中图分类号：TP309　　密级：公开

UDC：004　　学校代码：10094

河北师范大学

硕士学位论文

（学术学位）

改进卷积神经网络在网络安全态势评估中的应用研究

Research on the Application of Improved Convolutional Neural Network in Network Security Situation Assessment

研究生姓名：宿梦月

指导教师：赵冬梅　教授

一级学科：网络空间安全

二级学科：

研究方向：网络安全

论文开题日期：2022 年 5 月 6 日

二〇二三年五月二十五日

中图分类号：TP309　　密级：公开

UDC：004　　学校代码：10094

河北师范大学

硕士学位论文

（学术学位）

改进卷积神经网络在网络安全态势评估中的应用研究

Research on the Application of Improved Convolutional Neural Network in Network Security Situation Assessment

作 者 姓 名 ： 宿梦月

指 导 教 师 ： 赵冬梅　教授

一 级 学 科 ： 网络空间安全

二 级 学 科 ：

研 究 方 向 ： 网络安全

论文开题日期： 2022 年 5 月 6 日

摘　要

随着移动设备、云计算等新兴设施和技术的快速发展，存储在网络中的敏感信息数量也快速增长，一旦这些敏感信息遭到攻击，将会造成不可挽回的伤害。为了维护良好的网络环境，网络安全态势感知可以对网络运行环境进行评估，及时反应网络安全状况，避免造成重大损失。但是目前存在的网络安全态势评估模型存在准确率不高、参数量过大等问题，因此为了更加准确地对网络威胁进行响应，提高网络安全态势评估的准确率，本文进行了如下研究：

(1)　基于改进 Res2Net 的网络安全态势评估模型

该模型以 Res2Net 为基础框架，引入通道变换注意力机制和条形池化时空全局特征融合单元，对网络流量的时间和空间特征进行融合。条形池化时空全局特征融合单元利用条形池化特殊形状窗口拟合流量数据矩阵结构，将流量数据矩阵中每个元素所在的时间维度和特征变量维度进行全局聚合，有效捕捉特征长距离特征关系。引入通道变换注意力机制与条形时空全局特征融合单元串联组成通道-空间串联模块，对输入特征的通道关系和空间关系进行建模，提高模型特征提取能力，进而实现对网络安全态势评估准确率的提升。

(2)　基于 SaT-CNN 的网络安全态势评估模型

为了提高训练速度并维持高准确率，提出一种以 CNN 为基础框架，由一种时空信息联合提取模块堆叠而成的网络安全态势评估模型。其中时空信息联合提取模块从空间和时间角度对空间信息提取单元和时间信息提取单元并联，空间信息提取单元引入非对称卷积对空间特征表达能力进一步加强，时间信息提取单元则利用多尺度卷积构成双重时间窗口对短时、长时时间关联进行提取，增加时间信息多样性，之后通过门控机制进行将输出的包含空间和时间信息的特征图自适应融合，增强特征表达能力。

(3)　为了验证所提出的两组基于卷积神经网络的网络安全态势评估模型的有效性，在 UNSW-NB15 数据集中进行实验。通过对模型训练和测试的各项指标进行分析，证明本文提出模型在网络安全态势评估中的准确率有所提升。

关键词：网络安全　态势评估　卷积神经网络　特征空间　时间特征

Abstract

With the rapid development of emerging facilities and technologies such as mobile devices and cloud computing, the amount of sensitive information stored in the network is also growing rapidly, and once this sensitive information is attacked, it will cause irreparable harm. In order to maintain a good network environment, network security situation awareness can evaluate the network operating environment, timely reflect the network security situation, and avoid causing major losses. However, the current network security situation assessment model has problems such as low accuracy rate and excessive number of parameters, so in order to respond to cyber threats more accurately and improve the accuracy of network security situation assessment, the following research is carried out:

(1) Network security situation assessment model based on improved Res2Net

Based on Res2Net, the model introduces the channel shift attention mechanism and the spatiotemporal global feature fusion unit of bar pooling to fuse the temporal and spatial characteristics of network traffic. The spatiotemporal global feature fusion unit of bar pooling uses the special shape window of bar pooling to fit the flow data matrix structure, and globally aggregate the time dimension and feature variable dimension of each element in the flow data matrix, effectively capturing the long-distance feature relationship of features. The channel transformation attention mechanism and the bar spatiotemporal global feature fusion unit are introduced to form a channel-space series module to model the channel relationship and spatial relationship of the input features, improve the model feature extraction ability, and then improve the accuracy of network security situation assessment.

(2) Network security situation assessment model based on SaT-CNN

In order to improve the training speed and maintain high accuracy, a network security situation evaluation model based on CNN framework is proposed and stacked with a joint spatiotemporal information extraction module. Among them, the spatiotemporal information joint extraction module connects the spatial information extraction unit and the temporal information extraction unit in parallel from the spatial and temporal perspectives, the spatial

information extraction unit introduces asymmetric convolution to further strengthen the spatial feature expression ability, and the time information extraction unit uses multi-scale convolution to form a double time window to extract short-term and long-term time associations to increase the diversity of temporal information, and then adaptively fuses the output feature map containing spatial and temporal information through the gating mechanism to enhance the feature expression ability.

(3) In order to verify the effectiveness of the proposed two sets of network security situational awareness evaluation models based on convolutional neural networks, experiments were carried out in the UNSW-NB15 dataset. By analyzing the various indicators of model training and testing, it is proved that the accuracy of the proposed model in the network security situation assessment is improved.

Key Words: Network security, Situation assessment, Convolutional neural network, Feature space, Time feature

目　录

1 绪论.....1
1.1 研究背景及意义.....1
1.2 国内外研究现状.....3
1.2.1 基于数学模型的网络安全态势感知.....3
1.2.2 基于概率和知识推理的网络安全态势感知.....4
1.2.3 基于模式识别的网络安全态势感知.....5
1.3 本文主要研究内容.....7
1.4 论文组织结构.....7
2 相关研究理论.....9
2.1 网络安全态势感知相关定义.....9
2.1.1 态势感知.....9
2.1.2 网络安全态势评估.....10
2.2 卷积神经网络.....12
2.2.1 基本结构.....13
2.2.2 优化算法.....16
2.2.3 正向传播和反向传播.....18
2.3 数据集和时间序列化.....20
2.3.1 多变量时间序列的定义.....20
2.3.2 数据集.....21
2.3.3 数据预处理和时间序列化.....22
2.4 本章小结.....24
3 基于改进 Res2Net 的网络安全态势感知评估研究.....25
3.1 改进 Res2Net 模型构建.....25
3.1.1 Res2Net.....26
3.1.2 GCT 注意力机制.....27
3.1.3 条带池化时空全局特征融合单元.....30
3.1.4 通道-空间串联模块.....32
3.2 基于改进 Res2Net 网络安全态势感知评估过程建立.....33
3.3 实验结果与分析.....34
3.3.1 实验环境.....34
3.3.2 网络安全态势值量化.....34
3.3.3 实验指标.....35
3.3.4 UNSW-NB15 数据集实验结果分析.....36
3.4 本章小结.....40

4 基于 SaT-CNN 的网络安全态势评估研究 41
4.1 SaT-CNN 模型构建.....41
4.1.1 时空信息联合提取模块.....42
4.1.2 空间信息提取单元.....44
4.1.3 时间信息提取单元.....46
4.2 基于 SaT-CNN 网络安全态势评估过程建立 48
4.3 实验结果与分析.....49
4.3.1 实验环境及训练过程.....49
4.3.2 UNSW-NB15 数据集实验结果分析 50
4.4 本章小结.....54
5 总结与展望.....55
5.1 工作总结.....55
5.2 局限性与展望.....56
参考文献.....57

1 绪论

1.1 研究背景及意义

伴随着网络的蓬勃发展，网络空间已成为最大的“虚拟国家”。自 1969 年发明网络以来，网络空间与现实空间相互影响，相互渗透，成为政治、经济、文化、社会、国防等方面不可或缺的存在。如今，人类的生产生活也因为网络的存在发生翻天覆地的变化，衣食住行要依靠手机、电脑提供的互联网服务；在疫情的冲击下，学校教学课程的正常进行、企业日常事务的处理也都依赖着网络平台。网络发展至今已经深入到世界每个角落，与人类形影不离，如今每个人只需要在网络设备上简单操作就可以获取全世界的信息。

我国在 1994 年接入互联网以后，一直致力于网络空间发展，不断扩大信息基础设施规模，网络用户数量增长迅速，已经成长为网民数量第一的国家。根据世界互联网大会发布的《中国互联网发展报告 2022》蓝皮书记载，截至 2022 年 6 月，中国网民规模达到 10.51 亿，互联网普及率达到 74.4%；随着 IPV6 的升级改造，截至 2022 年 7 月，中国 IPv6 活跃用户数达 6.97 亿[1]。这几个庞大的数字证明我国网络建设的发展速度和网络用户规模增长速度是非常迅速的。这些年我国采取按照积极利用、科学发展、依法管理和确保安全的方针发展网络空间，保障网络空间的安全运行。由于网络发展带来越来越复杂的网络情况，因此我国相继出台多部法律法规完善网络空间治理法律体系，“十四五”规划提出要建设智慧城市和数字乡村，并且统筹营造良好的数字生态，加强网络安全保护，健全网络空间基础设施建设，完善网络空间治理体系，切实保护网络用户的合法权益[2]。网络安全关乎政权稳固、经济发展、科技进步和社会和谐，是国家总体安全的重要构成，维护网络空间安全已经成为我国未来科技发展的一大重点。

尽管我国持续发展网络空间建设，但是距离成为网络强国还有一段距离。如今，网络空间已成为和陆、海、空、天并列交织的第五维空间，关乎政权稳固、国防安全、社会稳定、经济发展和科技进步，具有高度的战略价值，牵一发而动全身。我国网络空间面临的安全威胁和风险隐患将持续存在，后疫情时代的网络安全局势更加深化复杂，不断扩大的网络基础设施日后也许会成为实体战争的诱饵，网络攻击层出不穷，主体、目标、手段和影响呈现出新的特点，治理网络空间面临着严重的挑战。

当前，新一轮科技革命和产业变革持续推进，疫情对世界经济的发展造成巨大的冲击，全球性问题加剧，这些因素导致网络空间安全的形势日渐复杂，同时也增加了网络空间安全治理的难度。欧盟网络安全局（ENISA）发布的《2021 年威胁态势报告》称，在 2020 年因疫情所发生的 DDoS 攻击大幅增加，攻击频率在 2020 年最后 6 个月增加 22%[3]。2020 年 12 月，美国“火眼”（FireEye）公司在审计中发现“太阳风”公司的 Orion 软件更新包中被植入后门，美国政府多个部门遭到入侵[4]。随后，2021 年由于虚拟加密货币的快速增值，DDoS 勒索攻击抬头，攻击方式从大规模通用攻击转变为更加具有针对性的攻击，运行模式也对应升级为“三重勒索”。政府实体、国防承包商、关键基础设施等组织机构成为主要攻击目标。2021 年 5 月，美国最大成品油管道运营商科洛尼尔管道运输公司遭到勒索软件攻击，5500 英里输油管被迫停运，导致美国多个州进入紧急状态，燃油供给遭受限制[5]。2022 年初，随着俄罗斯和乌克兰冲突加剧，网络安全事件频频发生，双方在对抗中没有忽视网络空间的影响，在虚拟空间中构建大批前沿阵地，组合运用分布式拒绝服务攻击、恶意软件、钓鱼攻击等手段，将火力覆盖至敌方网络领域，导致其政府、银行、网站瘫痪数小时,影响社会秩序[6]。瑞星公司发布的《2020 中国网络安全报告》显示[7]，该公司安全系统在 2020 年截取的病毒样本量高达 1.48 亿个，其中攻击类型包括木马、蠕虫、后门等，具体分布如下图 1.1 所示，攻击目标主要是政府和军工领域，因此采取有效措施对网络安全状况进行全局控制刻不容缓。

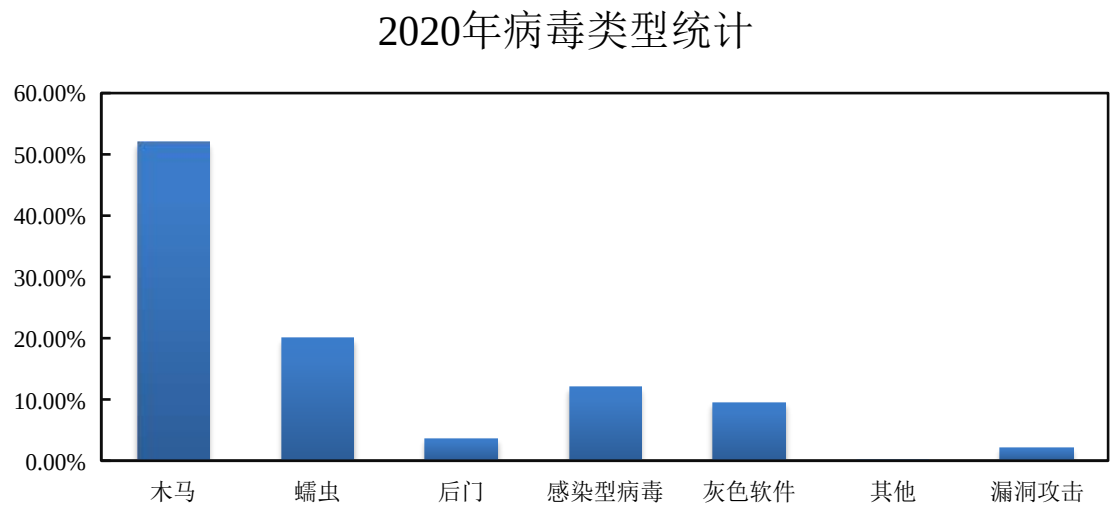


图 1.1　2020 年病毒类型分布统计

伴随着互联网、大数据、云计算的飞速发展，人类对网络空间依赖度的提高和网络资产数量的增加一定程度上增加网络数据暴露的风险。如此复杂的网络空间安全问题，

对于当前的网络安全态势感知研究也提出新的要求，如何准确快速的识别出攻击行为，并对此行为做出及时的处理策略成为目前的研究要点。许多学者针对此方面进行颇多研究，采用多种方法对网络流量的攻击行为进行识别，提高攻击行为的准确率，并计算当前网络空间安全态势情况，希望借此掌握网络空间的运行状况，提高网络的防御能力。但是在越来越复杂的网络环境中，流量数据结构发生变化，结构繁琐，处理困难，特征之间的关联难以分析，给网络安全态势分析带来一定的困难。

深度学习是机器学习的一个分支，依靠神经网络对输入数据进行特征信息提取，删除错误信息，随后根据这些信息去模仿人类的一个决策过程。卷积神经网络近几年在图片处理领域大放异彩，可以处理高维度、特征结构复杂的图片，具有非常强大的非线性特征学习能力。基于此，本文尝试使用卷积神经网络作为基础网络模型，结合网络流量数据的时间关联和特征空间关联，构建合适的特征提取模块对数据进行时间、空间上的特征关系进行建模，借此提高网络安全态势评估的准确率。

1.2 国内外研究现状

网络安全态势感知由 Tim Bass[8]将态势感知引入网络安全领域而来，发展至今拥有许多经典模型，总结下来网络安全态势感知分为三个步骤，分别是提取、评估和预测。目前应用于网络安全态势感知的研究方法如表 1.1 所示，下面将从以下三类方法对当前研究现状进行介绍。

表 1.1 网络安全态势感知方法

研究方法类型	主要思想	代表方法
基于数学模型	利用相关数学表达式，建立安全事件和态势值的对应关系	层次分析法、模糊综合评价法、集对分析法等
基于概率和知识推理	依靠专家经验和先验知识，采用逻辑推理计算安全态势	贝叶斯网络、马尔可夫博弈模型、D-S 证据理论等
基于模式识别	通过对模型的训练，自适应学习调整权值，得到输入与输出之间的关系	机器学习分类算法、深度学习分类算法、集成模型等

1.2.1 基于数学模型的网络安全态势感知

所谓基于数学模型即利用明确的数学表达函数，将分析出的态势元素集合和态势值

空间的映射关系。这类方法是网络安全态势研究中应用范围最广的一种法，代表性方法有层次分析法、集对分析法、模糊综合评价法等。由于从传感器收集的数据类型多样，所提取的态势元素具有复杂不确定的因素，这些元素具有层次结构，可以将这些难以量化的元素层层划分，使之具有条理性。层次分析法主要是利用该方法对复杂的态势元素进行层次切分，通过一个构造矩阵，得到目标元素的权重系数，对这些数值一一比对，确定他们的重要性顺序。陈秀真等[9]提出一种基于层次分析法的网络安全态势评估模型，该模型将网络按照规模分解为多个层次，分层对威胁状况因子进行计算，按照警报频率对其进行加权，计算整个网络的威胁指数，评估网络安全状况。Wang 等[10]则利用层次分析法对网络中存在的态势元素赋予权重值，避免权重因为主观因素而受到影响。韩晓露等[11]考虑到当今大数据环境下数据量爆炸式增长等原因，采用层次分析法建立态势评估指标体系，通过建造的直接模糊关系矩阵计算网络的综合评估值。FAN 等[12]将模糊认知图与层次分析法进行结合，利用模糊认知图对网络安全风险事件进行评估和量化，之后按照相关风险等级确定态势状况。Zhao 等[13]将网络结构和网络行为综合考虑，将 AHP 和通用脆弱性评分系统（CVSS）进行结合，提出一种基于微分流形的层次评估方法，从多角度综合分析网络态势状况，具有较好的实时性。Zhao 等[14]利用模糊粗糙集对数据进行归约，降低数据复杂度，之后采用组合分类器和粒子群算法对态势元素进行提取，减少提取时间。Alali 等[15]基于脆弱性、威胁、可能性和影响四个风险因素结合模糊推理模型生成风险评估结果，得到可能受到威胁的目标范围。Doynikova 等[16]基于 CVSS 评分系统对网络特征、攻击特征、对策等指标进行集合，对安全信息进行分析，不同的输入数据结合不同的评估方法，从而对准确性和效率进行提升。

