC值为0.945。

3.3 混合式架构

混合式深度网络方法结合了生成式方法和判别式方法,主要有生成对抗网络(Generative Adversarial Networks,GAN)和图神经网络(Graph Neural Networks, GNN)。

GAN是一种混合深层架构,包含两个神经网络,即生成器和判别器。GAN依赖于一个极小极大博弈,其中一个网络寻求最大函数值,另一个网络试图最小化函数值。在每个对抗性回合中,生成器从噪声中产生随机样本。然后鉴别器接收随机数据和实际样本,并试图区分它们。通常情况下,网络中的异常流量远少于正常流量,GAN能生成新数据,因此能用来解决入侵检测中数据类别不平衡的问题。

Park等[57]研究了基于重构误差和Wasserstein距离的生成对抗网络,以及自编码器驱动的深度学习模型。系统依次训练生成模型和自编码器模型,其中训练的生成模型用于训练自编码器模型。最后,系统通过应用训练好的生成模型和训练好的自编码器的编码器来训练预测模型,其中生成模型用于生成少数类数据,编码器用作特征提取器。实验结果表明,该模型在NSL-KDD数据集和UNSW-NB15数据集上的准确率分别达到了93.2%和87%,特别是,所提出的模型在检测NSL-KDD数据集中的R2L和探针类攻击表现出显着的性能。Yuan等[58]提出了一种称为B-GAN的数据平衡方法。它基于生成对抗网络,用于解决数据不平衡问题。由于入侵检测的数据集是连续建立的,因此B-GAN的生成器和鉴别器采用长短时记忆(LSTM)网络模型,它们可以更好地捕捉数据的特征,生成高质量的异常样本。通过对比在原始数据集和B-GAN方法平衡后的数据集的性能,实验结果表明,这些不同的入侵检测模型的性能得到了不同程度的提高。Zhu等[59]提出了一种基于辅助分类器的生成对抗网络的网络入侵检测策略。它用生成对抗网络模拟少数类数据在一定有界区间内的特征分布,并通过对抗训练不断逼近真实数据分布,获得大量可选择的训练数据,实现少数类数据增强。从而解决了分类问题中由于数据类别和数量分布不均衡而导致的分类不足和检测遗漏的问题。利用入侵检测数据集NSL-KDD进行了数据扩展实验。模型在优化后的结果的查准率和查全率远高于未经处理的直接分类的查准率和查全率。其中宏平均精度率从0.72提高到0.99,宏平均精度率提高幅度为37.50%。宏观平均召回率从0.75提高到0.99,宏观平均召回率提高幅度为32%。

深度学习(DL)在检测网络攻击方面表现出了令人印象深刻的结果,因为它们能够从平面数据中学习可泛化模式。然而,平面数据无法捕获攻击的结构性行为,这是有效检测的必要条件。相反,图结构提供了一个更加健壮和抽象的系统视图,攻击者难以逃避。最近,图神经网络(GNN)成功地从图结构数据提供的语义中学习到有用的表示。因此GNN方法也被成功地应用于入侵检测中。

Lo等[60]提出了一种基于GNN方法的E-GraphSAGE,它可以同时捕捉图的边缘特征和拓扑信息,用于物联网网络中的网络入侵检测。在根据入侵检测数据集构建图数据时,节点由IP地址和端口标识,而边表示两个节点之间的数据流。实际的流特征存储在边中,不像原始的GraphSAGE模型只使用节点特征。将E-GraphSAGE应用于四个物联网的入侵检测数据集最高取得了99.99%的准确率。与E-GraphSAGE相比,Lan等[61]提出的E-minBatch GraphSAGE算法具有更多的输入节点数,能够适应更复杂的网络结构。E-MinBatch GraphSAGE与E-GraphSAGE算法的区别在于聚合函数,E-MinBatch GraphSAGE聚合的不是周围相邻节点的信息,而是周围边缘信息的聚合。该模型的性能与原始的E-GraphSAGE在UNSW-NB15数据集上进行了比较,其中在二分类和多类分类任务中的准确性和F1得分都略有提高。对E-GraphSAGE的另一个改进由CHANG L等人[62]提供,在E-GraphSAGE的输出层增加了剩余连接,添加剩余连接作为处理高类不平衡的策略,目的是保留原始信息,提高少数类的性能。在此解决方案中观察到的改进的启发下,又提出了基于边缘的残差图注意网络(E-ResGAT)。两个模型在TON-IOT数据集的多分类下准确都比E-GraphSAGE有不同程度的提高。E-GraphSAGE的作者还通过将其应用于自监督方法,对模型进行了重要改进。这种名为Anomal-E[63]的新方法利用了相同的图结构(即流和端点分别表示边和节点)而不需要任何标签。选择E-GraphSAGE作为编码器来计算正边缘嵌入、全局图摘要和负边缘嵌入和修改过的深度图信息最大化(Deep Graph Infomax,DGI)方法用来最大化潜在空间中输入的不同部分之间的局部边缘信息以进行自监督学习。与E-GraphSAGE相比,该方法不需要任何标签,这使得该解决方案更适用于现实世界的场景。然而,大多数GNN方法都局限于考虑节点特征或边缘特征。ALTAF T等人[64]提出一个节点边图卷积网络(NE-GCONV)框架,该框架引入了一种同时具有节点和边特征的图结构,克服了这一局限性。实验结果表明,该模型在准确率和误报率方面优于其他GNN模型,并且计算效率高。DUAN G等人[65]提出了一种基于动态线图神经网络(DLGNN)的半监督学习入侵检测方法。该模型将网络流量转换成一系列的时空图。该方法进一步利用网络空间的自然拓扑结构和信息的主机到主机通信的交互演化,可以更有效地学习、分析和总结流量数据的特征,以基于更少的标记样本来有效地区分网络中的恶意行为。ZHANG Y等人[66]设计了一个新的框架-图入侵检测(GID)来实现入侵检测。首先将入侵检测任务转化为图节点分类任务。然后将类多头加权余弦相似度与网络重构技术的一些概念相结合,学习更好的图结构,同时保证图的光滑性、连通性和稀疏性。其次,利用图卷积网络(Graph Convolutional Network, GCN)来完成前面构造的数据图的表示学习任务。最后,将图学习和GNN参数优化结合到一个双层学习框架中,同时学习用于入侵检测的图和GNN参数。实验结果表明,该方法在小训练集和不平衡类别数据上具有显著的优势。Wang等[67]提出一种基于图注意力网络(Graph Attention Network, GAT)的基于行为相似度的图神经网络算法。首先,通过分析实际数据集的特点,提出了一种基于行为相似度的图构造方法。将数据流视为图中的节点,并将节点的行为规则用作图中的边,从而

构造每个节点具有相对均匀数量的邻居的图。然后,将边行为关系权值引入图注意力网络,利用数据流之间的关系和图的结构信息,提高网络入侵检测的性能。

3.4 不同类型入侵检测模型分析比较

深度学习技术的应用将入侵检测系统推向新的发展阶段,这些技术可用于网络入侵检测的特征提取和分类任务。相对于传统机器学习方法,深度学习在处理海量高维度网络流量数据时表现出更高的效率和检测准确率。表3列出了本调查中基于深度学习的IDS的部分论文。可以看出,大多数模型在数据集上测试时都取得了良好的准确率,KDD 99和NSL-KDD数据集仍然被广泛使用。

表3 多种入侵检测模型的性能比较

Tab. 3 Performance comparison of multiple intrusion detection models

模型	论文	方法	数据集	性能评估
RNN	[27]	XGBoost+RNN/LSTM/GRU	NSL-KDD,UNSW-NB15	XGBoost LSTM在NSL-KDD数据集上的准确率:88.13% XGBoost RNN在UNSW-NB15数据集上的准确率:87.07%
	[31]	AE+LSTM	NSL-KDD	Acc:89%
	[32]	AE+GRU	NSL-KDD,UNSW-NB15	在NSL-KDD和UNSW-NB15数据集上,准确率分别为89.54%和88.39%
AE	[35]	SCAE+SVM	NSL-KDD	Acc:89.93%,Recall:89.93%,f-measure:96.94%
	[38]	CVAE+CNN/GRU	CSE-CIC-IDS 2018[24]	CSE-IC-IDS 2018数据集的准确率分别为98.58%和98.56%
	[40]	SAE/SSAE/DAE/ContAE/CAE	UNSW-NB15	Acc: 87.16%,87.36%,86.05%,88.48%,86.66%
DBM	[41]	DBM+Softmax	NSL-KDD	Acc:93.52%
	[42]	RBM+SVM/DT/RF	NSL-KDD	Acc:83.05%,81.89%,79.87%
	[43]	RBM+3WD	NSL-KDD	Acc:96.1%
DBN	[45]	DBN+SVM	CICIDS 2017	Acc:97.74%,Recall:97.68%,f-measure:97.68%
	[46]	DBN+LSTM	KDD99, CICIDS 2017	在KDD99和CICIDS 2017数据集上,准确率分别为94.80%和86.35%
CNN	[49]	CNN+BiLSTM	NSL-KDD	Acc:99.31%
	[50]	MECNN	AWID[68],CIC-IDS2017	在AWID和CIC-IDS2017数据集上,准确率分别为99.96%和99.84%
	[53]	CANET	NSL-KDD,UNSW-NB15	在NSL-KDD和UNSW-NB15数据集上,准确率分别为99.74%和89.39%
GAN	[57]	GAN+CNN	NSL-KDD,UNSW-NB15	在NSL-KDD和UNSW-NB15数据集上,准确率分别为93.2%和87%
	[58]	B-GAN+LSTM	SWaT[69]	Acc:90.97%
GNN	[60]	E-GraphSAGE	BoT-IoT[70],TON-IOT[71]	在BoT-IoT和TON-IoT数据集上,准确率分别为99.99%和97.87%
	[62]	E-GraphSAGE M/ E-ResGAT	TON-IOT	ACC:99.88%,99.88%
	[63]	Anomal-E	NF-UNSW-NB15-v2[72, 73]	ACC:98.18%

综合而言,深度学习模型在入侵检测系统中的成功应用为网络安全领域带来了显著的突破。(1)对于RNN,LSTM和GRU成功克服了传统循环神经网络在训练过程中可能遭遇的“梯度消失或爆炸”问题,为入侵检测系统提供了更为可靠的检测精度。这一类模型的优势在于能够通过其特有的细胞结构来保持数据间的长期依赖关系。可以使用RNN,LSTM和GRU和其他神经网络组合构建入侵检测模型,提取准确描绘数据的时空特征,提高模型的准确率。(2)AE、DBM和DBN等深度学习技术在入侵检测系统中被广泛应用于特征提取和数据降维。这些方法通过学习数据的有效表示,能够从原始数据中提取出最具代表性的特征,从而帮助系统更好地理解和利用输入数据的关键信息。在入侵检测系统中,这些深度学习技术通常与其他分类模型相结合,用于对输入数据进行预处理或特征提取。通过这种方式,系统能够从大量的原始数据中筛选出最具有代表性和区分性的特征,为后续的分类过程提供更有价值的信息。这样的特征提取过程有助于提高系统对入侵行为的检测能力,使得系统能够更准确地识别潜在的安全威胁。(3)采用卷积神经网络构建的入侵检测模型可以更好地提取数据中的空间特征,提高模型的计算效率。并且由于其权值共享的特性,能够有效减少所要训练的参数,降低了模型的自由度,避免了在有限的数据集上花费大量时间进行拟合所造成的过拟合。CNN的多层次特性使其不仅可以用于特征提取,而且在分类任务中也表现出色。其在入侵检测的分类任务中展现出高准确率,对网络流量数据的分析更加精确和全面。(4)生成对抗网络则被广泛应用于处理数据集不平衡的情况。通过生成更多的异常样本,GAN有助于平衡数据集中正常和异常样本的比例,轻数据不平衡性带来的影响,提高模型的鲁棒性和泛化性能。(5)图神经网络凭借其出色的结构行为捕捉能力在入侵检测分类问题中表现卓越。对于涉及网络结构和节点关系的场景,GNN能够更好地理解网络流量的内在规律,进而提高分类准确性。表4更详细地列出了上述基于深度学习的入侵检测模型的优点和功能以及其适用情况。

表4 不同类型入侵检测模型的比较

Tab. 4 Comparison of different types of intrusion detection models

序号	模型	优点	功能	适用情况
1	RNN	捕捉网络流量中的时序特征	特征提取;分类	时序数据、网络流量等具有序列结构的数据
2	AE	自动学习数据中的有用特征;无监督学习	特征提取;数据降维;去噪;	
3	RBM	实现数据降维,以及可以无监督学习	特征提取;数据降维;去噪;	数据集较大,特征维数较多
4	DBN	学习特征的深层次信息,具有较强的泛化能力。	特征提取;分类	
5	CNN	更好地提取目标特征,提高入侵检测模型的计算效率	特征提取;分类	抓取网络流量的空间特征,作为高准确率的分类器
6	GAN	并生成少数类数据,处理数据集不平衡	数据增强;对抗训练	数据集不平衡
7	GNN	更好的捕获网络流量中的结构性行为, 学习网络节点中的复杂关系和特征,动态检测攻击;	分类	涉及网络结构和节点关系的场景