1.2.2 基于概率和知识推理的网络安全态势感知

概率和知识推理是依靠先验知识和概率，对安全态势采用逻辑推理的方法进行计算，最常用的方法有贝叶斯网络、马尔可夫博弈模型、D-S 证据理论等。基于知识推理的方法极其依赖专家积累的大量经验和先验概率，将这些已经存在的数据作为基础，利用模型学习专家的思考过程，模拟专家行为做出对应的决策。此类方法计算基础的态势评估结果处于离散的数值空间，对于评判网络空间的运行状况带有直观效果，方便简洁。Liao 等[17]使用扩展隐马尔可夫模型进行网络安全态势评估，定义状态转移矩阵的初始算法，融合多个系统的安全数据，通过推导出的隐状态概率分布序列求解当前网络态势

值。网络中包含多种设施，Hu 等[18]提出一种多维网络风险评估方法，使用隐马尔可夫模型对网络风险进行计算，利用网络节点关联提高风险评估的可靠性，及时反映态势状况。张恒巍等[19]建立了非合作非零和攻防博弈模型，针对攻防之间的目标对立性、非合作关系等特征，将防御方反击获得的收益考虑在内，对博弈均衡的混合策略进行分析，实现对攻击的有效预测。Niazi 等[20]提出一种基于贝叶斯和博弈论的评估模型，通过管理源和受损主机发起攻击的请求源之间进行的非合作动态贝叶斯博弈过程，提高检测概率并尽量减少误报。Lin 等[21]提出了一种基于贝叶斯攻击图和大数据的动态网络安全态势检测方法，利用大数据技术融合网络安全态势因素，然后利用漏洞预测算法实时预测未来漏洞数量，最后将新漏洞与贝叶斯攻击图相结合，推断攻击者后续的攻击行为。Li 等[22]将多个模型处理数据得到的概率值利用 D-S 理论对其进行融合，从而对网络安全进行分析。以上方法在数据量小时表现出不错的效果，但是随着网络规模越来越大，数据量呈指数级发展，对这些数据处理花费的成本和效率也需要考虑在内。

1.2.3 基于模式识别的网络安全态势感知

模式识别是利用计算机学习人类的大脑思考过程，根据数据的特点将其进行类别划分。这类方法对于态势感知而言，重点关注提取出的各种数据的特点，经过模型分析和学习，掌握每种攻击类型的特征，根据这些学习能力判断实测数据和训练数据之间的相似性，如果相似度达到我们事先规定的阈值，那么可以给予实测数据一个类型标签，确定它的态势状态。常用的方法有机器学习分类算法、深度学习分类算法、集成模型等。

机器学习是人工智能的一种应用，可以对输入数据进行特征分析，将获得特征的分布进行学习，从而根据过去的信息预测未来的状况[23]。许多模型采用机器学习算法为模型，添加参数优化方法，例如 Chen 等[24]通过引力搜索算法和支持向量机的组合对网络安全态势进行预测，引力搜索算法具有快速收敛的优点，帮助支持向量机进行优化；Hu Jingjing 等[25]为了减少模型训练时间，采取 MapReduce 进行分布式训练来提高训练速度，以支持向量机为基础模型，使用布谷鸟搜索算法进行参数优化，该方法减少了时间成本并且准确率有所提高；Zhao 等[26]将哈里斯鹰优化算法与卷积神经网络进行结合，对网络态势进行评估。Wang 等[27]利用粒子群优化算法对径向基网络进行优化，模型准确率得到提高；程家根等[28]利用模拟退火算法和混合递阶遗传算法优化径向基网络，两个算法之间相互补充，优化网络参数。王金恒等[29]结合遗传优化算法对概率神经网络的

修正因子进行优化，提高训练速度和准确率。

人工智能的发展使得深度学习应用广泛，可以对网络威胁进行分类和测试，在此之前的方法致力于对具有某些特征的攻击方式进行建模，但是这些特征并不具有鲁棒性，使用深度学习还可以面对更加复杂的威胁和攻击[30]。Yannis Nikoloudakis 等[31]采取神经网络检测发生的网络攻击，根据已知漏洞进行评估，提高了准确率。常用的深度学习方法是循环神经网络（Recurrent Neural Networks，RNN）和卷积神经网络（Convolutional Neural Networks，CNN）以及它们的变体。通过长短时神经网络（Long Short-Term Memory，LSTM），可以对数据的时间关联进行建模，CNN 使用原始数据作为网络的直接输入，参数相对较少，在图像识别领域具有很大优势。Dong 等[32]提出一种 LSTM 神经网络网络安全态势感知方法，通过 LSTM 网络挖掘态势数据的时间相关性，结合 Sigmoid 线性函数与布谷鸟搜索算法增强非线性能力和参数寻优速度，减少模型训练时间。随着网络结构日渐复杂，我们很难从客观角度出发，做出不带有主观性的决策，因此，在近期的研究中，学者们往往采用神经网络结合一些注意力机制模型应用于复杂的网络系统中[33]。Li 等[34]采用双重注意力机制，将流量特征分别提取，提高预测效率。何春蓉等[35]提出一种基于注意力机制的循环门控单元网络，深度挖掘数据之间的时间相关性，利用注意力机制为安全指标分配权重，结合粒子群算法优化模型参数，可以减小预测误差。YAO 等[36]将双向长短时神经网络结合时序卷积网络对网络安全态势数据进行处理，与传统方法相比更具有鲁棒性，更好地处理时间方面的关联。由于循环神经网络只能针对流量中的时间特征进行提取，不能对流量特征空间关联进行分析，所以张任川等[37]利用 CNN 的优点，结合深度可分离卷积和卷积分解对流量数据进行特征提取，减少训练时间并提高准确率。P. Nirmala 等[38]使用空洞卷积堆叠成自编码器对网络安全数据进行分类，该模型对攻击类型分类具有不错的效率。一些学者将 RNN 和 CNN 进行结合，对时间和空间维度的特征综合考虑。WANG 等[39]将流量转换为图片，利用 CNN 提取图片中的空间特征，之后使用 LSTM 提取蕴含的时间特征关系，通过实验证明将时间特征和空间特征进行联合提取有效增加模型的准确率。CAO 等[40]将 CNN 与 GRU 进行结合提取时空关系，利用池化进一步融合空间特征。

综上所述，虽然 RNN 可以对流量时间特征进行分析，但是存在参数过多，训练速度慢等缺点，因此为了进一步提高训练效率，增强分类能力，本文基于 CNN 对网络安

全态势评估进行研究。

1.3 本文主要研究内容

为了提高网络安全态势评估的准确率和特征提取能力，本文基于改进卷积神经网络对网络安全态势评估进行研究，主要研究内容如下：

(1) 基于改进 Res2Net 的网络安全态势评估模型

该模型以 Res2Net 为基础框架，引入通道变换注意力机制和条形池化时空全局特征融合单元，对网络流量的时间和空间特征进行融合。条形池化时空全局特征融合单元利用条形池化特殊形状窗口拟合流量数据矩阵结构，将流量数据矩阵中每个元素所在的时间维度和特征变量维度进行全局聚合，有效捕捉特征长距离特征关系。引入通道变换注意力机制与条形时空全局特征融合单元串联组成通道-空间串联模块，可以对输入特征的通道关系和空间关系进行建模，提高模型特征提取能力，进而实现对网络安全态势评估准确率的提升。

(2) 基于 SaT-CNN 的网络安全态势评估模型

该模型以 CNN 为基础框架，由一种时空信息联合提取模块堆叠而成。时空信息联合提取模块首先由空间信息提取单元和时间信息提取单元并联，之后将输出的包含空间和时间信息的特征图通过门控机制进行融合。空间信息提取单元利用非对称卷积和普通卷积对网络流量矩阵进行局部特征提取，基于卷积可加性对空间特征表达能力进一步加强；时间信息提取单元则采用多尺度卷积构成双重时间窗口对短时、长时时间关联进行提取，增加时间信息多样性；门控融合机制将时间和空间信息自适应分配权重，有选择的加强或削弱特征信息。该模型可以有效对网络流量的时间和特征空间关联进行分析，增强特征表达能力，减少模型参数和训练时间，并且保持高准确率。

(3) 为了验证所提出的两组基于卷积神经网络的网络安全态势感知评估模型的有效性，在 UNSW-NB15 数据集中进行实验。通过对模型训练和测试的各项指标进行分析，证明本文提出模型在网络安全态势评估中的准确率有所提升。

1.4 论文组织结构

本文提出两种基于改进卷积神经网络的网络安全态势评估模型，共分为五个章节对其进行阐述，具体安排如下：

第一章为绪论。首先介绍当今互联网的发展状况，讨论网络安全态势感知研究对当

今互联网发展的意义。之后系统介绍网络安全态势感知国内外的研究现状，最后介绍论文的主要研究内容和论文组织结构。

第二章为相关研究理论。第 1 节对态势感知和网络安全态势感知的定义进行介绍；第 2 节介绍卷积神经网络相关知识，包括卷积神经网络的基本结构、参数优化算法和参数正向传播和反向传播；第 3 节介绍多变量时间序列的定义和数据集的基本信息和预处理过程。

第三章为基于改进 Res2Net 的网络安全态势感知评估研究。第 1 节介绍本章所构建的网络模型的基本结构和搭建原理；第 2 节对态势评估流程进行叙述；第 3 节是实验仿真与结果分析，通过模型在数据集中的表现分析模型的学习能力。

第四章为基于 SaT-CNN 的网络安全态势评估研究。第 1 节介绍本章节所构建的 SaT-CNN 神经网络的基本架构和详细组成；第 2 节对整个网络安全评估流程进行叙述；第 3 节是实验仿真与结果分析，介绍该模型在数据集中的表现能力。

第五章为总结与展望。对整篇论文所做的工作进行总结，并提出未来工作的研究方向。

2　相关研究理论

本章节对于涉及的主要研究理论进行阐述，介绍网络安全态势感知和卷积神经网络的基本理论，为后面的研究夯实基础。首先介绍网络安全态势感知的相关定义，对于网络安全态势感知核心理论进行叙述。其次，因为本文主要利用卷积神经网络进行改进，所以具体介绍了卷积神经网络基本结构、优化算法和参数正向和反向传播。最后介绍本文实验所用的数据集和时间序列化过程。

2.1　网络安全态势感知相关定义

本小节介绍态势感知的起源和基本概念，解释态势感知如何进入网络安全领域生成网络安全态势感知这一概念的发展历程。

2.1.1　态势感知

态势感知（Situational Awareness，SA）起源于 20 世纪八十年代，最初是为满足二战后美国空军对于战争的需要而提出。在军事行动中，复杂多样的作战环境给情景评估带来许多困难，现场存在许多噪声、烟雾，并且环境瞬息万变，如何准确评估当前的情况成为难点。态势感知的明确定义由 Endsley[41]在 1988 年提出，认为态势感知具有三个层次，分别是认知、理解和预测，即通过对时间和空间中的环境信息进行认知，分析它们在此时此环境中表现的特点和意义，从而对于未来状态更好地预测。图 2.1 即为 Endsley 给出的飞行员决策模型。

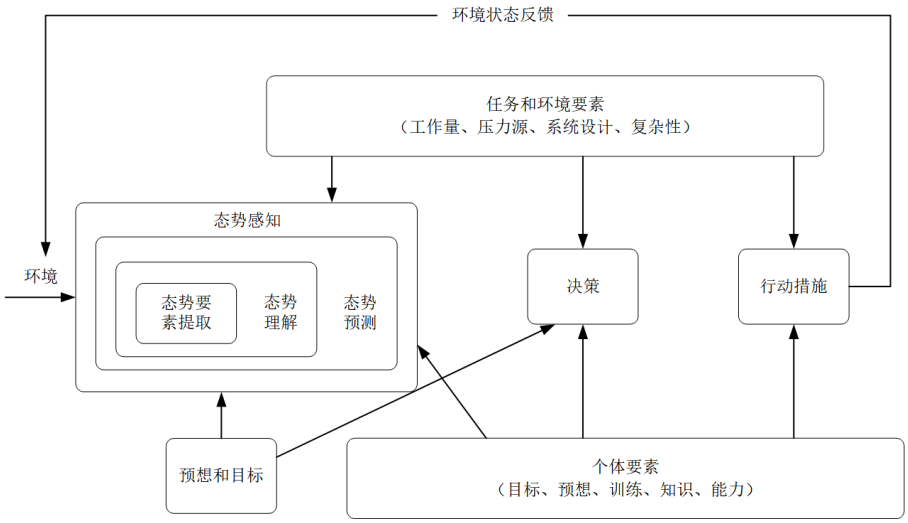


图 2.1　Endlsey 态势感知模型

在军事领域，态势感知主要是收集士兵的战场数据进行分析，掌握不同环境的作战特点，从而帮助飞行员在执行任务时通过分析环境信息，快速解决当前的形势和未来趋势，执行正确的战术和指令。比如飞行员在执行任务时，首先用自己的感官收集飞行环境中的各类元素以及它们的相关特征，例如驾驶员观察飞机显示器是否提示飞行高度过低或者飞机越过山脉时所感受到周围地势的变化情况，这些元素和特征具有特定的模式，代表态势感知的第一步骤，通过这些环境元素反映的情景进行分析，辅助飞行员做出更为准确的行动计划。完成态势感知的情景信息收集之后，对这些信息进行分析，比如在飞行过程中驾驶员注意到显示器警示灯亮起，代表前方有特殊情况发生，附近可能有敌机靠近，驾驶员将会针对警示灯的信息做出相对应的对策。通过理解数据的信息，将特定目标与收集的信息相互关联，从而完成对战争环境的态势评估。之后分析敌军飞机的数量和飞行方向是否影响自己的任务，制定相对应的反映策略和措施。通过当前已知数据来预见未来将会发生事件的可能性，不断地前向映射，制定解决方案就是态势感知的第三步，对未来态势发展进行预测。

2.1.2 网络安全态势评估

网络安全态势感知（Network Security Situation Awareness，NSSA）由 Tim Bass 在 1999 年提出，是从态势感知演变而来。NSSA 可以通过海量的网络数据全面、动态地监测网络空间的安全风险，对当前的运行状况进行理解分析，因为网络攻击具有很强的隐蔽性，因此要重点注意携带攻击特征的流量，分析是否为恶意攻击，预估该攻击会造成多少范围的危害，及时确定处理的策略，避免造成不可挽回的后果。网络安全态势感知系统的分析数据来源依赖于终端，防火墙、日志文件系统等设施记录的信息更加详细和具体，与原始数据包相比，生成的数据也更为具象化。

Endsley 指出态势感知是由自下而上的数据驱动和自上而下的目标驱动相互交替运行的，因此数据在态势感知中是尤为重要的。当前许多网络安全设施的数据结构多种多样，为更好地适应结构多样的数据，美国数据融合实验室将多个数据源产生的异构数据进行融合，提出 JDL 数据融合模型[42]，该模型将数据源到终端使用者之间的过程分为五个层次，提取网络中不同的目标进行融合，经过不同级别的处理和反馈，对网络安全态势有一个清楚的分析，从而帮助网络管理人员对网络中发生的状况采取措施进行应对。在此基础之上，Tim Bass 等认为，应该从异构数据进行融合的角度出发，搭建网络

安全态势感知模型。也就是说，要从网络数据出发，才能更好地分析网络安全态势。因此，在 JDL 数据融合模型基础之上提出一种基于多源异构数据的网络安全态势感知功能模型，具体结构如下图 2.2 所示。