4 网络入侵检测系统的应用

基于深度学习的入侵检测系统以其对复杂数据模式的学习能力和高效的特征提取能力，成为网络安全领域的研究热点。其在网络和云技术、银行业、社交网络等领域的广泛适用性，有许多入侵检测系统技术已被用来解决不同应用的问题。在本节中，我们将介绍基于深度学习的入侵检测系统在三个领域的具体应用，包括软件定义网络、物联网和车联网安全。这些应用场景将展示基于深度学习的入侵检测系统在实际环境中的效果和价值，进一步突显了其在提高网络安全性和保护数据安全方面的重要性。

4.1 软件定义网络(Software Defined Network，SDN)

SDN的开发目的是通过从集中位置控制和管理整个网络来降低传统网络的复杂性。这种新模型通过提供一个称为SDN控制器的新独立平面，引入了传输平面和控制平面的分离。如今，由于这种新范式的各种优势，许多商业和工业企业正在其网络环境中(尤其是数据中心)采用这种解决方案。然而，新兴的SDN技术可能会导致许多安全漏洞和威胁，例如中间人(Man-in-the-Middle Attack，MITM)攻击、拒绝服务(DoS)、过载饱和攻击。因此，部署入侵检测系统来监控恶意活动对于SDN网络架构至关重要。

Gadze等[74]分析了基于深度学习的模型在识别和缓解SDN中DDoS攻击方面的性能。他们调查的主要重点是检测UDP、TCP和ICMP(Internet Control Message Protocol)洪水攻击。将深度学习模型的性能与经典机器学习模型进行了比较，LSTM和CNN等基于DL的模型相对于经典的基于ML的模型的性能表现较好。他们的实验结果表明，LSTM是最好的模型，准确率为89.63%，可应用于SDN控制器中的DDoS检测和缓解。另一方面，SVM在基于线性的模型中表现最好，准确率为86.85%。Maeda等[75]提出了一种基于深度学习的僵尸网络检测方法。所提出的系统首先检测受感染的主机，然后使用SDN分离该主机。为了检测恶意软件，使用从传统网络上收集的僵尸网络流量中获得的数据进行训练，然后测试检测性能。僵尸网络流量被重新传输以隔离SDN中受僵尸程序感染的设备，并且与ML分类器定义的源IP的连接被堵塞和隔离。在文献[76]中，作者提出了一种针对SDN系统的DDoS攻击检测和缓解模型[76]。该模型基于SVM技术作为分类器。为了获得更好的精度并减少测试时间，该模型使用了带有遗传算法(Genetic Algorithm，GA)的核主成分分析(kernel principal component analysis，KPCA)技术，KPCA技术被用来从数据集中提取主要特征，并从DDoS向量中减少它们的维度，GA用于选择合适的特征以优化不同的SVM参数。实验结果表明，在DDoS数据集上，KPCA有效地发挥作用，所提模型的准确率达到98.907%。

4.2 物联网

物联网(Internet of Things，IoT)是互联网的下一次革命，通过互联网作为骨干网，以远程方式连接和管理智能终端设备。物联网环境中的事件由终端设备感知。由于物联网中传感器的资源限制特性及其部署环境，提供有效的安全性成为一项重大挑战。物联网设备的部署环境容易受到黑客、恶意软件和病毒等入侵者的多种攻击。这些入侵者的主要目的是发起各种形式的攻击，从而破坏网络中的数据完整性。此外，入侵者还可能发起拒绝服务(DoS)攻击，从而耗尽网络和设备资源。入侵检测系统的设计和部署可以很好地解决这一问题。因此，IDS已被广泛用于监测物联网环境中的攻击行为，以便在物联网通信中提供有效的安全性[77]。

Roy等[78]提出了一个IDS模型，该模型利用DL来识别资源受限的物联网系统中的网络攻击和异常情况。由于结合了消除多重共线性、采样和降维等优化，该模型使用相当少的训练数据和更少的训练时间来确定检测入侵的重要特征。该模型在不同数据集上的研究结果表明，具有较低的误报率和较高的检测率。它在多个性能参数上超越了以前的模型，最值得注意的是，与传统的资源密集型入侵检测系统不同，所提出的模型是轻量级的，可以部署在功率和储存能力有限的物联网设备上。为了识别攻击，文献[79]提出了一种基于混合PCA-GWO的深度神经网络(DNN)分类器模型[79]。他们的方法更适合于医疗物联网环境，其中智能医疗对象使用基于网络的唯一IP地址相互通信。该方法利用灰狼优化技术进行特征提取，有助于最大限度地减少使用DNN模型进行分类过程所得出的特征数量。结果表明，分类模型的准确率很高，并且训练所需的时间很短。Davahli等人[80]提出了一种面对物联网无线网络的入侵检测系统(IoTIDS)，该系统基于机器学习的高性能轻量级入侵检测技术。IoTIDS基于遗传算法(Genetic Algorithm，GA)和灰狼优化器(Grey Wolf Optimizer，GWO)的混合，称为GA-GWO。混合算法利用GA和GWO的优点和良好特性，主要目的是通过消除冗余和不相关的流量数据，降低大量无线流量数据的维数，从而降低了IoTIDS的计算复杂度。使用AWID无线网络数据集来评估GA-GWO在IoTIDS上的有效性，实验结果表明，提出的混合方法在各种指标展现了更高的性能。Li等人[81]通过应用基于分歧的半监督学习算法，提出了半监督学习和协作IDS架构，旨在通过交换和共享数据来提高物联网(IoT)网络中单个检测器的检测性能。在评估中，使用数据集和真实物联网网络环境来研究该方法在检测性能和误报率方面的性能。实验结果表明，与传统的监督机器学习分类器相比，该方法通过自动利用未标记的数据来更有效地检测入侵并减少误报。Moizuddin等[82]提出了一种基于广义平均灰狼优化算法(Generalized Mean Grey Wolf Optimization，GMGWO)和堆叠式弹性收缩自动编码器(Elastic Contractive Auto Encoder，ECAE)的IDS。他们的研究中使用的GMGWO方法被证明可以选择合适的特征来训练分类器模型。该研究还引入了ECAE，它结合了套索和岭回归的优点。在物联网数据集BoT-IoT上进行评估时，分类器模型在二分类和多分类性能指标方面优于最先进的方法。此外，所提出的模型还证明了其在无需额外训练的情况下从未标记数据中学习特征以及任意测试数据的泛化有效性。

4.3 车载网络(In-Vehicle Networks，IVN)

控制器局域网(Controller Area Network，CAN)是使用最广泛的车载网络通信协议，其仍然缺乏合适的安全机制的实现，这使得CAN总线容易受到许多网络攻击。各种入侵检测系统已被研究人员成功地用于识别汽车中的网络攻击。对于车载网络，CAN数据也可以被视为顺序数据或多变量时间序列数据。大多数CAN ID都是根据定义的时间间隔或事件序列进行传输的，该属性可用于识别此类序列中的异常情况。入侵检测系统是一种很有前途的汽车安全增强技术，几乎不需要对车辆的现有基础设施进行调整。深度学习技术可以增强汽车IDS的能力，提高检测的准确性和精确度[83]。

Han等[84]提出了一种基于控制器局域网报文的周期性事件触发间隔来检测和识别车辆网络异常的方法。为此，作者首先定义四种攻击场景，然后提取这些场景对应的正常和异常驾驶数据。接下来，分析每个CAN ID的事件触发间隔并根据定义的时间窗口测量统计时刻。计算出的特征值用于训练ML模型，如DT，RF和XGBoost，以识别攻击。实验结果表明，使用两个真实的数据集与现实的攻击表现出较高的异常和攻击检测能力。Avatefipour等[85]提出了一种有效的CAN总线流量异常检测模型。该方法是一种改进的单类支持向量机，它采用一种改进的蝙蝠算法(Modified Bat Algorithm，MBA)作为参数优化算法。提出的MOCSVM方法用于检测CAN流量中的恶意网络攻击行为。所提出的方法背后的基本思想是建立一个模型的基础上，正常的CAN总线流量，其中包含在一个给定的正常流量中传输的消息ID的重复模式。为此，MBA-OCSVM算法可以将与正常流量的任何偏差(例如，增加的消息出现频率或消息泛洪)检测为离群值。为了证明所提出的模型的高性能，三种方法，即传统的一类SVM，隔离森林，MBA-OCSVM进行了比较。实验结果表明，与其他异常检测方法相比，该方法具有最高的检测率和最低的误报率。CAN数据的顺序行为可用于检测异常行为，利用这一特性，Song等[86]提出了一种基于深度卷积神经网络(DCNN)的IDS，以保护CAN总线免受网络攻击。在注入攻击期间，ID的顺序模式由于频繁的帧注入而改变。作者利用这一变化来检测消息注入攻击。使用Inception-ResNet作为DCNN模型，具有29×29×1输入和二进制输出。HCRL CH数据集

用于评估所提出的解决方案。对于所有攻击类型,DCNN模型的性能都优于基线模型。Jedh等[87]使用LSTM-RNN模型来检测CAN总线中的恶意消息注入。他们在连续的时间窗口中使用CAN ID的消息序列图来计算余弦相似性和皮尔逊相关性,然后将其用作LSTM模型的特征。为了评估该模型的性能,他们使用了一个真实的车辆数据集,其中包含捏造的转速和车速信息。实验结果表明,消息序列图的余弦相似性和皮尔逊相关性可有效检测转速和车速信息的注入,准确率达98.45%。Hanselmann等[88]介绍了一种基于LSTM的IDS CANet,用于识别CAN总线中的攻击。他们为每个CAN ID使用单独的LSTM模型,并将输出串联成一个潜在向量。该模型以无监督的方式训练的,并且初始信号值和重建信号值之间的差异用于定义正常状态。作者使用一个包含13个ID的真实车辆数据集和一个包含10个ID的合成数据集SynCAN进行性能评估。选择了六种攻击和两种基线模型来评估模型性能。实验结果表明,该模型对两个数据集的所有攻击都具有较高的检测率和较低的误报率和漏报率,它的表现都优于基线模型。

5 挑战与未来研究方向

虽然深度学习模型在入侵检测中取得了令人满意的结果,但在实际商业环境中的广泛应用仍然面临一些挑战。模型的性能可能受到数据集特定性的影响,而在真实世界的网络环境中,数据分布和特征可能更加复杂和多样化。因此,对于深度学习模型在更广泛和复杂场景中的适应性和鲁棒性,仍需要进行更多的深入研究和验证。在未来的研究中,有几个关键问题值得深入考虑,以进一步推动入侵检测领域的发展。

(1)误报率高的问题。尽管基于深度学习的IDS都达到了很高的检测率,但在检测异常情况时会表现出不确定性,大多数基于异常的IDS都试图建立一个模型,以捕捉常规流量的每一种潜在行为或模式。但这尤其困难,因为事实证明,这些模型往往偏向于占主导地位的类别,从而导致较大的误报率[89]。此外,高误报率会导致高成本,因为需要花费大量时间来分析报告的活动,而这些活动最终被证明是正常的网络流量。未来的一个研究目标可以聚焦在提高模型的检测率并减少误报率。例如,文献[90]提出了一种基于风险分析的入侵检测系统的新方法,通过采用模糊逻辑风险分析技术来分析产生的警报,从而降低IDS的误报率[90]。

(2)零日攻击指所有以前没有发现的新攻击。大多数基于DL的IDS解决方案只能应对已知的攻击类型,这些系统在检测零日攻击时很容易失败(尽管模型在已知领域可能具有很高的准确性)。一些潜在的分类失败原因包括[91]:(1)在离线模式下使用非常老的数据集(如KDD99或NSL-KDD)训练模型。这些数据集非常老旧,缺乏当前的流量模式和攻击信息。(2)在单一数据集上训练模型,引起偏差问题并引入限制性训练。(3)假设训练数据和测试数据来自相同的分布。(4)不考虑重新训练模型,以增强其检测新发现攻击的能力。IDS的一个必要功能必须是准确预测已知攻击和零日攻击,而这些攻击是模型事先不知道也从未遇到过的[92]。要准确检测零日攻击,就必须建立超越受限训练限制的模型。模型必须具有通用性,并能对完全不同的样本做出准确预测。一种常见的策略是使用典型的ML训练和测试拆分比例(70:30)拆分数据集,其中每个标签必须同时存在于训练集和测试集中。然后对分类器进行训练,在测试集中进行预测,以获得最佳结果。

(3)高质量的数据集对于测试和验证提出的网络入侵检测系统(NIDS)至关重要。理想的数据集应包含大量网络流量数据,并附带详细描述攻击和正常行为的标签。为了推动未来研究的发展,建议采用更新、更全面的入侵检测数据集,例如CIC IoT Dataset2023[93]。此外,为了确保方法的有效性,研究人员还应当努力使用真实的数据集,例如ISOT CID[94]数据集进行实验。这样的数据集能够更准确地模拟实际网络环境,提高研究结果的可信度和泛化性。

(4)实时检测问题。入侵检测系统(IDS)追求的一个关键目标就是实时检测。然而,目前大多数入侵检测系统仍然依赖于离线状态下的公开数据集进行研究,而没有在真实网络环境中进行实际应用。随着不断涌现的新型网络攻击方式,恶意网络流量的检测变得尤为紧迫和关键。因此,如何有效地将经过训练的模型应用于实时检测,以抵御不断变化的网络攻击,将成为未来入侵检测系统研究的重要焦点。此外,优化和改进深度模型结构,以适应不断演化的网络环境,也将是未来发展的关键挑战。