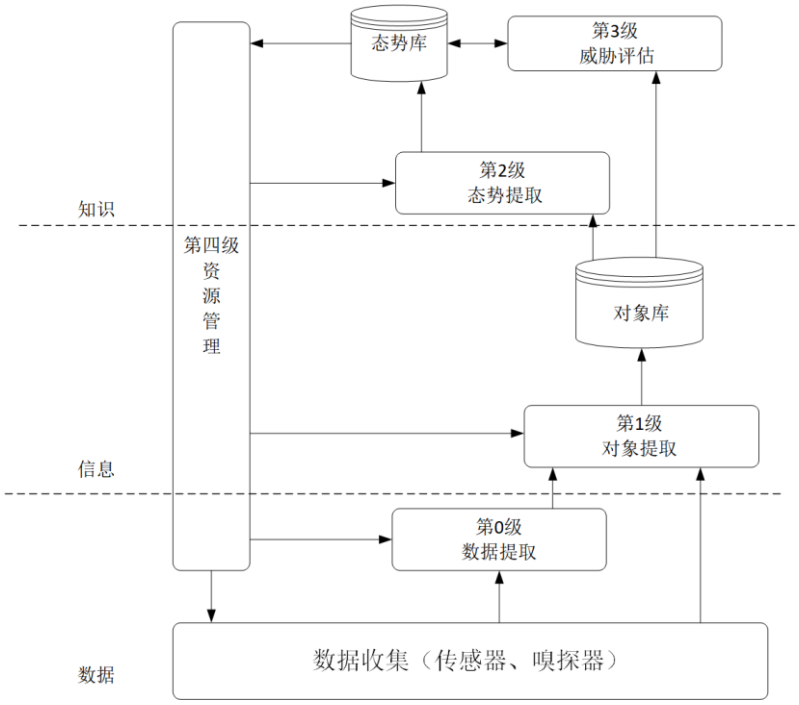


图 2.2　网络安全态势感知数据融合模型

该模型共分为三个层次，分别是数据、信息和知识。首先在网络传感器这端收集需要分析的态势数据，这些数据用作态势感知的后续分析。之后分析提取的数据关联，将不同的目标实体加入对象库。最后是关联提取出的关键数据，对这些数据进行网络环境态势评估，分析当前环境是否存在威胁，以及对未来网络产生的不良影响进行评估。在这个过程中，资源管理处于一个管理员的位置，负责调度相关资源，实时监控整个态势感知流程。

在网络安全态势感知的发展历程中，提出了几十种网络安全态势感知模型，比如 Boyd 控制循环模型（OODA），但是最为基础的还是最初的 Endsley、JDL 和 Bass 模型，这些模型为后续态势感知的发展打造坚实的基础。归根究底，这些模型的功能和目的是一致的，即对网络安全态势要素的提取、评估和预测。本篇文章的工作主要对网络安全态势评估进行。

网络安全态势评估在网络安全态势感知研究中起到非常关键的作用，它是指利用一些方法对收集的具有实时性的网络安全事件和流量数据进行分析和学习，及时发现网络

中存在的安全威胁，从而对网络系统整体的威胁风险和影响范围进行评估，实时反映整个系统的运行状况，帮助管理人员掌握当前网络安全情况，当危险到来之前可以采取一些对应措施来防范或者减少网络攻击产生的伤害。态势评估主要依赖于多元分布式传感器收集的各项数据，通过关联和整理这些数据，提取出更加准确全面、具有代表性的特征信息，继而按照所构建的网络安全态势值评估方法进行计算，得到当前网络环境安全状况的一个具体数值或者定性描述，这些数据便作为判断整体网络运行状况的依据。网络态势评估等价于一个函数映射出的数据特征和态势值之间的关系，它侧重于评估网络威胁发生后产生的后果，所计算的安全态势值的大小随着网络安全状况的变化而变化。

2.2 卷积神经网络

人工神经网络是将生物神经元的连接模拟为神经元节点之间的权重值，这些权重经过激活函数的计算，与输出形成非线性映射关系，输出激活后的数值。经过这些操作之后的模型增强非线性表达能力，可以拟合更多类型数据的特征分布。卷积神经网络作为人工神经网络的一种，起源于对动物大脑视觉皮层的研究中发现“感受野”，即对输入图像空间的某一部分非常敏感，通过“感受野”将整个空间进行覆盖，得到完整的图像空间视野。许多学者针对此类现象进行许多研究，搭建出了第一个 CNN 实现网络。之后随着深度学习的广泛应用，卷积神经网络在图像分类、ECG 分析、网络安全等领域均得到很好的应用。

近年来，CNN 得到极大的发展，衍生出许多具有代表性的模型。AlexNet 是 2012 年由 ALex 和 Hinton 提出的一种卷积神经网络[43]，以高准确率获得 ILSVRC 比赛的冠军，引入 Relu 函数代替原始的 Sigmoid 激活函数，提高训练速度。VGG 模型在 2014 年提出，该模型叠加多个卷积层，并且采用小型卷积核替代 ALexNet 中的较大卷积，网络层的增加从而提高网络的非线性拟合能力，使得该模型可以学习更加繁琐的特征表达。GoogleNet 系列[44]改善多层次卷积堆叠带来的参数过大、模型难以优化等问题，采用多分支结构，并行处理输入的数据，增加特征表达的多样性。2015 年，何凯明等[45]提出一种具有跳跃连接的卷积神经网络 ResNet，通过构建残差模块去改善由于网络层数过深产生的梯度消失和梯度爆炸问题，并且加速网络训练的收敛[46]。总而言之，卷积神经网络存在权重共享和平移不变性的特点，可以减少网络参数的训练数量，具有很强的特征提取能力。作为深度学习中的一个重要分支，利用卷积提取特征时，像一枚印章按照均匀的步

长向前移动，对输入的数据进行信息提取。在面对计算量庞大的数据时，卷积神经网络可以并行提取特征，计算速度有所提升。

2.2.1 基本结构

卷积神经网络基本结构如下图 2.3 所示，一般存在一个输入层和输出层，具体网络结构由卷积层、池化层、全连接层堆叠而来。

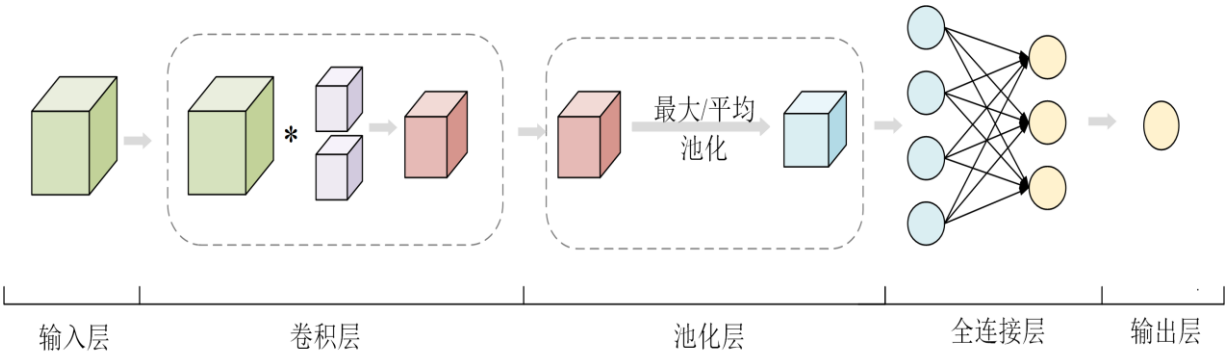


图 2.3 卷积神经网络基本结构

(1) 输入层

在此层中，主要作用是对输入网络的数据进行转换，方便后续神经网络进行处理，可以输入一维或多维数据。在本研究领域中，网络流量数据经过时间序列化转换为单通道二维矩阵进行输入。

(2) 卷积层

卷积层是主要利用一个提前设置好尺寸的卷积核（滤波器），在输入特征图上沿着固定方向移动，每次滤波器覆盖的特征元素按照固定公式进行计算。卷积操作用于提取输入中的局部区域特征，局部区域大小按照卷积核大小决定，每个卷积覆盖下的元素经过计算均集中在输出的一个元素上，将整个输入特征图具有的特征进行提取。卷积操作如图 2.4 所示，一个大小为4×4的特征矩阵，经过一个3×3大小的滤波器，按照步长为 1 沿着从左到右、从上到下方向移动，每次覆盖 9 个特征元素，将滤波器矩阵与覆盖子矩阵按照元素相乘，它们的相加之和就是这种特征图输出的一个元素。假设有一输入为 X，K 表示大小为 $m\times n$ 的卷积核，y 为输出，那么 y 中的每个元素可表示为：

$$y_{(i,j)}=(X,K)_{(i,j)}\sum_{i=0}^{m}\sum_{j=0}^{n}x_{(i+m,j+n)}\cdot\omega_{(m,n)} \tag{2.1}$$

当卷积核在输入图中进行滑动时，为了减少模型训练复杂度，具有局部连接和权重共享的性质。

1)　局部连接

全连接层通过将上层的每个输出元素和当前层的神经元连接，会产生许多参数。如图 2.5 所示，全连接层将上层和当前层的神经元逐一连接，而卷积核关注于局部覆盖的特征区域，即上层神经元只和当前层部分神经元相连。该操作可以减少全连接导致的参数数量，提高模型训练效率，并且因为输入中的特征存在较强的局部相关性，可以通过高层特征聚合增强局部特征信息。

2)　权重共享

卷积核只能捕捉输入图中的一种特定特征，其中的参数不会随着特征变化，如图所示，可发现相同颜色的输出连接是由同一权重计算而来，因此经过卷积计算的输出是由同一卷积核采用相同权重计算而来。不同的卷积核提取不同的特征，即拥有不同的权重。权重共享也可以减少参数数量。

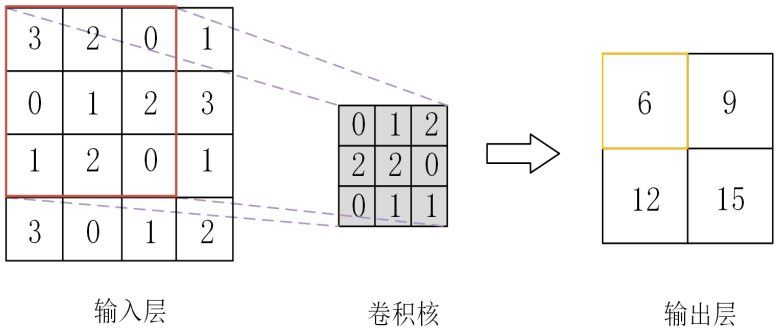


图 2.4　卷积操作示意图

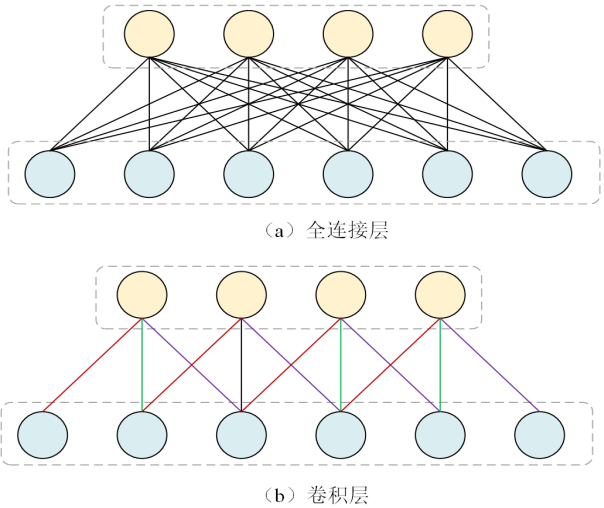
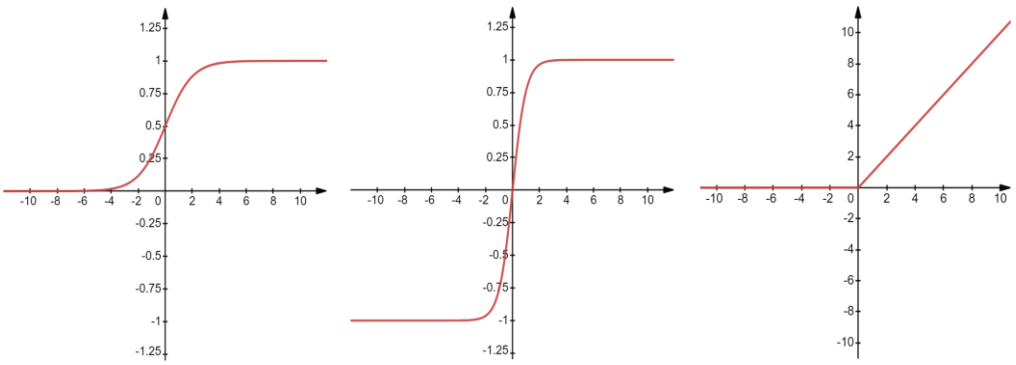


图 2.5　全连接层与卷积层对比

(3)　激活层

激活函数可以增加模型的非线性计算能力，提高数据的拟合程度，使得学出的模型能够较好地识别特征之间复杂的非线性关联性。在网络中，上层的输出值作为当前层的输入，利用激活函数将输入空间映射到输出空间中。常用的激活函数有 Sigmoid 函数、Tanh、ReLu 函数等，函数曲线如图 2.6 所示。



（a） Sigmoid 函数　　（b）Tanh 函数　　（c）ReLu 函数

图 2.6　激活函数图像

Sigmoid 函数具体表示由公式（2.2）所示，输出范围为 0 到 1，伴随着输入值的增大和缩小，该函数所输出的结果梯度逐渐变小，由此导致训练过程中产生梯度消失，影响模型的训练和学习。

$$Sigmoid = \frac{1}{1+e^{-x}} \tag{2.2}$$

Tanh 函数具体表示由公式（2.3）所示，输出范围为-1 到 1，相对 Sigmoid 函数而言收敛速度更快，但是随着输入值增大和缩小，函数梯度趋近于 0，容易导致梯度消失。

$$Tanh = \frac{e^{x}-e^{-x}}{e^{x}+e^{-x}} \tag{2.3}$$

ReLu 函数的具体表示由公式（2.4）所示，输出由输入值正负决定。当输入值属于负值时，函数输出为一直保持为 0，若输入为正时，输出按照将按照梯度为 1 的趋势变化，输出为它本身的值。该函数只需要进行简单加乘便可以加速梯度下降的收敛速度，一定程度上缓解梯度消失问题。

$$Re\,Lu = \begin{cases} 0 & (x \le 0) \\ x & (x > 0) \end{cases} \tag{2.4}$$

(4)　池化层

在数据庞大的矩阵中，充斥着多种信息，通过卷积对其计算可以扩大感受野，对输

入矩阵有一个综合特征提取，但是存在特征维度过高，不易对后续进行分类，易导致过拟合。池化通过构建一个固定大小的窗口在输入图上进行滑动，对窗口覆盖的数据进行计算，筛选去除掉一些非重要信息，余下对于类别有益的信息，并且进一步减少模型参数数量。目前主要使用的有最大池化（Max Pooling）和平均池化（Mean Pooling），最大池化是指在选定范围内，筛选最大值作为这部分的代表值；平均池化是指在这一部分内的元素计算一个平均值代表这部分的特征。图 2.7 所示为设置2×2大小窗口，经过计算输出大小为2×2的池化结果。

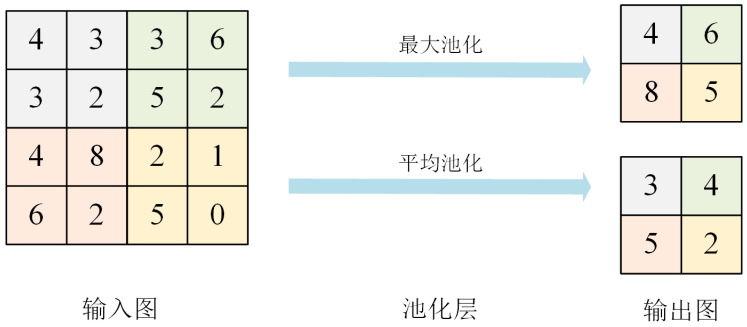


图 2.7　两种池化类型示意图

(5)　全连接层和输出层

全连接层对于分类任务而言，常和 Softmax 函数结伴而行。通过全连接层可以将二维矩阵平铺成一个一维向量，之后与权重矩阵相乘，再加上偏置，经过非线性组合计算的向量利用 Softmax 函数将每个类别的概率在 0 到 1 的范围进行映射。

2.2.2　优化算法

模型学习过程中参数学习是为了达到损失函数的最小值，梯度下降方法可以让损失函数快速达到局部最低点，加快训练速度，使得网络优化更加稳定。常用梯度下降包括三类方法，分别是随机梯度下降（Stochastic Gradient Descent，SGD）、批量梯度下降（Batch Gradient Descent，BGD）和小批量梯度下降（Mini-Batch Gradient Descent，MBGD）。

对于神经网络$f\left(x,\theta\right)$而言，输入样本数为m，损失函数为$J\left(\theta,x,y\right)$。SGD 在每一次迭代是采用一个样本进行梯度更新，可表示为：

$$\theta_t=\theta_{t-1}-\eta\cdot\nabla_\theta J_i\left(\theta_{t-1},x_i,y_i\right) \tag{2.5}$$

但是每次迭代只用一个样本，如果遇到数据量大时，只使用部分样本可能就会到达最优

点，局部收敛并不能代表所有样本的趋势。

BGD 每次训练采用全部样本进行迭代，如果每次迭代选取样本数目为m，最终参数更新表示为：

$$\theta_t = \theta_{t-1} - \eta \cdot \frac{1}{m} \sum_{i=1}^{m} \nabla_\theta J_i\left(\theta_{t-1}, x_i, y_i\right) \tag{2.6}$$