(5)数据集不平衡问题。由于数据集收集过程中难以为所有攻击类和正常类收集相同数量的记录,数据集不平衡是不可避免的。深度学习中,数据集的质量直接影响模型的训练和检测结果。在模型训练时,通常需要足够多的样本来调整神经网络的各个参数。目前用于入侵检测的训练集中,正常流量样本通常占据大部分,而恶意流量样本数量相对较少。训练数据不平衡可能导致训练后的模型存在严重的偏向性,即模型可能过于关注正常流量数据,从而显著降低对异常流量数据的识别率。解决数据不平衡问题对于提高入侵检测系统性能至关重要。在未来的入侵检测系统(IDS)研究中,过采样和欠采样技术是常见的平衡数据集的方法,其中SMOTE及其变种是广泛使用的过采样方法,通过合成新的少数类样本来增加数据集的多样性[28]。同时,Random Under-Sampling等欠采样方法[95]通过减少正常类样本数量,使得数据集中正常类和攻击类样本的比例更为均衡。除了传统的过采样和欠采样技术,生成少数类样本的方法也引起了研究者的关注。采用自编码器(CAE)、条件变分自编码器(CVAE)[38]和生成对抗网络(GAN)[57-59]等生成少数类样本,以丰富数据集的多样性,综合运用这些方法,可以有效应对数据集不平衡问题,提高模型的鲁棒性和泛化能力。

(6)网络数据流量大和维度高的问题。网络数据流量通常是大规模的时序数据,包含大量的网络通信记录,这些网络数据通常具有高维度的特征,例如源地址、目标地址、端口号顿号,协议等。网络数据流量大通常意味着会消耗更多的计算资源,对计算机硬件要求较高。未来的研究可以更加关注轻量化的入侵检测模型和基于分布式的入侵检测系统,轻量化模型有助于在计算资源受限的设备上部署入侵检测系统,提高系统的实际可用性[96]。通过分布式架构,可以将数据分割成小块进行处理,充分利用多个计算节点的并行计算能力。这有助于提高整体的处理速度,缓解大规模数据流量对单一计算节点的压力[97]。此外,未来的研究可以进一步探索利用特征选择和降维技术来应对数据维度庞大的挑战,选择对入侵检测任务最为关键的特征,从而减少数据维度[15]。

(7)半监督学习[98]、迁移学习[99]、强化学习[100]以及集成学习[101]等方法在入侵检测系统(IDS)方面尚未得到广泛的研究和评估。未来的研究很可能会集中在这些方向上,在入侵检测中,通常难以获取大量标签样本,半监督学习可以用于处理入侵检测中标签数据不足的问题,其可以充分利用有标签样本和无标签样本,通过整合未标记的数据提高模型的性能。迁移学习在源领域训练的模型知识可以迁移到目标领域,减少在目标领域的样本需求,加速模型的训练过程。应用于入侵检测中,当源领域和目标领域存在一定的相似性时,通过迁移学习可以更好地适应新的入侵特征。强化学习能够通过与环境的交互学习,适应动态变化的入侵行为,还可以在实时环境中不断优化策略,提高入侵检测的实时性。机器学习模型可能在检测不同类型的攻击有不同的敏感性。可以通过组合多个模型,可以提高整体模型的鲁棒性和泛化能力,降低过拟合风险。另外,通过将深度学习模型与传统机器学习模型结合,可以在保留重要信息的同时减少数据的维度,提高入侵检测系统的效率和处理能力。深入研究这些方向有望为未来的入侵检测系统的设计和性能提供更多创新和可行性,为入侵检测领域带来更多的突破和进展[102]。

6 结语

随着新技术的出现和网络流量的快速增长,研究人员一直在研究深度学习在入侵检测中的应用。深度模型可以有效处理复杂的网络流量数据,自动学习数据特征的相关性,其成为应对不断演变的网络威胁的有力工具。本文详细论述了基于深度学习的网络入侵检测

系统的研究现状，涵盖了入侵检测系统、数据集与评价指标、深度学习算法的应用以及相关问题和展望。尽管目前已经提出和应用了各种改进的深度学习的方法，但入侵检测性能仍有提升的空间。未来的目标是建立能够在准确性、效率和实时性方面都表现出色的基于深度学习的入侵检测模型，以应对日益复杂的网络流量和威胁。

参考文献（References）

[1] LV Z, QIAO L, LI J, et al. Deep-learning-enabled security issues in the internet of things [J]. IEEE Internet of Things Journal, 2020, 8(12): 9531-8.

[2] BAJPAI P, SOOD A K, ENBODY R J. The art of mapping IoT devices in networks [J]. Network Security, 2018, 2018(4): 8-15.

[3] ANDERSON J P. Computer security threat monitoring and surveillance [J]. Technical Report, James P Anderson Company, 1980.

[4] FANG L, LI Y, LIU Z, et al. A practical model based on anomaly detection for protecting medical IoT control services against external attacks [J]. IEEE Transactions on Industrial Informatics, 2020, 17(6): 4260-9.

[5] MICHIE D, SPIEGELHALTER D J, TAYLOR C C, et al. Machine learning, neural and statistical classification [M]. Ellis Horwood, 1995.

[6] AL-OMARI M, RAWASHDEH M, QUTAISHAT F, et al. An intelligent tree-based intrusion detection model for cyber security [J]. Journal of Network and Systems Management, 2021, 29(2): 20.

[7] ALAM S, SONBHADRA S K, AGARWAL S, et al. One-class support vector classifiers: A survey [J]. Knowledge-Based Systems, 2020, 196: 105754.

[8] 程超，武静凯，陈梅. 一种基于RBM-SVM算法的无线传感网络入侵检测算法 [J]. 计算机应用与软件，2022，39(05)：325-9.（Cheng C, Wu J K, Chen M. A Wireless Sensor Network Intrusion Detection Algorithm Based on RBM-SVM Algorithm [J] Computer Applications and Software, 2022, 39(05): 325-9）

[9] 张昊，张小雨，张振友，等. 基于深度学习的入侵检测模型综述 [J]. 计算机工程与应用，2022，58(06)：17-28.（Zhang H, Zhang X Y, Zhang Z Y, et al. A Review of Intrusion Detection Models Based on Deep Learning [J] Computer Engineering and Applications, 2022, 58(06): 17-28）

[10] WANG N, CHEN Y, XIAO Y, et al. Manda: On adversarial example detection for network intrusion detection system [J]. IEEE Transactions on Dependable and Secure Computing, 2022, 20(2): 1139-53.

[11] 刘拥民，杨钰津，罗皓懿，等. 基于双向循环生成对抗网络的无线传感网入侵检测方法 [J]. 计算机应用，2023，43(01)：160-8.（LIU Yongmin, YANG Yujin, LUO Haoyi, HUANG Hao, XIE Tieqiang. Intrusion detection method for wireless sensor network based on bidirectional circulation generative adversarial network [J]. Journal of Computer Applications, 2023, 43(01): 160-8.）

[12] MOHAMMADPOUR L, LING T C, LIEW C S, et al. A survey of CNN-based network intrusion detection [J]. Applied Sciences, 2022, 12(16): 8162.

[13] 白万荣，魏峰，郑广远，等. 基于TCN-BiLSTM的入侵检测算法研究 [J]. 计算机科学，2023，50(S2)：941-8.（Bai W R, Wei F, Z G Y, et al. Research on Intrusion Detection Algorithm Based on TCN BiLSTM [J] Computer Science, 2023, 50 (S2): 941-8）

[14] DENNING D E. An intrusion-detection model [J]. IEEE Transactions on software engineering, 1987, (2): 222-32.

[15] THAKKAR A, LOHIYA R. A survey on intrusion detection system: feature selection, model, performance measures, application perspective, challenges, and future research directions [J]. Artificial Intelligence Review, 2022, 55(1): 453-563.

[16] VASILOMANOLAKIS E, KARUPPAYAH S, MüHLHäUSER M, et al. Taxonomy and survey of collaborative intrusion detection [J]. ACM computing surveys (CSUR), 2015, 47(4): 1-33.

[17] OU Y-J, LIN Y, ZHANG Y. The design and implementation of host-based intrusion detection system [C]//2010 third international symposium on intelligent information technology and security informatics. IEEE, 2010: 595-598.

[18] HAMED T, DARA R, KREMER S C. Network intrusion detection system based on recursive feature addition and bigram technique [J]. computers & security, 2018, 73: 137-55.

[19] EDEH D I. Network intrusion detection system using deep learning technique [J]. Master of Science, Department of Computing, University of Turku, 2021.

[20] WU P. Deep learning for network intrusion detection: Attack recognition with computational intelligence [D]; UNSW Sydney, 2020.

[21] TAVALLAEE M, BAGHERI E, LU W, et al. A detailed analysis of the KDD CUP 99 data set [C]//2009 IEEE symposium on computational intelligence for security and defense applications. Ieee, 2009: 1-6.

[22] PROTIĆ D D. Review of KDD Cup '99, NSL-KDD and Kyoto 2006+ datasets [J]. Vojnotehnički glasnik/Military Technical Courier, 2018, 66(3): 580-96.

[23] MOUSTAFA N, SLAY J. UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set) [C]//2015 military communications and information systems conference (MilCIS). IEEE, 2015: 1-6.

[24] SHARAFALDIN I, LASHKARI A H, GHORBANI A A. Toward generating a new intrusion detection dataset and intrusion traffic characterization [J]. ICISSp, 2018, 1: 108-16.

[25] DONG B, WANG X. Comparison deep learning method to traditional methods using for network intrusion detection [C]//2016 8th IEEE international conference on communication software and networks (ICCSN). IEEE, 2016: 581-585.

[26] DENG L. A tutorial survey of architectures, algorithms, and applications for deep learning [J]. APSIPA transactions on Signal and Information Processing, 2014, 3: e2.

[27] KASONGO S M. A deep learning technique for intrusion detection system using a Recurrent Neural Networks based framework [J]. Computer Communications, 2023, 199: 113-25.

[28] WEI W, CHEN Y, LIN Q, et al. Multi-objective evolving long-short term memory networks with attention for network intrusion detection [J]. Applied Soft Computing, 2023, 139: 110216.

[29] DONKOL A A E-B, HAFEZ A G, HUSSEIN A I, et al. Optimization of intrusion detection using likely point PSO and enhanced LSTM-RNN hybrid technique in communication networks [J]. IEEE Access, 2023, 11: 9469-82.

[30] SYED N F, GE M, BAIG Z. Fog-cloud based intrusion detection system using Recurrent Neural Networks and feature selection for IoT networks [J]. Computer Networks, 2023, 225: 109662.

[31] MUSHTAQ E, ZAMEER A, UMER M, et al. A two-stage intrusion detection system with auto-encoder and LSTMs [J]. Applied Soft Computing, 2022, 121: 108768.

[32] MUSHTAQ E, ZAMEER A, NASIR R. Knacks of a hybrid anomaly detection model using deep auto-encoder driven gated recurrent unit [J]. Computer Networks, 2023, 226: 109681.

[33] KANNA P R, SANTHI P. Hybrid intrusion detection using mapreduce based black widow optimized convolutional long short-term memory neural networks [J]. Expert Systems with Applications, 2022, 194: 116545.

[34] UDAS P B, KARIM M E, ROY K S. SPIDER: A shallow PCA based network intrusion detection system with enhanced recurrent neural networks [J]. Journal of King Saud University-Computer and Information Sciences, 2022, 34(10): 10246-72.

[35] WANG W, DU X, SHAN D, et al. Cloud intrusion detection method based on stacked contractive auto-encoder and support vector machine [J]. IEEE transactions on cloud computing, 2020, 10(3): 1634-46.

[36] MUHAMMAD G, HOSSAIN M S, GARG S. Stacked autoencoder-based intrusion detection system to combat financial fraudulent [J]. IEEE Internet of Things Journal, 2020, 10(3): 2071-8.

[37] BALASUBRAMANIAM S, VIJESH JOE C, SIVAKUMAR T, et al. Optimization enabled deep learning-based DDoS attack detection in cloud computing [J]. International Journal of Intelligent Systems, 2023, 2023.

[38] LIU C, ANTYPENKO R, SUSHKO I, et al. Intrusion detection system after data augmentation schemes based on the VAE and CVAE [J]. IEEE Transactions on Reliability, 2022, 71(2): 1000-10.

[39] BOPPANA T K, BAGADE P. GAN-AE: An unsupervised intrusion detection system for MQTT networks [J]. Engineering Applications of Artificial Intelligence, 2023, 119: 105805.

[40] VAIYAPURI T, BINBUSAYYIS A. Application of deep autoencoder as an one-class classifier for unsupervised network intrusion detection: a comparative evaluation [J]. PeerJ Computer Science, 2020, 6: e327.

[41] COLI G O, AINA S, OKEGBILE S D, et al. DDoS attacks detection in the IoT using deep gaussian-bernoulli restricted boltzmann machine [J]. Modern Applied Science, 2022, 16(2): 12.

[42] ROSA G H D, RODER M, SANTOS D F, et al. Enhancing anomaly detection through restricted Boltzmann machine features projection [J]. International Journal of Information Technology, 2021, 13: 49-57.

[43] HONG L, HAN B. Intrusion detection method based on constrained Boltzmann machine and delayed decision [C]// Proceedings of the 2022 6th International Conference on Electronic Information Technology and Computer Engineering. 2022: 979-985.