每次迭代需要所有样本，会需要大量计算资源，减缓训练速度。

MBGD 进一步改进 BGD 的缺点，每次迭代采用部分样本，如果每次迭代选取k个样本，参数更新可表示为：

$$g_t = \frac{1}{k} \sum_{i=1}^{k} \nabla_\theta J_i\left(\theta_{t-1}, x_i, y_i\right) \tag{2.7}$$

$$\theta_t = \theta_{t-1} - \eta \cdot g_t \tag{2.8}$$

公式中η代表学习率，用于控制每次权重更新量，如果学习率选取过小会导致收敛速度减慢，设置过大会导致收敛过程不断震荡，无法收敛至最优。动量法基于物理学动量概念，将最近一段时间的梯度加权平均作为更新方向。引入动量因子ρ，代表历史梯度对当前梯度的影响，当这段时间梯度方向不一致时，参数的更新幅度减小，梯度方向一致时，参数加快更新，具体过程如下，g_t代表第 t 次迭代更新梯度：

$$m_t = \rho m_{t-1} + \eta g_t \tag{2.9}$$

$$\theta_t = \theta_{t-1} - m_t \tag{2.10}$$

基于学习率设置不当会导致训练震荡，RMSprop 算法计算梯度平方加权平均值，设置衰减率β控制历史信息获取量，使得学习率不会一直衰减，可以进行调整，其中ε是为了保持数值稳定设置的极小数：

$$r_t = \beta r_{t-1} + \left(1-\beta\right) g_t \odot g_t \tag{2.11}$$

$$\theta_t = \theta_{t-1} - \frac{\eta}{\sqrt{r_t + \varepsilon}} \odot g_t \tag{2.12}$$

Adam 算法结合动量法和 RMSprop 算法的优点，对梯度进行一阶矩衰减系数（平均值）和二阶矩衰减系数（方差）计算，即对梯度和梯度平方进行加权平均：

$$m_t = \beta_1 r_{t-1} + \left(1-\beta_1\right) g_t \tag{2.13}$$

$$r_t = \beta_2 r_{t-1} + (1-\beta_2) g_t \odot g_t \tag{2.14}$$

β^1 和 β^2 为衰减率。由于加权平均值在初期会与真实的均值和方差有一定差距，尤其是当衰减率均趋近于 1 时，偏差会增加，因此需要对 m_t 和 r_t 进行修正：

$$\hat{m}_t = \frac{m_t}{1-\beta_1^t} \tag{2.15}$$

$$\hat{r}_t = \frac{r_t}{1-\beta_2^t} \tag{2.16}$$

参数更新如下：

$$\theta_t = \theta_{t-1} - \frac{\eta}{\sqrt{\hat{r}_t} + \varepsilon} \odot \hat{m}_t \tag{2.17}$$

2.2.3 正向传播和反向传播

卷积神经网络的训练过程中，输入图经过多个卷积层和池化层组成的网络层处理，其中卷积和池化通过内部参数进行特征提取。因此网络层通过初始设定的参数进行特征计算，之后根据损失函数值进行反向传播学习参数。

(1) 前向传播

1) 卷积层前向传播

对于卷积层的前向传播一般为输入层与卷积层之间、隐藏层与卷积层之间前向传播。假设当前卷积层为第 l 层，上一层的输出即该层的输入向量，为 a^{l-1}，那么经过第 l 层的卷积核 W^l 运算之后，结合添加偏置 b^l，得到该层净输入 z^l，最后通过激活函数 $\sigma(\bullet)$，输出 a^l，用以下公式表示：

$$a^l = \sigma\left(z^l\right) = \sigma\left(W^l a^{l-1} + b^l\right) \tag{2.18}$$

2) 池化层前向传播

池化层前向传播是对输入图进行缩小，用下面公式表示，a^{l-1} 代表上一层的输出，a^l 则是当前池化层输出，可表示为：

$$a^l = pool\left(a^{l-1}\right) \tag{2.19}$$

(2) 反向传播

神经网络中采用损失函数衡量模型学习效果，其中网络中的权重和偏置根据反向传播进行参数学习。主要流程为：通过损失函数值了解网络中误差总值，将误差传递至上层，通过计算出每一层的误差项δ^l对参数进一步求偏导，按照下列公式进行参数更新，W^l和b^l分别为第l层的权重矩阵和偏置量，η是学习率，ΔW^l和Δb^l代表权重和偏置的误差。

$$W^l = W^l - \eta \cdot \nabla W^l \tag{2.20}$$

$$b^l = b^l - \eta \cdot \nabla b^l \tag{2.21}$$

设置J为损失函数，真实y和最终输出a^L之间的误差可表示为下面公式：

$$J(W,b,x,y) = \frac{1}{2}\left\|a^L - y\right\|_2^2 = \frac{1}{2}\left\|\sigma\left(W^L a^{L-1}\right) - y\right\|_2^2 \tag{2.22}$$

对最终输出层求解W和b的梯度：

$$\frac{\partial J}{\partial W^L} = \frac{\partial J}{\partial z^L} \cdot \frac{\partial z^L}{\partial W^L} = \delta^L \cdot \frac{\partial z^L}{\partial W^L} \tag{2.23}$$

$$\frac{\partial J}{\partial b^L} = \frac{\partial J}{\partial z^L} \cdot \frac{\partial z^L}{\partial b^L} = \delta^L \cdot \frac{\partial z^L}{\partial b^L} \tag{2.24}$$

1) 卷积层反向传播

根据当前卷积层l的梯度对$l-1$层返回的误差项δ^{l-1}进行调整，即：

$$\delta^{l-1} = \delta^l * rot180\left(W^l\right) \odot \sigma\left(z^{l-1}\right) \tag{2.25}$$

其中δ^l代表当前卷积层的误差项，δ^{l-1}代表上一层的误差项，$rot180$代表将对卷积核进行翻转180°，z^{l-1}是上一层的输出。

2) 池化层反向传播

池化是下采样，所以反向传播即为上采样，下一层的误差项对于当前层特征的一个区域，因此反向传播将误差项的值按照池化类型传播到原始对应区域中，该误差项可表示为:

$$\delta^{l-1} = upsample\left(\delta^l\right) \odot \sigma\left(z^{l-1}\right) \tag{2.26}$$

2.3 数据集和时间序列化

本小节首先介绍本文使用的数据集，通过分析数据集发现具有时间序列的特点，因此对时间序列和多元时间序列进行介绍。最后介绍数据集的处理过程，包括数据清洗、归一化、时间序列化等操作，其中因为数据集具有时间特性，对时间序列化进行详细介绍。

2.3.1 多变量时间序列的定义

时间序列存在于人类生活的各个领域，比如在医疗领域、气象领域、图像领域等均有涉及。下面给出时间序列的具体定义。

定义 1：时间序列指的是某个对象或某个指标产生的单个或者若干个变量在不同时间上产生的观察值组成的序列。假设一个时间序列T 长度为n，那么可以表示为：

$$T=\{t_1,t_2,t_3,\cdots,t_n\} \tag{2.27}$$

定义 2：多变量时间序列则是由多个单变量时间序列组成，它们有相同的时间起点和终点，数据可以用矩阵形式表达，每一行作为一个时间点，每一列作为一个单元时间序列。假设存在一个多变量时间序列T ,数量为N ，其中t_i 代表某一时刻的向量，里面包括m 个特征点，在固定时间点的情况下，该向量表示为：

$$t=\{x_i^1,x_i^2,x_i^3,\cdots,x_i^m\} \tag{2.28}$$

x_i^m 代表多变量时间序列中某一时间点i 的某一特征m 的具体值，因此多变量时间序列的最终表现形式为：

$$T=\begin{bmatrix} x_1^1 & x_2^1 & \cdots & x_1^m \\ x_2^1 & x_2^2 & \cdots & x_2^m \\ \vdots & \vdots & x_i^j & \vdots \\ x_n^1 & x_n^2 & \cdots & x_n^m \end{bmatrix} \quad i=1,2,3,\cdots,n \ \ j=1,2,3,\cdots,m \tag{2.29}$$

在网络安全态势感知领域，用户进行网上访问时发送的一系列数据包按照时间排列到达目标主机，因此网络流量数据具备时间序列的特征。每一条数据包含多个特征，每个特征各自是一条单变量时间序列，这些数值按照数据包的顺序进行排列，组成一组多变量时间序列。这些特征之间通常具有空间互相关，比如 TCP 建立连接的往返时间、三次握手发送的报文之间的时间通过报文中的时间戳均可以进行关联，关注这些联系有

助于分析攻击类型的特征和网络空间的安全状况。从时间维度分析，每个单变量序列内随着时间变化，形成一条曲线，具有某种趋势具有时间自相关的性质，因此将时间维度和特征变量空间维度进行联合考虑，形成时空相关性，这也是本文研究内容的出发点。

2.3.2 数据集

在网络安全态势感知研究领域中，数据是态势评估的基础，选择合适的训练数据集对当前网络安全态势评估技术发展是非常重要的。一般来说，目标网络的实时流量捕捉才能直观代表网络当前的运行状况，但是由于搭建网络成本较高，且缺乏普适性，因此产生了很多经典数据集供以研究，例如 DARPA、KDDCup-99 等数据集[47]。但是经研究发现，该数据集缺乏真实表示的网络流量，强调高重复计数，有数据包丢失的可能性，攻击类型描述也不够清晰[48]。KDDCup-99 是通过处理 DARPA98 数据集之后得来的，但是存在大量冗余数据，导致训练的模型对于冗余条目进行偏移，对于其他数目小的类型识别不敏感。以上介绍的数据集太过悠久，不能代表当今网络攻击类型的所有情况，因此不能满足现阶段的研究需求。

表 2.1　训练集与测试集中攻击类型数目

攻击类型	训练集	测试集
Normal	542576	351150
Generic	118198	61878
Exploits	16574	11439
Fuzzers	9137	5390
DoS	5642	4907
Reconnaissance	5582	3530
Analysis	873	670
Backdoor	759	666
Shellcode	593	371
Worms	67	43
总和	700001	440044

UNSW-NB15 数据集[49]是澳大利亚网络安全中心网络安全研究小组搭建一个网络攻击场景，配有三台虚拟服务器用于正常活动和恶意攻击，共生成 49 列特征。数据集包含的攻击类型较新，共十种攻击标签。该数据集包含四个 CSV 文件，每个文件均包

含真实的网络正常行为和攻击活动数据，考虑到算力等问题，选择 UNSW-NB15_3.CSV 和 UNSW-NB15_4.CSV 作为本篇文章的训练集和测试集，两个数据集攻击类型的分布情况如表 2.1 所示。

2.3.3 数据预处理和时间序列化

(1) 数据预处理

数据集中存在一些特殊数值需要进行处理才可使用。数据集包含数值型特征和字符型特征。其中神经网络对字符型数据不能直接处理，需要转化为模型所能识别的二进制字符。数据集内包含一些污染数据，包括一些空值、特殊值，其中某些特征的数据量级存在一些极端情况，数值之间相差过大。这些问题对模型学习过程会造成一定的影响，因此要将数据集进行预处理，才能达到模型输入的要求。

1) 字符型数据编码

针对字符型数据，要将原始数据转变成模型所能识别的编码格式，本文选择独热编码（One-Hot Encoding）对数据进行处理，给字符赋予单独标签，用数字代替，经过转化后的数据可以输入模型进行学习。在 UNSW-NB15 数据集中存在 proto、state 和 service 三列字符型特征，这三列分别记录流量的传输协议、使用协议的状态和具体使用的哪种服务，使用独热编码将其进行转化。

2) 特征丢弃和异常值处理

数据集一共包含 49 个特征，经过筛选，删除 srcip、sport、dstip、dsport、stime、ltime、ct_flw_http_mthd、is_ftp_login、ct_ftp_cmd。前六个特征代表起始主机和目标主机的 IP 地址、端口号以及包的发送和到达时间，这些特征在模型学习上没有特殊的价值，因此将其删除。后面三个特征则是存在大量缺失值，对于模型学习产生不良影响，因此将其删去。最终的数据集留下 40 列特征，包含两列标签，一个代表二分类标签，用于分辨正常活动和异常活动；另一个是十分类标签，记录每条数据的具体攻击类型。

3) 原始数据归一化

数据集内的一些特征数值量纲单位存在一定的差异，例如有些特征数值范围在$[0,1]$，有些特征数值却在$[0,10000]$范围内。当模型学习数据时，高维数据会占据大量的存储空间，降低梯度下降求解最优解的速度，因此采取数据标准化操作可以将数值控制在特定的范围内，处理方法如下面公式所示：

$$x_{ij} = \frac{x_{ij} - Mean_j}{MAD_j} \tag{2.30}$$

其中 x_{ij} 代表第 i 个时间的数据内第 j 维特征值，MAD_j 代表第 j 维特征的平均绝对偏差，$Mean_j$ 代表第 j 维的平均值。计算整个数据集中每一维特征的平均值和平均绝对偏差之后，每列特征均会保持标准正态分布缩小特征的度量范围，减小数值范围过大带来影响。

经过以上步骤处理后的数据集扩展维度为 198，其中包括两列二分类和十分类标签。

(2) 时间序列化

在网络安全态势感知领域常用的数据集一般由网络环境中捕捉的数据包处理而来，每个数据包内包含各种协议端口与发送字节大小等信息，同时数据包之间按照时间排序，因此数据包之间包含时间的流动信息。当攻击行为发生时，往往不是一瞬间，而是发送大量数据流，比如经典的 DDoS（Distributed Denial of Service）攻击，利用分布在世界各地的僵尸网络对目标靶机发动攻击，一些看似很正常的网络请求行为大批量地消耗系统资源，导致网络不能提供正常的服务。所以攻击行为也许不是一蹴而就，有时会逐渐渗透到目标系统中。网络流量数据包因为网络情况等影响因素，不会一直相连，往往会形成攻击流量正常流量相交织的情况，基于此，只关注单条流量信息无法考察历史数据条的特征。因此为维护数据条之间的自然时间顺序，也为更好地检测攻击行为，不能随机切分数据。

基于以上论述，引入针对于时间序列的滑动时间窗口方法对数据集进行处理，此方法可以充分考虑到每个时刻前的历史数据，具体过程如图 2.8 所示。本文用 X 代表网络安全态势感知数据集，经过数据预处理的数据集会扩展为高维特征向量，每条向量表示为 x_i，其中 $x_i \in X, i = 0,1,2,\cdots\cdots,T$，数据集的大小为 $N \times T$，N 代表扩展后的特征维度，T 代表此数据集的时间跨度，即数据集共有多少条时间序列。利用滑动窗口对数据集进行切割，窗口在数据集中沿着时间轴均匀移动，输出的每个数据片包含t条数据，t代表滑动窗口的大小，输出的数据片大小为 $N \times T$。与此同时，每个数据片的代表标签也会有相应的变化，时间窗口不仅在数据集上移动，在标签序列中也会沿着时间轴移动，假设时间窗口大小设为 5，则切分的第 1 条数据包括 5 个数据条，为 $[x_1, x_2, x_3, x_4, x_5]$，标签则会取标签序列 $Label$ 中的 $label_5$，以此类推，完成数据集的时间序列化。因为本篇文章

针对的是态势评估方法，因此每个数据切片对应的标签均是数据本身对应的标签。

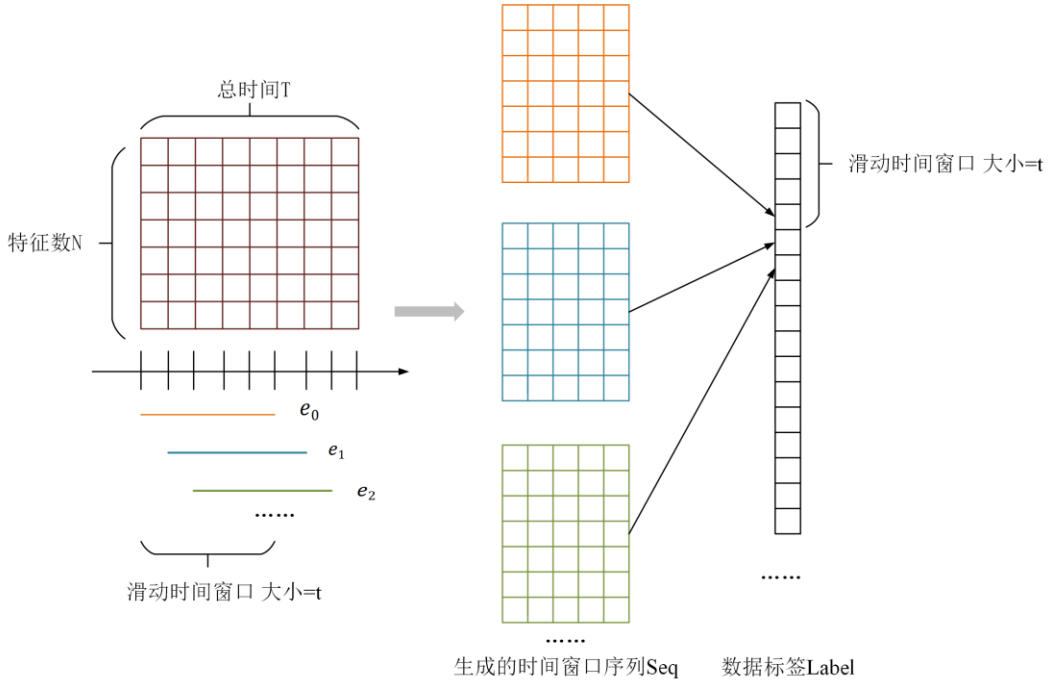


图 2.8　时间序列化过程

2.4　本章小结

本章节对网络安全态势感知基本理论和所用卷积神经网络基本原理进行介绍。首先对态势感知的定义进行阐述，介绍网络安全态势感知的定义和经典模型；其次对网络安全态势评估理论进行叙述；之后对于卷积神经网络的原理、优化方法和参数传播过程进行叙述；最后介绍多变量时间序列的定义，对数据集进行初步分析和预处理。