[44] MAYURANATHAN M, MURUGAN M, DHANAKOTI V. RETRACTED ARTICLE: Best features based intrusion detection system by RBM model for detecting DDoS in cloud environment [J]. Journal of Ambient Intelligence and Humanized Computing, 2021, 12(3): 3609-19.

[45] ZHANG H, LI Y, LV Z, et al. A real-time and ubiquitous network attack detection based on deep belief network and support vector machine [J]. IEEE/CAA Journal of Automatica Sinica, 2020, 7(3): 790-9.

[46] CHEN A, FU Y, ZHENG X, et al. An efficient network behavior anomaly detection using a hybrid DBN-LSTM network [J]. Computers & Security, 2022, 114: 102600.

[47] SARKAR N, KESERWANI P K, GOVIL M C. A better and fast cloud intrusion detection system using improved squirrel search algorithm and modified deep belief network [J]. Cluster Computing, 2024, 27(2): 1699-718.

[48] A. ALISSA K, SHAIBA H, GADDAH A, et al. Feature subset selection hybrid deep belief network based cybersecurity intrusion detection model [J]. Electronics, 2022, 11(19): 3077.

[49] KANUMALLI S S, LAVANYA K, RAJESWARI A, et al. A scalable network intrusion detection system using bi-lstm and cnn [C]//2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS). IEEE, 2023: 1-6.

[50] CHEN Y, LIN Q, WEI W, et al. Intrusion detection using multi-objective evolutionary convolutional neural network for Internet of Things in Fog computing [J]. Knowledge-Based Systems, 2022, 244: 108505.

[51] WU Y, NIE L, WANG S, et al. Intelligent intrusion detection for internet of things security: A deep convolutional generative adversarial network-enabled approach [J]. IEEE Internet of Things Journal, 2021, 10(4): 3094-106.

[52] ULLAH F, ULLAH S, SRIVASTAVA G, et al. IDS-INT: Intrusion detection system using transformer-based transfer learning for imbalanced network traffic [J]. Digital Communications and Networks, 2024, 10(1): 190-204.

[53] REN K, YUAN S, ZHANG C, et al. CANET: A hierarchical cnn-attention model for network intrusion detection [J]. Computer Communications, 2023, 205: 170-81.

[54] EL-GHAMRY A, DARWISH A, HASSANIEN A E. An optimized CNN-based intrusion detection system for reducing risks in smart farming [J]. Internet of Things, 2023, 22: 100709.

[55] CHEN C, SONG Y, YUE S, et al. Fcnn-se: An intrusion detection model based on a fusion CNN and stacked ensemble [J]. Applied Sciences, 2022, 12(17): 8601.

[56] PINGALE S V, SUTAR S R. Remora based Deep Maxout Network model for network intrusion detection using Convolutional Neural Network features [J]. Computers and Electrical Engineering, 2023, 110: 108831.

[57] PARK C, LEE J, KIM Y, et al. An enhanced AI-based network intrusion detection system using generative adversarial networks [J]. IEEE Internet of Things Journal, 2022, 10(3): 2330-45.

[58] YUAN L, YU S, YANG Z, et al. A data balancing approach based on generative adversarial network [J]. Future Generation Computer Systems, 2023, 141: 768-76.

[59] ZHU N, ZHAO G, YANG Y, et al. Aec_gan: unbalanced data processing decision-making in network attacks based on ACGAN and machine learning [J]. IEEE Access, 2023.

[60] LO W W, LAYEGHY S, SARHAN M, et al. E-graphsage: A graph neural network based intrusion detection system for iot [C]// NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium. IEEE, 2022: 1-9.

[61] LAN J, LU J Z, WAN G G, et al. E-minbatch graphsage: An industrial internet attack detection model [J]. Security and Communication Networks, 2022, 2022.

[62] CHANG L, BRANCO P. Graph-based solutions with residuals for intrusion detection: The modified e-graphsage and e-resgat algorithms [J]. arXiv preprint arXiv:211113597, 2021.

[63] CAVILLE E, LO W W, LAYEGHY S, et al. Anomal-E: A self-supervised network intrusion detection system based on graph neural networks [J]. Knowledge-based systems, 2022, 258: 110030.

[64] ALTAF T, WANG X, NI W, et al. NE-GConv: A lightweight node edge graph convolutional network for intrusion detection [J]. Computers & Security, 2023, 130: 103285.

[65] DUAN G, LV H, WANG H, et al. Application of a dynamic line graph neural network for intrusion detection with semisupervised learning [J]. IEEE Transactions on Information Forensics and

Security, 2022, 18: 699-714.

[66] ZHANG Y, YANG C, HUANG K, et al. Intrusion detection of industrial internet-of-things based on reconstructed graph neural networks [J]. IEEE Transactions on network science and engineering, 2022.

[67] WANG Y, HAN Z, LI J, et al. BS-GAT Behavior Similarity Based Graph Attention Network for Network Intrusion Detection [J]. arXiv preprint arXiv:230407226, 2023.

[68] KOLIAS C, KAMBOURAKIS G, STAVROU A, et al. Intrusion detection in 802. 11 networks: Empirical evaluation of threats and a public dataset [J]. IEEE Communications Surveys & Tutorials, 2015, 18(1): 184-208.

[69] GOH J, ADEPU S, JUNEJO K N, et al. A dataset to support research in the design of secure water treatment systems [C]// Critical Information Infrastructures Security: 11th International Conference, CRITIS 2016, Paris, France, October 10 - 12, 2016, Revised Selected Papers 11. Springer International Publishing, 2017: 88-99.

[70] KORONIOTIS N, MOUSTAFA N, SITNIKOVA E, et al. Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset [J]. Future Generation Computer Systems, 2019, 100: 779-96.

[71] MOUSTAFA N. A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets [J]. Sustainable Cities and Society, 2021, 72: 102994.

[72] SARHAN M, LAYEGHY S, PORTMANN M. Towards a standard feature set for network intrusion detection system datasets [J]. Mobile networks and applications, 2022: 1-14.

[73] SARHAN M, LAYEGHY S, MOUSTAFA N, et al. Netflow datasets for machine learning-based network intrusion detection systems [C]//Big Data Technologies and Applications: 10th EAI International Conference, BDTA 2020, and 13th EAI International Conference on Wireless Internet, WiCON 2020, Virtual Event, December 11, 2020, Proceedings 10. Springer International Publishing, 2021: 117-135.

[74] GADZE J D, BAMFO-ASANTE A A, AGYEMANG J O, et al. An investigation into the application of deep learning in the detection and mitigation of DDOS attack on SDN controllers [J]. Technologies, 2021, 9(1): 14.

[75] MAEDA S, KANAI A, TANIMOTO S, et al. A botnet detection method on SDN using deep learning [C]//2019 IEEE International Conference on Consumer Electronics (ICCE). IEEE, 2019: 1-6.

[76] SAHOO K S, TRIPATHY B K, NAIK K, et al. An evolutionary SVM model for DDOS attack detection in software defined networks [J]. IEEE access, 2020, 8: 132502-13.

[77] CHAABOUNI N, MOSBAH M, ZEMMARI A, et al. Network intrusion detection for IoT security based on learning techniques [J]. IEEE Communications Surveys & Tutorials, 2019, 21(3): 2671-701.

[78] ROY S, LI J, CHOI B-J, et al. A lightweight supervised intrusion detection mechanism for IoT networks [J]. Future Generation Computer Systems, 2022, 127: 276-85.

[79] RM S P, MADDIKUNTA P K R, PARIMALA M, et al. An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture [J]. Computer Communications, 2020, 160: 139-49.

[80] DAVAHLI A, SHAMSI M, ABAEI G. Hybridizing genetic algorithm and grey wolf optimizer to advance an intelligent and lightweight intrusion detection system for IoT wireless networks [J]. Journal of Ambient Intelligence and Humanized Computing, 2020, 11(11): 5581-609.

[81] LI W, MENG W, AU M H. Enhancing collaborative intrusion detection via disagreement-based semi-supervised learning in IoT environments [J]. Journal of Network and Computer Applications, 2020, 161: 102631.

[82] MOIZUDDIN M, JOSE M V. A bio-inspired hybrid deep learning model for network intrusion detection [J]. Knowledge-based systems, 2022, 238: 107894.

[83] LAMPE B, MENG W. A survey of deep learning-based intrusion detection in automotive applications [J]. Expert Systems with Applications, 2023, 221: 119771.

[84] HAN M L, KWAK B I, KIM H K. Event-triggered interval-based anomaly detection and attack identification methods for an in-vehicle network [J]. IEEE Transactions on Information Forensics and Security, 2021, 16: 2941-56.

[85] AVATEFIPOUR O, AL-SUMAITI A S, EL-SHERBEENY A M, et al. An intelligent secured framework for cyberattack detection in electric vehicles' CAN bus using machine learning [J]. Ieee Access, 2019, 7: 127580-92.

[86] SONG H M, WOO J, KIM H K. In-vehicle network intrusion detection using deep convolutional neural network [J]. Vehicular Communications, 2020, 21: 100198.

[87] JEDH M, OTHMANE L B, AHMED N, et al. Detection of message injection attacks onto the can bus using similarities of successive messages-sequence graphs [J]. IEEE Transactions on Information Forensics and Security, 2021, 16: 4133-46.

[88] HANSELMANN M, STRAUSS T, DORMANN K, et al. CANet: An unsupervised intrusion detection system for high dimensional CAN bus data [J]. Ieee Access, 2020, 8: 58194-205.

[89] ABDULGANIYU O H, AIT TCHAKOUCHT T, SAHEED Y K. A systematic literature review for network intrusion detection system (IDS) [J]. International Journal of Information Security, 2023, 22(5): 1125-62.

[90] QASSIM Q, PATEL A, MOHD-ZIN A. Strategy to Reduce False Alarms in Intrusion Detection and Prevention Systems [J]. International Arab Journal of Information Technology (IAJIT), 2014, 11(5).

[91] AHMAD R, ALSMADI I, ALHAMDANI W, et al. Zero-day attack detection: a systematic literature review [J]. Artificial Intelligence Review, 2023, 56(10): 10733-811.

[92] DUESSEL P, GEHL C, FLEGEL U, et al. Detecting zero-day attacks using context-aware anomaly detection at the application-layer [J]. International Journal of Information Security, 2017, 16 (5): 475-90.

[93] NETO E C P, DADKHAH S, FERREIRA R, et al. CICIoT2023: A real-time dataset and benchmark for large-scale attacks in IoT environment [J]. Sensors, 2023, 23(13): 5941.

[94] ALDRIBI A, TRAORE I, QUINAN P G, et al. Documentation for the isot cloud intrusion detection benchmark dataset (isot-cid) [J]. University of Victoria, 2020.

[95] MIAH M O, KHAN S S, SHATABDA S, et al. Improving detection accuracy for imbalanced network intrusion classification using cluster-based under-sampling with random forests [C]//2019 1st international conference on advances in science, engineering and robotics technology (ICASERT). IEEE, 2019: 1-5.

[96] HE M, HUANG Y, WANG X, et al. A lightweight and efficient IoT intrusion detection method based on feature grouping [J]. IEEE Internet of Things Journal, 2023.

[97] IDRISSI M J, ALAMI H, EL MAHDAOUY A, et al. Fed-anids: Federated learning for anomaly-based network intrusion detection

systems [J]. Expert Systems with Applications, 2023, 234: 121000.

[98] LI S, CAO Y, LIU S, et al. HDA-IDS: A Hybrid DoS Attacks Intrusion Detection System for IoT by using semi-supervised CL-GAN [J]. Expert Systems with Applications, 2024, 238: 122198.

[99] LATIF S, BOULILA W, KOUBAA A, et al. DTL-IDS: An optimized Intrusion Detection Framework using Deep Transfer Learning and Genetic Algorithm [J]. Journal of Network and Computer Applications, 2024, 221: 103784.

[100] 李贝贝, 宋佳芮, 杜卿芸, et al. DRL-IDS:基于深度强化学习的工业物联网入侵检测系统 [J]. 计算机科学, 2021, 48(07): 47-54. (Li B B, Song J R, Du Q Y, et al. DRL-IDS: Industrial Internet of Things Intrusion Detection System Based on Deep Reinforcement Learning [J] Computer Science, 2021, 48(07): 47-54)

[101] MOHY-EDDINE M, GUEZZAZ A, BENKIRANE S, et al. An effective intrusion detection approach based on ensemble learning for IIoT edge computing [J]. Journal of Computer Virology and Hacking Techniques, 2023, 19(4): 469-81.

[102] ASHARF J, MOUSTAFA N, KHURSHID H, et al. A review of intrusion detection systems using machine and deep learning in internet of things: Challenges, solutions and future directions [J]. Electronics, 2020, 9(7): 1177.

This work is partially supported by National Natural Science Foundation of China (62276091) and the Henan Province Science and Technology Research Project (232102210132).

Deng Miaolei, born in 1977, holds a PhD and is a professor. His research interests include information security and IoT technology.

Kan Yupei, born in 2000, is a master's student. His research interests include information security and intrusion detection.

Sun Chuanchuan, born in 1998, is a master's student. His research interests include deep learning and information security.

Xu Haihang, born in 1999, is a master's student. His research interests include deep learning and intrusion detection.

Fan Shaojun, born in 2001, is a master's student. Her research interests include deep learning and intrusion detection.

Zhou Xin, born in 1999, is a master's student. His research interests include deep learning and information security.