3　基于改进 Res2Net 的网络安全态势感知评估研究

本章节介绍一种基于 Res2Net 的网络安全态势评估方法。利用 Res2Net 作为基础网络框架，将经过时间序列化的数据矩阵作为输入。根据输入数据的特点，构建一种条带池化时空全局特征融合单元，利用横、纵两个方向的池化操作，对特征图进行时间与特征空间方向的特征聚合，将输入矩阵的全局信息有效糅合在一起，扩大感受野范围。引入通道变换注意力机制，对输入数据通道维度的变换进行建模，将其与条带池化时空特征融合单元进行串联，组合成通道-空间串联模块。本章方法在 UNSW-NB15 数据集上验证该模型有效性。

3.1　改进 Res2Net 模型构建

本章节构建改进 Res2Net 模型的出发点是：为了更好地将网络安全时间数据进行特征提取，利用深度神经网络对深层次特征的提取能力，以 Res2net 为基础框架，搭建对网络安全时间数据的时间和空间特征进行全局提取的模型。

该模型由三个部分组成，具体模型组成由图 3.1 所示。

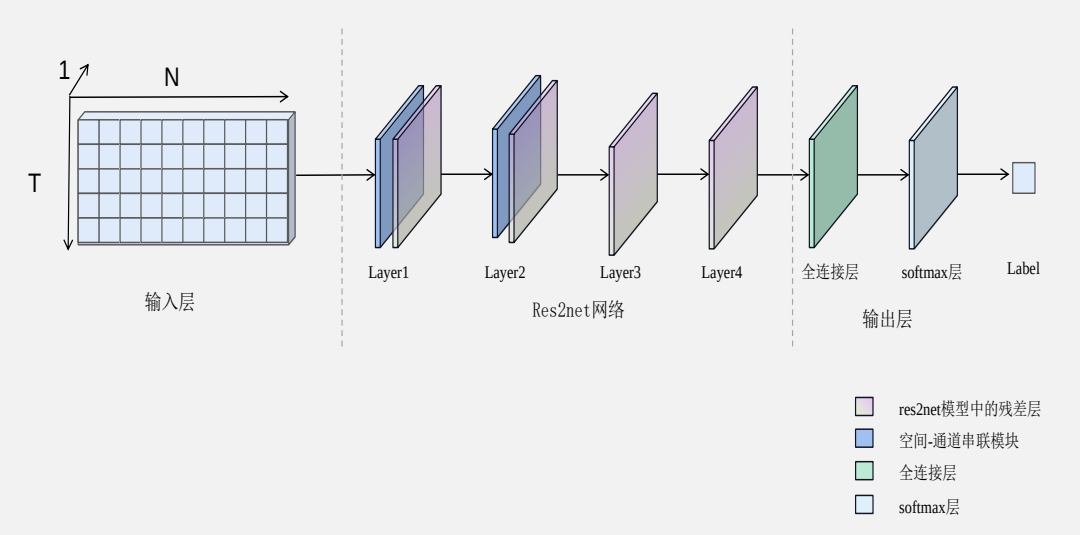


图 3.1　改进 Res2net 模型图

(1)　输入层。经过数据预处理，即对数据集进行特征扩维，独热编码等操作，将原始数据集转化为神经网络便于处理的数据形式。为将数据之间的时间相关性进行保留，使用滑动时间窗口将安全事件数据进行划分，具体时间序列化操作按照第二章介绍的序列化方法，使每个输入数据包含时间维度的信息，又包括特征空间信息。经过时间窗口处理的数据分片中，包含 T 条数据，每列特征之间存在特征间的相互关系，将这些关系称作空间关系；每条数据又是按照时间顺序排列而成，数据之间蕴含随时间变化的特征

信息。为更好地将这些信息结合在一起，设计每个数据切片为矩形矩阵，大小为 $N \times T$，N 代表经过预处理之后的特征维度大小，T 则是时间窗口的大小。

(2) 网络安全态势特征提取模型。由于 Res2Net 在图像领域展现出的优秀效果，所以将其引入网络空间安全态势感知领域进行尝试。根据这些数据特性，设计一个条带池化时空全局特征融合单元。利用卷积提取特征图之后，由于特征图横、纵方向分别包含空间、时间信息，利用非对称池化方式，对特征图信息进行更深层次的过滤，从而将特征图从空间、时间维度，分别进行特征聚合，之后将提取的时空特征进行融合。该模型引入 GCT 注意力机制，用于提取通道间的特征，并将其与条带池化时空全局特征融合单元串联成为通道-空间串联模块。通道注意力机制有助于激发通道间的竞争和合作关系，从而对有益的通道信息进行加强。该模型采用 Res2Net18 结构，拥有四个层次，考虑到经过卷积会有一些信息损失，并且所处理的数据维度并不是很高，因此将所提出的通道-空间串联模块放入前两个层次之前。

(3) 输出层。当模型对网络安全事件数据进行特征提取之后，使用全连接层和 Soft max 层对输出类型进行预测，确定概率最大的类别为最终输出类别。

3.1.1 Res2Net

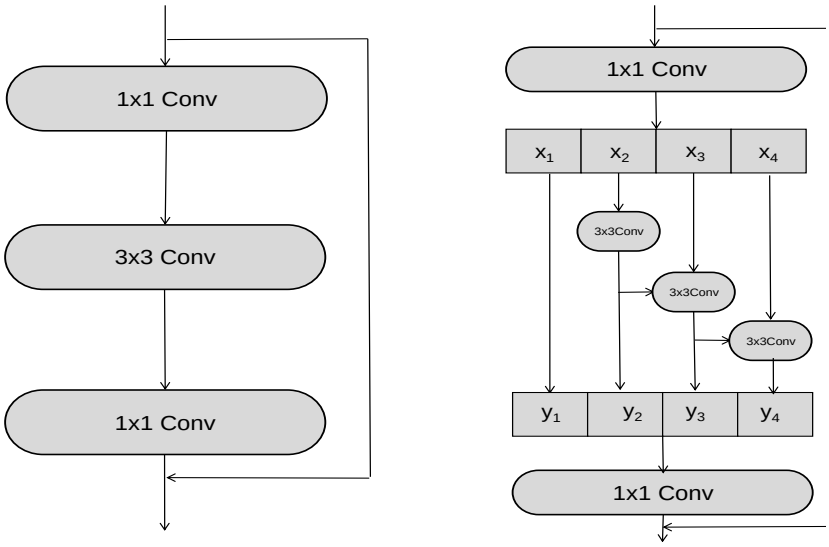


图 3.2 残差模块与 Res2Net 模块

当前输入图中的特征信息尺度各不相同，通过多次卷积计算之后可能会损失一部分局部信息，因此为保留更多重要信息，GAO 等 [50]提出一种 Res2Net，它是在 ResNet 的基础之上进行延伸而来。基本思想是从多尺度信息出发，利用组卷积增加尺度的多样性，更好地将局部信息和全局信息进行融合，增强每层网络的感受野。与 ResNet 模型对比

而言，是采用一组卷积替代残差模块的3×3卷积。具体操作为：将经过1×1卷积的特征图从通道维度进行分组，利用卷积对输入自己组的特征图进行特征提取，之后与前一组输出特征图送到另一组卷积核中，另一组卷积核重复以上操作。经过上述处理，特征图在多重不同层次的卷积核处理之下，包含的多尺度信息非常丰富，并且具有很大的感受野。组卷积和特征分组已经证明有助于提升模型的性能，因此组卷积的添加对网络产生积极作用，具有更强的多尺度信息提取能力，丰富提取信息的感受野，不同尺度的特征信息有助于模型性能的提升。ResNet 的残差模块和 Res2net 的模块结构对比如图 3.2 所示。

假设现在经过1×1卷积之后输出通道数是 M ,分组数设为 S ，那么经过通道分组，每组特征图通道数为 M/S ,每组可以用 x^i 表示，均具有相同原始输入图特征分布。组卷积的特征提取过程可参考公式（3.1）。卷积核用 $K_i(\ )$ 代替，经过卷积核的输出定义为 y_i 。对于第一组3×3卷积，为减少模型参数，将其忽略。当特征图组 x^i 与上一组卷积的输出 $K_{i-1}(\ )$ 组合之后继续进入下一组卷积进行特征提取。每一个卷积均可以连接到上一组卷积的输出，经过多层叠加之后导致卷积核可以接收在它之前提取的所有特征信息，并且这些信息的尺度各不相同，感受野的范围也随之增加，特征信息更加丰富。

$$y_i=\begin{cases} x_i & i=1 \\ K_i(x_i) & i=2 \\ K_i(x_i+y_i-1) & 2<i\le s \end{cases} \tag{3.1}$$

3.1.2 GCT 注意力机制

注意力机制指的在杂乱无章的信息中选择对完成目标任务最有帮助的信息。当注意力机制对输入的信息处理时，并不是挑选一些信息进行计算，而是关注全部的信息，对输入特征图中每个元素赋予一个权重值，该权重值代表本元素在输入特征图中发挥作用的程度，证明是否属于重要特征。由于经过卷积输出的特征图具有多个通道，因此可以输出多张特征图，每个特征矩阵蕴含的特征重要性也各不相同。因此，为得到更加具有代表性类型特征，对通道的权值进行一个自适应的调整，可以将模型的注意力聚焦到权重值高的通道上，改善模型的分类能力。

SENet 是一种经典的通道注意力机制模型，通过对通道之间的相关性进行建模，得到每个通道一个具体权重值，代表本通道在所有通道中的重要程度，按照大小顺序排列权重向量，加强有益特征，抑制无用的特征。该模块包括输入层、挤压层和激励层三个

部分。通过通道变化和全局平均池化将每个通道挤压，之后经过激励层，该部分采用全连接层对通道维度的特征信息进行整体建模，通过这些通道重要性权值对后续类型识别提供帮助。之后得到最终的通道重要性特征图 S 和原始输入特征图的通道进行融合，从而得到一个融合通道重要性信息的特征图。

SENet 虽然将通道之间的重要性进行计算，但是通过全连接层聚合通道间关系时会增加许多复杂参数，难以分析不同通道间的关联性。因此 Yang 等[51]提出一种注意力机制 GCT，通过归一化模块取代全连接层对通道之间的关联信息进行建模。该模块通过数学逻辑运算计算每张通道特征图内的信息，完成单通道内的全局信息聚合，之后利用门控机制对通道间特征信息进行转化，使得每个通道与其他通道形成竞争或者合作的关系。模块结构会引入一系列可学习的参数，会随模型训练进行调整。

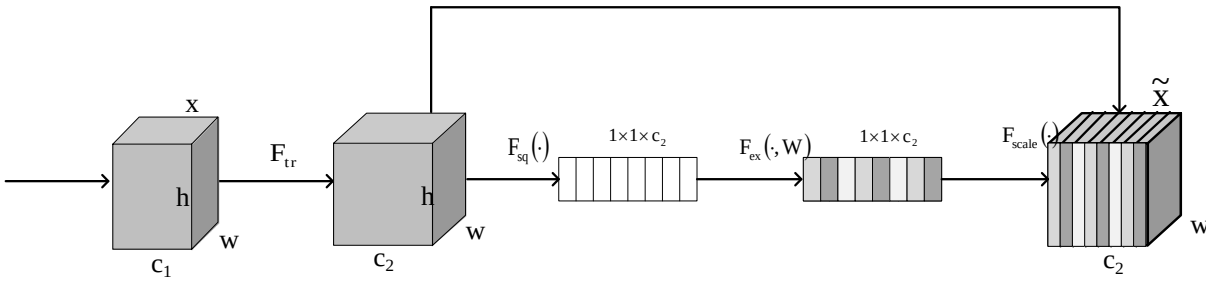


图 3.3　SENet 模块

GCT 通道注意力转换模块具体结构如图 3.4 所示，该单元共分为三部分，通过可解释的参数变量对通道间的关系进行建模。设定输入特征图大小为 $C\times H\times W$，经过三部分处理，该单元所包含可学习参数为 α、β、γ。

(1)　全局上下文嵌入（Global Context Embedding）

对于一个大小为 $C\times H\times W$ 的输入特征图，首先要对每个通道内包含的全局上下文信息进行聚合，对通道间关系进行建模。如果使用 SENet 中的全局平均池化进行全局信息聚合，在某些特殊情境下会失效，例如当进行 Instance Normalization 之后添加 SE 模块，会导致经过全局平均池化的输出是恒定的，每个通道的平均值相同。为避免这个问题，Yang 等通过对比，采取 L2 范数计算每个通道内的信息，通过给定一个维度和通道数相同的权重向量 $\alpha=\left[\alpha_1,\alpha_2,\cdots,\alpha_c\right]$，将其按照公式（3.2）计算，其中 x_c 代表输入特征图中第 c 个通道的特征图，ε 是为了防止出现导数为 0 的情况。由于每个通道内的显著特征各不相同，因此可以通过参数向量 α 的学习控制通道的权重大小。该操作使得模型学习到单通道相对独立于其他通道的情况。

$$s_c = \alpha_c \left\| x_c \right\|_2 = \alpha_c \left\{ \left[\sum_{i=1}^{H} \sum_{j=1}^{W} \left(x_c^{i,j} \right)^2 \right] + \varepsilon \right\}^{\frac{1}{2}} \tag{3.2}$$

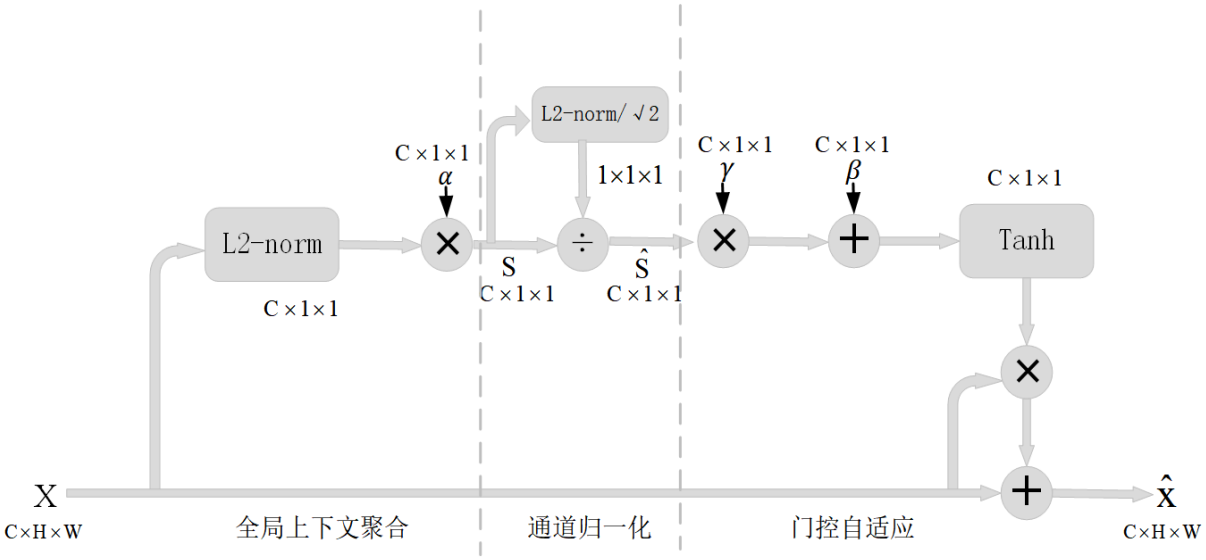


图 3.4　GCT 注意力机制

(2)　通道归一化（Channel Normalization）

当对每个通道进行特征聚合之后，整个原始特征图输出一个维度为$C\times1\times1$、每个通道均包含自己的全局信息的特征。通道归一化具体操作表示为公式（3.3），将每个通道的权重进行归一化计算，采用 L2 范数进行跨通道操作，建立起通道间的竞争关系。将这些通道的权重映射在同一范围，如果存在某一单通道内数据特征明显，经过计算之后与其他通道形成差距，那么将对这个通道信息加强；如果某一通道信息量不大，特征不明显，那么将会调整该通道的重要性。ε 的意义在于防止出现特殊情况，$\sqrt{C}$ 的作用是考虑到通道数过大会导致数值增大，因此将其进行调整。

$$\hat{s}_c = \frac{\sqrt{C} s_c}{\left\| s \right\|^2} = \frac{\sqrt{C} s_c}{\left[\left(\sum_{c=1}^{C} s_c^2 \right) + \varepsilon \right]^{\frac{1}{2}}} \tag{3.3}$$

(3)　门控自适应（Gating Adaptation）

设置门控向量为$\gamma = [\gamma_1, \gamma_2, \cdots, \gamma_c]$，门控偏置向量为$\beta = [\beta_1, \beta_2, \cdots, \beta_c]$，使用 Tanh 激活函数对输出的数据进行计算控制每个通道的激活状态，形成最终通道关系，具体过程如公式（3.4）所示。门控权重被正向激活代表该通道与其他通道之间的关系是竞争；门控权重被负向激活代表该通道与其他通道形成合作关系。当门控权重和偏执值为 0 时，可以将原始特征图传递到下一层，参考公式（3.5），等价于 ResNet 中的 Identity 设置，

可以有效减缓深层网络退化。在模型最初设置γ和β初始为0，可以增加模型稳定性。

$$\hat{x}_c = x_c\left[1+tanh\left(\gamma_c\hat{s}_c+\beta_c\right)\right] \tag{3.4}$$

$$\hat{X} = F\left(X\mid\alpha,0,0\right)=1X=X \tag{3.5}$$

3.1.3 条带池化时空全局特征融合单元

经过对网络安全事件数据的具体分析，发现数据是按照时间顺序进行排列，每条数据都和上方数据形成联系。为了更好地将时间和空间信息进行提取，引入条带池化进行操作。

(1) 条带池化基本原理

条带池化是由Hou等[52]在2020年提出用于图像领域的一种池化方式。常见的池化方式有最大池化和平均池化，它们进行计算的区域为一个方形。但是在图像中有许多以条形存在的物体，而条状池化恰好可以用一个长条形框沿着空间领域滑动获取特殊形状的特征关系。条带池化包括横向和纵向两个方向的池化操作，可以从不同方向捕获特征图所含的特征关系。由于条带池化所覆盖距离较长，因此可以建立特征图包含的长距离依赖关系。条带池化具体操作如下：

假设存在一张大小为$H\times W$的特征图输入条带池化中，包括纵向条带池化和横向条带池化。在纵向条带池化中，按照输入特征中的每一列所占尺寸即$H\times 1$作为一个池化窗口，对池化窗口覆盖的数据即特征图中的一列进行平均值计算，得到该窗口范围池化后的特征；在横向条带池化中，按照输入特征中的每一行即$1\times W$作为一个池化窗口，同样对窗口覆盖下的数据即特征图中的一行信息进行平均值计算，得到覆盖范围池化后的特征。经过纵向条带池化后输出的特征图可以表示为$y^v\in R^W$：

$$y_j^v = \frac{1}{H}\sum\nolimits_{0\le i\le H} x_{i,j} \tag{3.6}$$

横向条带池化后的输出表示为$y^h\in R^H$：

$$y_i^h = \frac{1}{W}\sum\nolimits_{0\le j\le W} x_{i,j} \tag{3.7}$$

(2) 条带池化与网络安全态势数据的适配性分析

网络安全态势数据是由日志文件系统、捕捉流量包工具进行收集之后，按照时间进行排列的字符串数据。经过相关人员的分析，提取数据包具有价值的数据，假设数据集

为 $X=[x_1,x_2,\cdots x_T]$，时间跨度为 T，每条数据包含 n 个特征变量。为更好地维系数据之间的时间相关性，按照滑动时间窗口大小 t 对数据集进行划分，形成尺寸为 $t\times n$ 的数据矩阵，$x_{i,j}$ 表示时间为 i 时的数据行中第 j 个特征变量，具体可表示为：

$$X=\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_T \end{bmatrix}=\begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{T1} & x_{T2} & \cdots & x_{Tn} \end{bmatrix} \tag{3.8}$$

由于输入的数据结构简单，具有简单的横纵交叉联系，而条带池化又可以按照横、纵两个方向进行池化，因此通过平均值的计算可以将同行或者同列的元素信息进行提取，扩大感受野，建立元素之间的长距离依赖关系，使得数据片中每个元素不再只和周围信息进行交互，也可以将该元素所在的行列信息进行互通，从而可以有效保留该元素的时间全局关系和变量空间全局关系。

(3) 条带池化时空全局特征融合单元

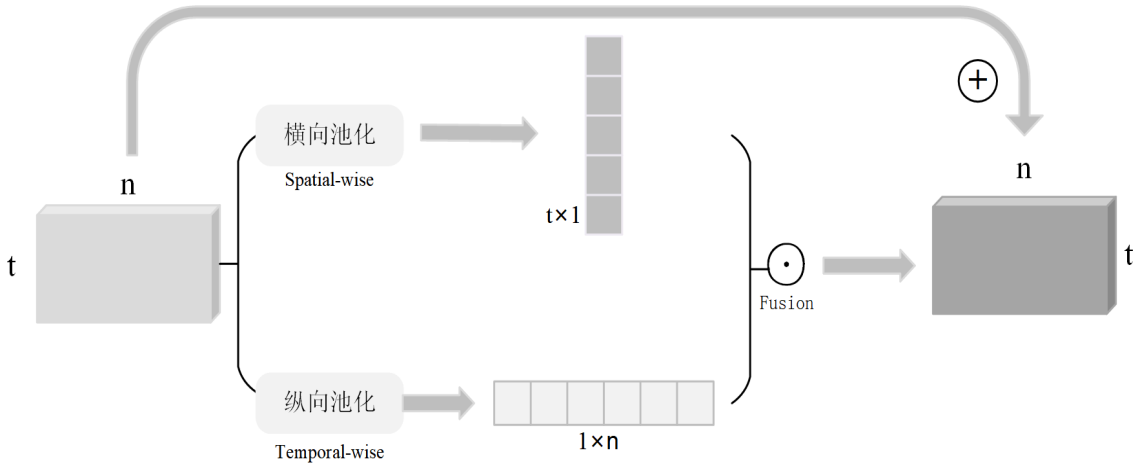


图 3.5 条带池化时空全局特征融合单元

条带池化时空全局特征融合单元以原始数据的时间关系和特征变量空间关系为起点，对其分别进行横（空间）、纵（时间）两个方向的自适应平均池化。具体结构如图 3.5 所示，若输入大小为 $t\times n$ 的流量数据特征图，对其进行纵向池化，求取每一列的平均值，即每一个特征变量所包含的单元时间序列的均值，形成维度为 $1\times n$ 的特征图，可表示为 $A=[a_1,a_2,\cdots,a_n]$；输入特征图使用横向池化，对每一行数据求取均值，即对每一

条流量数据内的特征空间向量的均值，所得特征图大小为$t\times1$，表示为$B=[b_1,b_2,\cdots,b_t]^T$。通过条带池化可以将横（空间）、纵（时间）两个方向中每一行或每一列的全局信息进行聚合，使得两个特征图分别带有时间维度和空间维度的特征关系。

为将所提取的时间、空间特征进行全局交互，借用矩阵相乘的思想，将时间信息和空间信息进行显式的计算，即：

$$B\times A=\begin{bmatrix}b_1\\b_2\\\vdots\\b_t\end{bmatrix}\times\begin{bmatrix}a_1 & a_2 & \cdots & a_n\end{bmatrix} \tag{3.9}$$

通过计算可以得到每个元素位置的时空交互信息，输出维度为$t\times n$：

$$D=\begin{bmatrix}d_{11} & d_{12} & \cdots & d_{1n}\\d_{21} & d_{22} & \cdots & d_{2n}\\\vdots & \vdots & \ddots & \vdots\\d_{t1} & d_{t1} & \cdots & d_{tn}\end{bmatrix} \tag{3.10}$$

之后将输出的特征图与原始特征图相加，从而将原始特征图中每个元素获得与之位置对应的时空信息。

3.1.4 通道-空间串联模块

上文介绍的 GCT 注意力机制，利用门控和 L2 范数对通道间的信息进行建模，从而激活通道间的竞争和合作关系。条带池化时空全局特征融合单元是利用条带池化，对于时间维度和空间维度分别进行平均池化，那么池化窗口所覆盖的面积恰好是输入数据的一行或是一列，由此可得到包含时间或空间维度的信息，最终经过数据融合将原始输入与经过融合的输出进行相加，使得原始数据中每个元素均获得一个独一无二的时空关系。Woo 等[53]指出，注意力模块在组合时，不同的放置顺序对输入特征图中提取的有效信息存在差异，经实验证明，先对通道关系进行注意力机制再对空间进行注意力加权会产生更优的效果。因此，本文将 GCT 模块和条带池化时空全局特征融合单元串联，加强对输入数据特征提取的能力，提高后续态势评估的准确度。具体结构参考图 3.6，首先通过 GCT 模块对初始特征图的通道关系进行显式建模，提取通道之间的关键特征，之后连接时空全局特征融合单元，用于空间维度。

由于整个模型的输入是单通道图，因此经过卷积增加通道数量之后，每个通道所包含的信息依然是整张原始特征图，通道数的上升可以增加特征的多样性，并且捕捉通道之间的相互依赖关系有助于模型关键特征的提取。经过通道注意力之后，每个通道特征

图均带有通道权重信息，将其输入时空全局特征融合单元对输入数据的时空关系进行建模，增强特征的长距离依赖关系，有效筛选单一元素周围的无用元素，聚合其所具有的时间信息和空间信息，增强特征的表达能力。

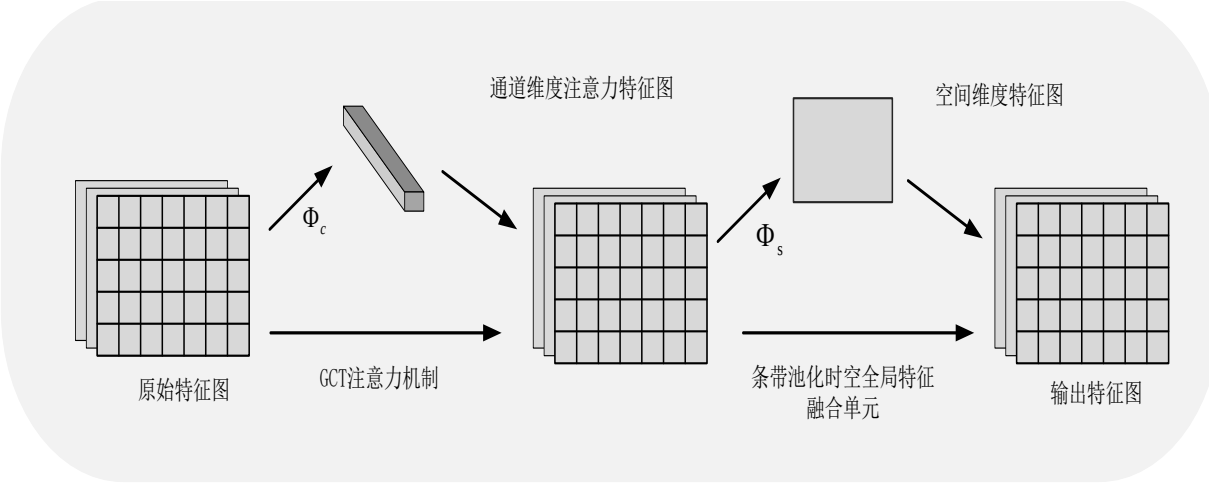


图 3.6　通道-空间模块

3.2　基于改进 Res2Net 网络安全态势感知评估过程建立

基于改进 Res2Net 网络安全态势感知评估模型具体流程如图 3.7 所示。

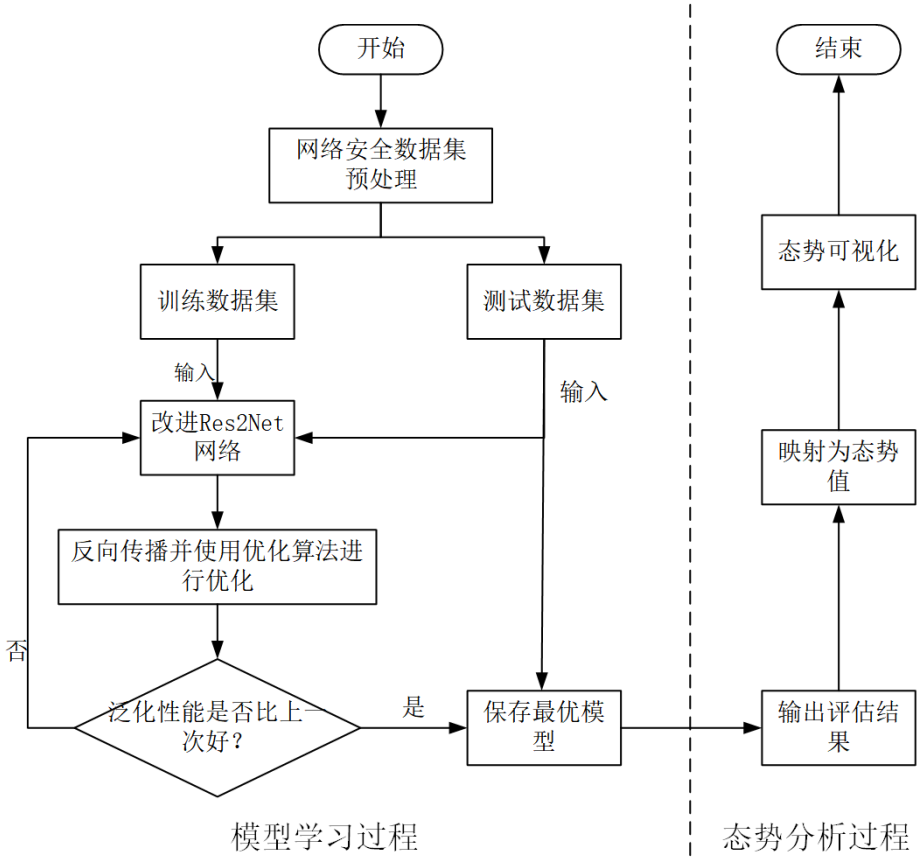


图 3.7　基于改进 Res2Net 网络安全态势评估模型流程图

步骤 1：数据预处理。为使输入的数据更加符合模型，避免干扰因素对模型评价产生影响，对数据集中的缺失值、异常值等信息进行清除。针对存在的字符型数据，由于模型不能直接处理，因此利用独热编码对其转换为可处理的数值型。为保留数据集中每条数据存在的时间关联，引入滑动时间窗口对数据集进行切割，每片数据时间帧包含时间窗口大小的数据条。该步骤在第二章已经详细论述。

步骤 2：经过处理的数据集分为训练集和测试集。

步骤 3：将训练数据集输入改进 Res2Net 模型。在训练时，模型从训练集中选择数据进行前向传播，学习数据中包含的特征信息。随后计算真实标签和预测标签之间的误差，利用优化器对误差进行优化，反向传播调整模型参数直至最优。最终将获得的最优神经网络模型参数进行保存，用于后续使用。

步骤 4:将学得的最优模型对测试集进行预测，按照网络安全态势评估指标体系将其预测的攻击类型标签转换为态势值，按照图形化方法描绘当时的网络安全态势直观曲线。

3.3 实验结果与分析

3.3.1 实验环境

本章节模型实验在一台远端服务器上进行，该服务器的配置信息如表 3.1 所示。

表 3.1 实验环境

软硬件名称	配置
操作系统	Ubuntu 18.04.1
GPU	NVIDIA GeForce RTX 2080Ti
深度学习框架	Pytorch1.7.0
编程语言	Python3.6
CUDA	11.0

3.3.2 网络安全态势值量化

网络安全态势评估指标在网络安全态势评估中占有重要位置，制定合适的决策指标是应对网络威胁的主要因素[54]。将收集的网络安全事件数据进行分析之后，将其转化成具体的数值或文字，对于管理人员快速掌握网络运行状况具有较大的帮助。一般来说，根据评估形式的不同，可以分为定性评估和定量评估，网络安全态势评估值代表当时网络的危险程度，因此对于态势值的设定，可以依据攻击事件造成损失的轻重程度来进行

设定。本章态势值设定主要采取 Li 等人[55]的态势设定方案，按照攻击类型造成危害范围的影响差异，对这些攻击进行排序，对其赋予一个定量态势值，具体态势值量化对照参照表 3.2。

表 3.2　态势值量化对照表

攻击类型	态势值	攻击类型	态势值
Normal	0	Generic	5
Analysis	1	Shellcode	6
Reconnaissance	2	Worms	7
DoS	3	Exploits	8
Fuzzers	4	Backdoor	9

3.3.3　实验指标

本章实验基于混淆矩阵（Confusion Matrix）对模型的优劣进行分析，采取准确率（Accuracy）、精确率（Precision）、F1 值（F1-Score）三项指标来评估本章模型对于网络流量数据的学习能力，这些指标可以较全面地分析模型的攻击类型预测效果是否优秀。

表 3.3　混淆矩阵

基础指标	意义
TP	真阳性，真实值为正的样本在预测时也为正值
FP	假阳性，真实值为负的样本在预测时为正值
TN	真阴性，真实值为负的样本在预测时也为负值
FN	假阴性，真实值为正的样本在预测时为负值

对于一个二分类问题，可以依据上述表 3.3 描述的基础指标进行计算。

(1)　准确率

对于准确率而言，它代表在模型进行预测时，预测标签和对应的真实标签一致的样本数量占总样本数量的比例，按照下面的公式进行计算。

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN} \tag{3.11}$$

(2)　精确率

精确率更加关注预测样本的标签是否与原样本标签一致，侧重于每个类别样本中预

测正确的样本数量，即当预测为第一类的样本数量中真的为第一类的样本数量有多少。关于精确率的计算，参考下面公式。

$$Precision = \frac{TP}{TP + FP} \tag{3.12}$$

(3) F1 值

F1 值是综合的评判指标，可以更好地衡量各类样本在模型中的预测效果，它以精确率和召回率为依据进行计算，使它们的加权调和平均数。

$$F1 = \frac{2 \times Recall \times Precision}{Recall + Precision} \tag{3.13}$$

3.3.4 UNSW-NB15 数据集实验结果分析

本实验采用 UNSW-NB15 数据集，具体信息和预处理过程在第二章第三节已经介绍。本章提出一种基于改进 Res2Net 的网络安全态势评估模型，具体结构由所构建的条带池化时空全局特征融合模块（简称时空融合模块）和 GCT 模块串联而来的通道-空间模块，组成改进的 Rse2Net 模型，以此为基础进行对比实验，模型参数如表 3.4 所示：

表 3.4 模型参数配置

参数	具体设置
输入大小	（1，5，196）
Batch size	512
Epoch	20
优化器	Adam
损失函数	交叉熵损失函数
学习率	0.0001
Dropout	0.1

对该数据集进行二分类实验和十分类实验两组实验，设置二分类实验是为了初步验证模型在攻击类型识别上的有效性，十分类在标签类别和数量方面进一步细化，因此十分类实验的目的是在二分类结果基础上对模型有效性进一步分析和验证。

(1) 基于改进 Res2Net 的二分类态势评估实验分析

1) 关于测试集的准确率、精确率、F1 值对比

对比实验结果如表 3.5 所示，通道-空间模块指标（加粗标记）代表最终的改进模型，

准确率为 99.14%，精确率为 99.13%，F1 值为 99.14%，对比基础的 Res2Net 均有提升，证明本文方法可以对输入数据进行更好地分类。由于最终模型包括时空融合模块和 GCT 模块，为验证它们在模型中发挥的作用大小，对它们输出的指标进行分析，发现各项指标均优于比 Rse2Net，证明这两个模块结构可以有效提取输入数据特征，增强分类效果。并且时空融合模块在三项指标中均高于 GCT 模块，证明对网络流量数据进行时空角度的特征提取是有效的。引入决策树、LSTM、ResNet 模型进行对比，可发现本模型在准确率指标等方面均优于这些模型，证明本模型对于网络安全态势评估是有效的。

表 3.5　实验指标对比

模型	Res2Net	GCT	时空融合模块	通道-空间模块	准确率（%）	精确率（%）	F1 值（%）
DT					91.23	91.32	91.17
LSTM					98.15	98.14	98.14
ResNet					98.74	98.72	98.73
Res2Net	√				98.87	98.86	98.86
GCT	√	√			99.11	99.11	99.11
时空融合模块	√		√		**99.12**	**99.13**	**99.12**
通道-空间模块	√			√	**99.14**	**99.13**	**99.14**

2)　关于训练集和测试集的 loss 损失和准确率对比

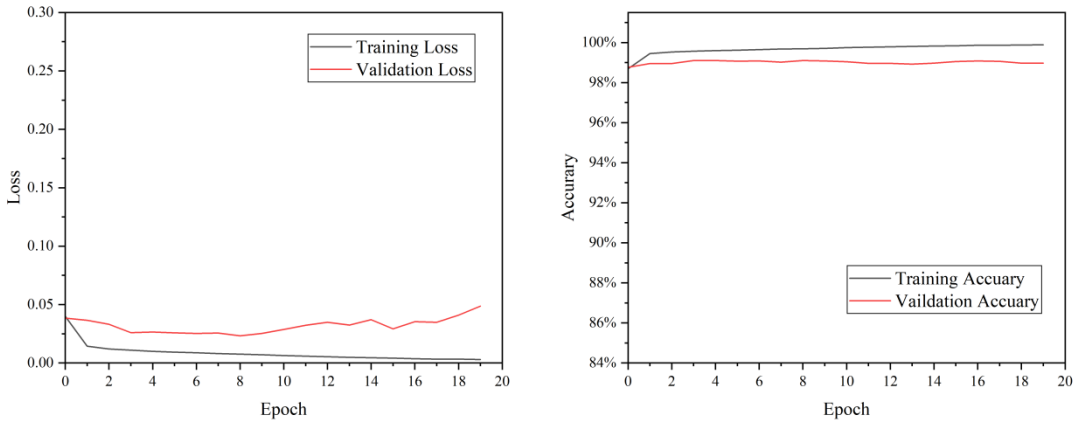


图 3.8　训练集和测试集 loss 值（左）和准确率（右）曲线

观察图 3.8 中训练集和测试集的损失变化，发现模型收敛速度较快，在极少轮次内已经达到模型损失最低点，随后训练集继续学习，不断减小损失值，测试集则存在一些

波动。结合图右发现训练集的准确率逐渐增加并逐渐趋于稳定，测试集的准确率维持在99%周围，处于平缓状态。

3)　测试集经过改进 Res2Net 模型评估的态势值可视化

通过观察下面的态势曲线图，可以发现，大部分数据呈现红色曲线，覆盖蓝色的真实值，说明模型的分类能力较好，可以准确地识别攻击类型。

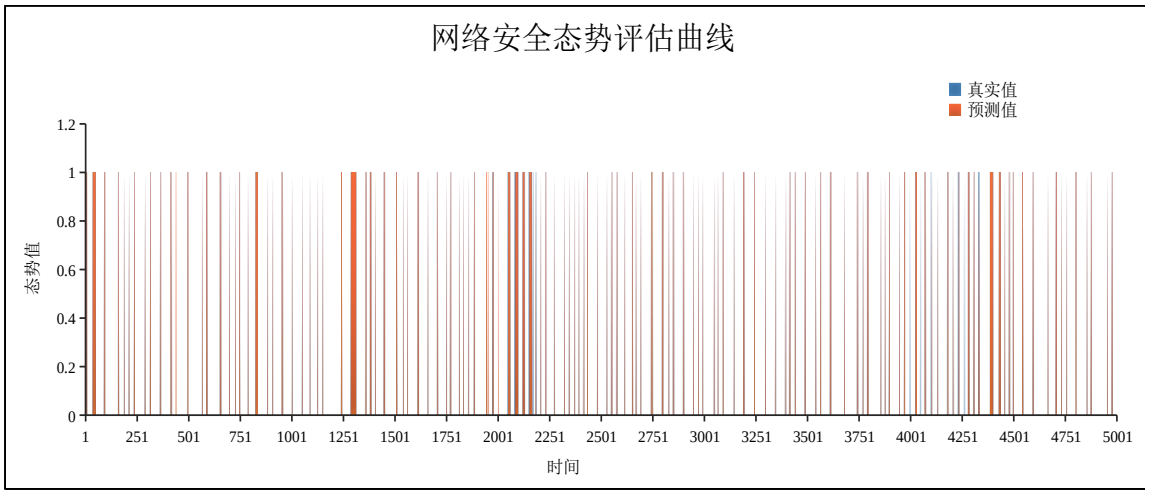


图 3.9　测试集态势评估曲线

(2)　基于改进 Res2Net 的十分类态势评估实验分析

1)　关于测试集的准确率、精确率、F1 值对比

表 3.6　实验指标对比

模型	Res2Net	GCT	时空融合模块	通道-空间模块	准确率（%）	精确率（%）	F1 值（%）
DT					87.63	88.32	87.51
LSTM					90.31	90.15	90.28
ResNet					94.05	93.67	93.86
Res2Net	√				94.75	94.50	94.31
GCT	√	√			96.70	96.72	96.45
时空融合模块	√		√		**96.79**	**96.73**	**96.59**
通道-空间模块	√			√	**96.83**	**96.86**	**96.61**

结合表 3.6 对模型十分类实验性能进行评价，通过对比发现，本章所构建的模型在各项指标中比决策树、LSTM、ResNet、Res2Net 模型表现优异，在准确率等指标中均

表现优异，证明本文所构建的通道-空间模块有助于数据集的特征提取。我们将最终模型中的 GCT 模块和时空融合模块进行分析，发现时空融合模块比 GCT 模块表现优异，证明对网络流量进行时空特征提取是有益的，可以提高模型的分类水平，两个模块进行组合比单一模块具有一些提升，准确率等指标均有上升。其中时空融合模块的准确率等指标比 GCT 模块均高出 0.01~0.14%，证明时空融合模块对时空特征的提取是有效的，并且时空特征有助于提高攻击分类的准确率。

2) 关于训练集和测试集的 loss 损失和准确率对比

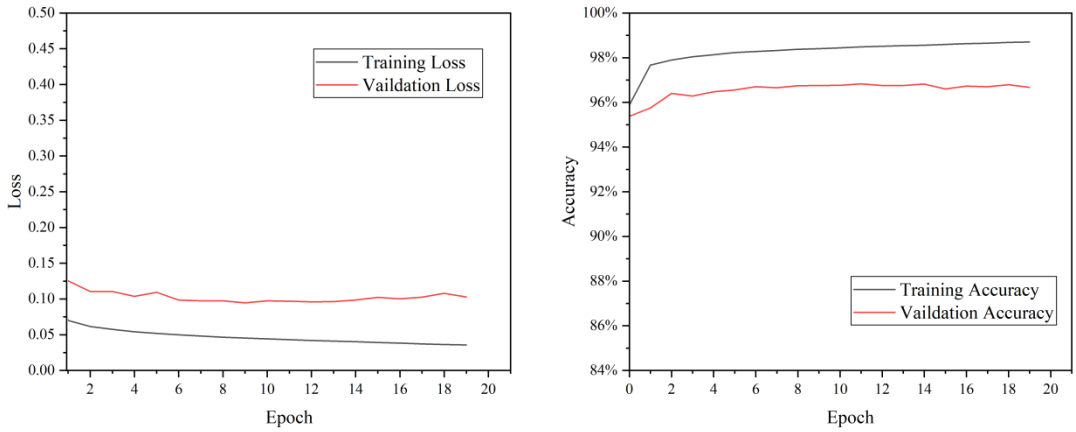


图 3.10 训练集和测试集 loss 值（左）和准确率（右）曲线

观察图 3.10，通过损失曲线图可发现，模型在 10 个 Epoch 内便达到损失最低点，而后训练集不断学习，损失值逐渐减小，训练集的准确率随着损失值的减小而逐渐上升，测试集的准确率在 96.5%左右逐渐平缓。

3) 测试集经过改进 Res2net 模型预测的态势值可视化

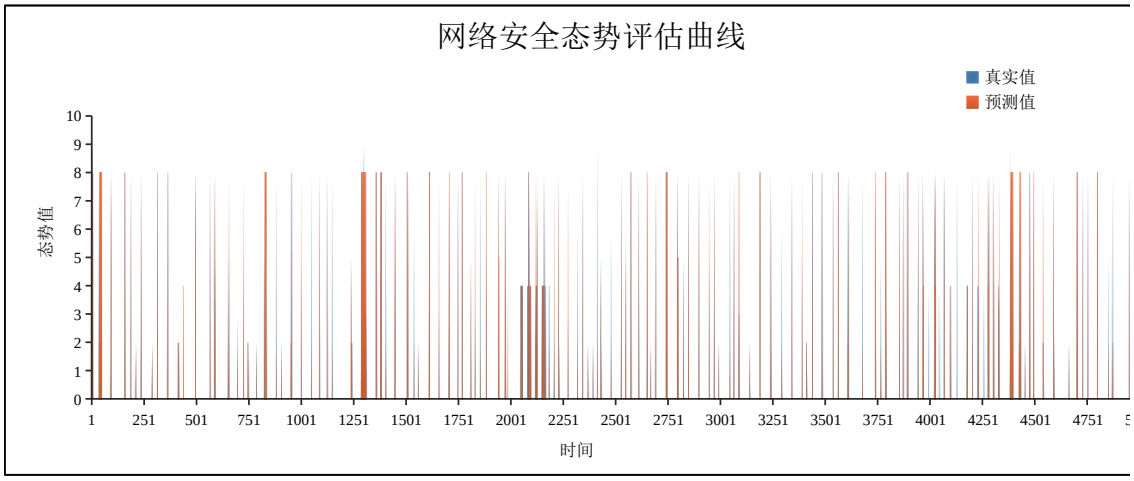


图 3.11 测试集态势评估曲线

通过观察图 3.11，可以直观发现红色态势预测值大面积覆盖在蓝色真实值之上，说

明模型的准确率较高，对攻击类型可以有效区分，从而帮助后续工作人员掌握网络运行信息，规避安全风险。

3.4 本章小结

本章提出一种基于改进 Res2Net 的网络安全态势评估模型。该模型将 Res2Net 与通道-空间模块进行结合，通过对数据集时空特征的深度提取，实现对网络安全态势的评估过程。通道-空间模块由门控通道变换注意力机制和条带池化时空全局特征融合单元，串联而成，经过对输入特征通道关系的提取可以增加通道的竞争与合作关系，对无效信息抑制；条带池化时空全局特征模块采用条带池化对整张特征图中包含的时间特征和空间特征进行提取，利用其特殊形状窗口对特征图中每个元素所在位置的时间信息和空间信息进行提取，经过融合输出蕴含丰富时空信息的特征。

本章实验在 UNSW-NB15 数据集中进行，通过对评价指标的分析，证明本章模型在攻击类型方面具有较高的准确率，从时空角度设计模型对网络流量数据的拟合程度更高。

4　基于 SaT-CNN 的网络安全态势评估研究

第三章所介绍模型虽然在准确率等方面得到提升，但由于深层卷积神经网络对比浅层卷积神经网络仍然存在参数量大的问题，训练速度减慢，易过拟合，为了改善模型训练速度，并且保持较高的准确率，本章节基于网络流量在时间和空间上的关联性，提出一种从时空角度提取特征的卷积神经网络（Spatial and Temporal-Convolutional Neural Network，SaT-CNN）用于实现网络安全态势评估。该模型由一种时空信息联合提取模块（Union Extraction Module of Temporal and Spatial Information，UEMoTaSI）堆叠而成，该模块从时间和空间角度设计两个特征提取单元，将其并联之后的输出通过门控融合机制对时空信息进行融合，较好地将流量空间信息和时序信息进行结合。之后在 UNSW-NB15 数据集中对本模型的准确率、精确率、F1 值等实验指标进行验证。

4.1　SaT-CNN 模型构建

本文设计的网络安全态势感知模型如图 4.1 所示，提出一种基于时空信息联合提取模块的卷积神经网络，该网络利用 CNN 对特征信息的敏感程度，从数据的时空特性出发构建，用于提高对网络流量的辨别度。

本模型分为三个部分，具体过程如下：

(1)　数据预处理

将数据集进行清洗之后，通过设置合适的滑动窗口大小，对数据集进行切分，将一维向量的流量数据，扩展为具有时间维度的二维矩阵，具体操作方法在第二章第四节已经详细介绍。

(2)　输入 SaT-CNN 模型

第二部分为用于训练数据的神经网络。通过该模型提取流量的空间信息和时间信息，捕获特征之间的依赖关系和序列内部的时间相关性。该网络的主要结构是基于 CNN 构建一个时空信息联合提取模块，通过堆叠该模块形成最终的 SaT-CNN。该模块包括一个时间信息提取单元（Time Feature Extraction Unit，TFEU）和空间信息提取单元（Spatial Feature Extraction Unit，SFEU），两个单元以并联方式结合在一起，分别提取全局空间信息和时序信息。空间信息提取单元将输入特征中每个元素之间进行相连，拥有广阔的感受野，有助于该模块对于输入数据空间信息进行建模。时间信息提取单元，利用不同尺度大小的不规则卷积核，按照时间维度进行特征提取，不同尺度的时间信息可

以加强时序的特征表达能力，将有助于攻击类型识别的信息进行更深一步的加强操作。两个单元并联运行，通过门控计算两个分支的权重进行自适应的特征融合，将学习到的时间相关性和空间相关性形成整个特征空间的时空交互。

(3) 输出层

模型学习过程中通过全连接层和 Softmax 函数，组成合适的分类器，把经过卷积提取的特征展平，对最后特征的攻击类型进行识别。

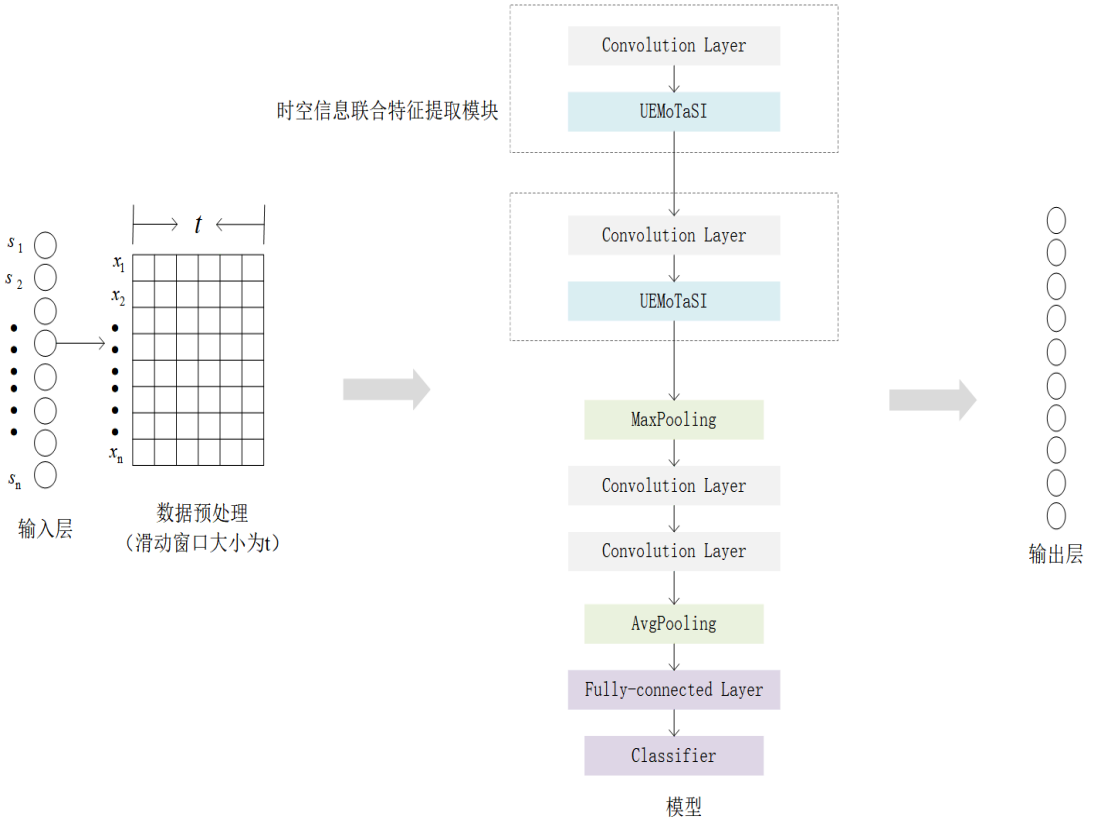


图 4.1　基于 SaT-CNN 网络安全态势评估模型

4.1.1　时空信息联合提取模块

经过时间序列化处理的数据矩阵既包含特征空间的相关信息，又包括时间上的相互关联，为了将流量数据间的时空特征联系得到最大显化，提出一种时空信息联合提取模块 UEMoTaSI，本模块旨在把流量的特征空间和时间上的流动信息相结合，在对特征空间进行处理的同时，包含时间维度的信息，继而将流量矩阵蕴含的内部信息更好地提取出来，帮助模型提高攻击类型的辨别能力。因此设计一个时间空间信息联合提取模块，该模块从时间、空间两个维度出发，构建对输入数据矩阵进行更深层的特征提取。模型结构如下图 4.2 所示。该模型分为两个部分，第一部分是并联时空信息提取单元，将特征矩阵同时输入两个信息特征提取单元，得到两张具有不同特征相关性的特征图。为将

两个路径的输出更好地融合，引入一个基于门控的融合机制，通过门控权重去筛选对识别类型更加有益的特征，自适应地将两个分支融合在一起，更好地帮助分类。

下面对两个机制进行详细介绍：

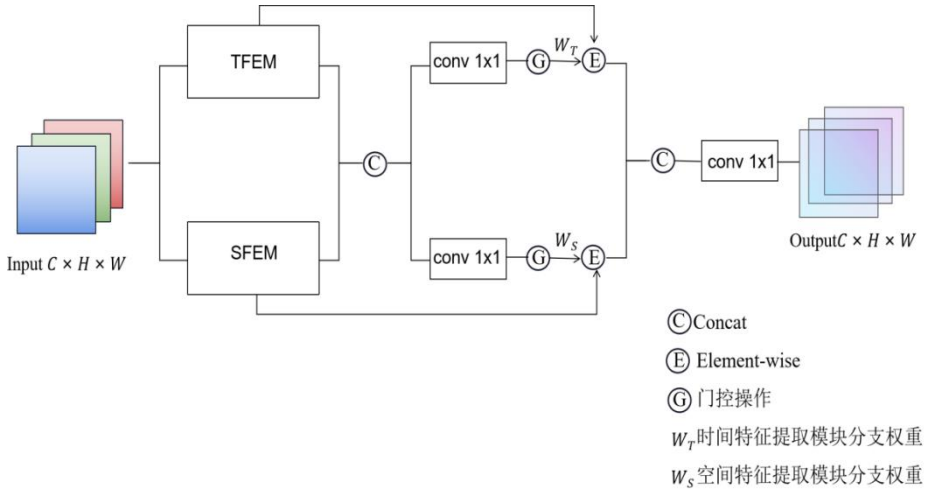


图 4.2　时空信息联合提取模块

(1)　时空特征提取单元并联机制

将二维数据矩阵输入到由并联而成的空间信息提取单元 SFEU 和时间信息提取模块 TFEU 中，空间信息提取模块更好地提取全局信息，将整个时间窗口切片包含的流量信息进行更深层次的提取，并加强全局特征的采样，捕捉流量窗口的上下文信息。时间信息提取模块从时间角度出发，提取二维矩阵中的纵向时间关联，关于流量数据序列之间的依赖关系进行处理，来提高对网络攻击类型的辨别能力。通过时间、空间两个信息提取单元的并联操作，每个分支的输出均带有明显的时空特点，更好地关注单一角度的信息表达，提高模型的建模能力。

(2)　基于门控的融合机制

为更好地利用矩阵中蕴含的特征信息，引入门控融合机制[56]对经过卷积的特征图进行筛选，计算出两个分支的权重，此权重代表每个分支进行融合时各自特征的贡献程度，决定两个分支在信息融合之前提供的信息有多少。最后将权重和分支输出的特征矩阵进行逐元素相乘，这样本模型不仅探索时间步之间的时间依赖性，还要关注每个时间步中特征之间的交互。具体操作如下：

假如设置时空特征并联部分输出的特征图，分别为S和T，S代表空间信息提取单元输出的特征向量，T代表时间信息提取单元输出的特征向量。两个特征向量首先进行通道维度的融合操作，如果S具有n_s个通道，T具有n_T个通道，那么经过 Concat 之后

输出的特征图F通道数n如下面公式（4.1）所示。其次将特征图分两个独立的路径，使用一个1×1卷积去降低通道的数量，使得后期学习的权重维度与原特征图匹配，Sigmoid 函数对其作用生成权重值，两个路径输出的权重即为W_S和W_T，该操作可以表示成公式（4.2）和（4.3），其中C和b代表卷积操作和卷积产生的偏差。之后将得到的两组权重矩阵W_S和W_T，分别和原路径的特征图S和T进行逐元素相乘，自适应地调整时间和空间特征对最终分类的贡献程度，将输出的特征在此进行 Concat 合并，得到特征图F_{END}，整个过程可以用公式（4.4）表示。最终端连接一个1×1卷积进行通道降维，并增加特征图的表达能力。至此，完成整个门控融合机制。

$$n = n_s + n_T \tag{4.1}$$

$$W_S = \sigma\left(C_1 \times F + b_1\right) \tag{4.2}$$

$$W_T = \sigma\left(C_2 \times F + b_2\right) \tag{4.3}$$

$$F_{END} = CONCAT\left[\left(W_S \odot S\right),\left(W_T \odot T\right)\right] \tag{4.4}$$

4.1.2 空间信息提取单元

空间信息提取模块 SFEU（Spatial Feature Extraction Unit）用于提取流量矩阵中的全局信息，利用卷积核的移动，将整个信息矩阵覆盖，引入 ACNet（Asymmetric Convolutional Network）的不对称卷积核[57],利用两个条形卷积核1×3和3×1，另外添加一个3×3的规则卷积核进行特征提取，三个分支输出的特征图进行相加，这样可以对全局信息特征进行加强，并且代替3×3卷积，减少计算量，既增强主干，又不需要额外的参数量。同时，不规则的条状卷积核也符合网络流量数据的特点。要处理的流量帧是一个矩阵，它的横行和纵列分别具有不同的含义，其中每个元素都带有时间和特征类别的标记，经过行、列组合而成，根据它的横纵交叉特点，利用不对称卷积也可以提取相应的空间局部特征，并增强特征表达能力。空间信息提取单元结构参考图 4.3。

(1) 卷积的可加性

在保证输入相同的前提下，将几个大小可以互相计算的卷积核按照相同步长进行移动，会产生相同大小的输出，将它们的输出相叠加得到最终输出，这些卷积核在相应的位置也被叠加，则产生的这个卷积核会产生和相加前的卷积核相同的效果，即它们的最终输出是一样的。基于此，可以发现二维卷积是具有可加性的。

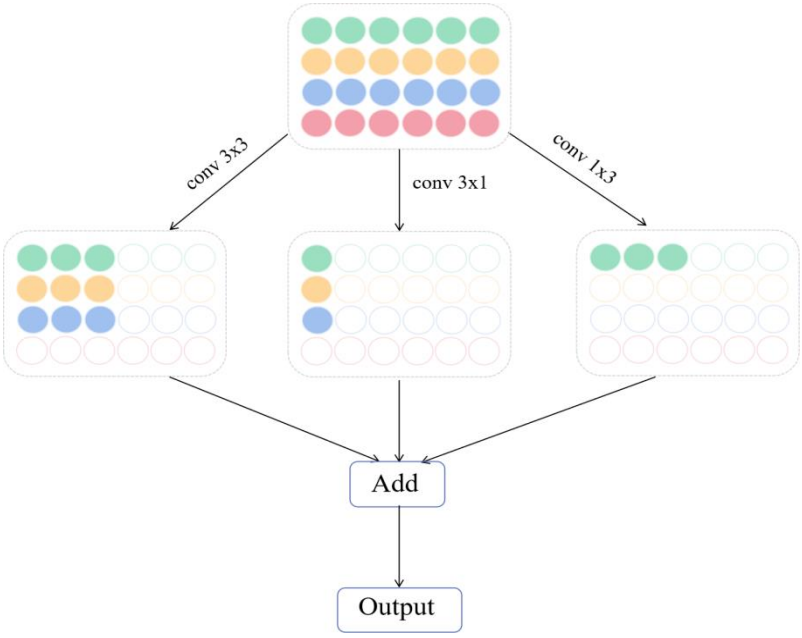


图 4.3　空间信息提取单元

如下面公式所述，I 代表矩阵，$K^{(1)}$、$K^{(2)}$、$K^{(3)}$ 是两个二维卷积核，具有兼容尺寸，可以相互计算。$\oplus$ 代表三个卷积核按照相应的位置进行相加，这样操作并不会带来训练参数的增加。

$$I*K^{(1)}+I*K^{(2)}+I*K^{(3)}=I*\left(K^{(1)}\oplus K^{(2)}\oplus K^{(3)}\right) \tag{4.5}$$

假如利用滑动窗口对卷积进行验证，现在有一个大小为 $H\times W$ 的卷积核，设置通道数为 D，将通道数是 C 的特征图输入，$F\in R^{H\times W\times C}$ 表示卷积核，$M\in R^{U\times V\times C}$ 表示输入，$O\in R^{R\times T\times D}$ 代表输出特征图，对于这一层的第 j 个卷积核，输出特征映射通道为下面所示：

$$O_{:,:,j}=\sum_{K=1}^{C}M_{:,:k}*F_{:,:,k}^{(j)} \tag{4.6}$$

输入特征图第 k 个通道表示为 $M_{:,:,k}$，$*$ 表示的是卷积算子，卷积在 $M_{:,:,k}$ 上面进行滑动，$F_{:,:,k}^{(j)}$ 代表卷积核第 k 个通道。

对于一个指定的点 y，使用卷积核 $F^{(j)}$ 计算输出 $O_{:,:j}$，公式如下：

$$y=\sum_{c=1}^{C}\sum_{h=1}^{H}\sum_{w=1}^{W}F_{h,w,c}^{(j)}X_{h,w,c} \tag{4.7}$$

X 代表输入 M 上相应的滑动窗口，如果使用两个共同的卷积滑动窗口，那么当这两个卷积生成的输出通道相加，公式（4.5）成立。

因此非对称卷积是具有兼容性的，条状卷积核可以和正常卷积进行相互叠加，可以

减少正常卷积的计算量，并且不会损失卷积提取特征的效果。

(2) 非对称卷积在本研究领域的适用性分析

经过分析，卷积具有很强的兼容性，三个分支卷积的融合可以对中心区域再次进行巩固从而达到加强作用。非对称卷积核对于网络安全态势感知数据更加匹配，经过分析已经解到处理的数据帧是一个矩阵，每行每列均带有一定的特征，行列交织，这代表矩阵中每个元素既包含横向的数据信息也包括纵向的时序信息，因此采用非对称的卷积核可以更加贴合矩阵的特性，对特征进行更加详细的特征提取。1×3卷积关注每个数据行内的特征的关联，提取每个特征与其他特征之间的关联，详细分析每个特征之间的影响；3×1卷积核则关注纵向的时序关联，每个特征随着时间而变化，这个变化的趋势又包含着攻击类型的具体特征。基于此基础，结合一个方形卷积，对于全局信息进行建模，利用卷积的可加性将三个分支的特征图进行相加，方形卷积对全局信息处理，非对称卷积核提取的特征进行补充。经过空间特征模块的处理最终得到一个自适应提取全局信息和局部信息的特征图，既包含空间信息和时序关联，也对特征信息进行加强。

4.1.3 时间信息提取单元

本小节介绍时间信息提取单元 TFEU，单元结构如下图 4.4 所示。该单元利用不同尺度的条形卷积核进行特征提取，每个纵向条形卷积核横向移动，提取每个特征内不同时间观测到的数值组成的序列，提取它们之间的关系。本模块采用3×1和5×1的卷积核，两个卷积核分别对数据切片进行建模，不同大小的卷积核具有不同大小的特征提取范围，从而形成两个时间关联提取窗口，3×1卷积提取短时特征，另一个5×1卷积提取长时特征。因为网络流量数据时间跨度较大，每一个到达的数据包并不一定会一直按照顺序排列，数据帧之间存在一定的时间跨度，因此只看短序列的表示特征不一定可以准确判断攻击类别，更长的时间序列代表着更多的时间信息。所以对于时间序列而言，双重时间窗口可以在不同的时间尺度上提取特征，提取多种长度的特征数据，将长时信息和短时信息更好地结合在一起，具有更好的学习能力，模型效果也会有一定的提升。

时间信息提取单元包括两个部分，双重时间窗口进行长短时特征提取和长短时特征融合两部分。

对于长短时特征提取，首先数据帧首先进入得是两个分支，有两个大小不一样的条形卷积核组成，这些卷积等价为两个不同尺度的时间窗口，用于提取数据帧的长时和短时信息。3×1卷积代表短时信息分支，该分支可以将局部时序信息进行提取，将近期流量数据的变化情况进行分析；5×1卷积则是长时信息分支，用于提取长时间的时序信息，

提取范围更大。这些条形卷积，每一次移动，均覆盖一个特征变量时间序列的一部分，按照步长进行移动时，将每个特征变量内的时间特征进行提取，因为卷积核大小有差异，所以每个卷积核覆盖的面积也不同，这样操作可以增加每个单特征时间序列的时间特征多样性，包含更多的时间信息，在长时特征提取的同时，利用短时特征对其进行加强。

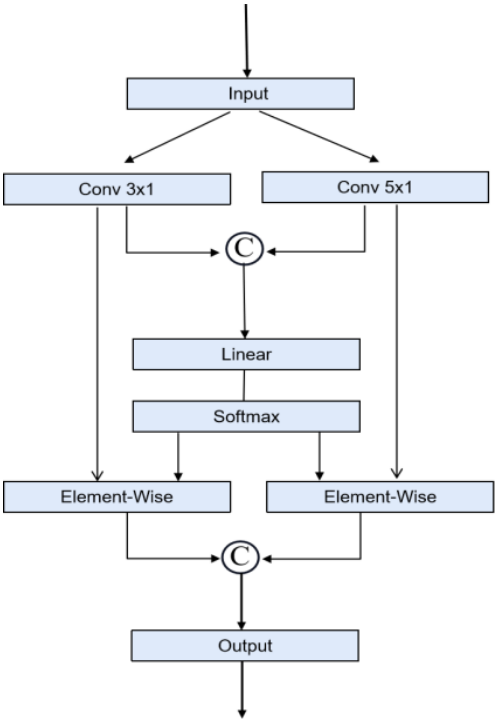


图 4.4　时间特征提取单元

之后对于双重时间窗口的输出有三条路径：

路径 1：将两个输出按照通道进行合并，假如短时分支具有 c_1 个通道，长时分支具有 c_2 个通道，那么经过合并后输出的特征图通道为 c_1+c_2。简单的通道合并会损失两个分支的特征表达[58]。为减缓这一现象，引入一种自适应权重融合机制，将级联后的特征图转换维度，伸展成一维扁平化向量，连接一个线性层，然后利用 Softmax 函数对其进行计算，输出一个元素为 2，映射范围在 0 到 1 的向量，设为 $[g_1,g_2]$,该向量代表两个短时分支和长时分支各自的权重，每个权重用来进行后续操作。

路径 2：短时分支的输出与上一部分计算的权重 g_1 进行逐元素相乘，得到的特征图融入权重值，决定该分支对于最后输出的贡献有多少，权重越大，对于最终分支特征融合时的比例占比也更多。

路径 3：长时分支同路径 2 操作相同，将输出与权重 g_2 逐元素相乘。

最终将路径 2 和 3 的输出进行通道级联，形成最终的时间特征提取模块的输出。

4.2 基于 SaT-CNN 网络安全态势评估过程建立

本文主要是对网络流量包含的攻击活动进行识别和监测，及时发现具有威胁性的危险活动，因为我们处理的数据具有时间自相关和空间互相关，因此从这两个角度出发，构建一个神经网络模型对其进行训练和学习。如图 4.5 所示，下面介绍本章节模型的网络安全态势感知评估流程。

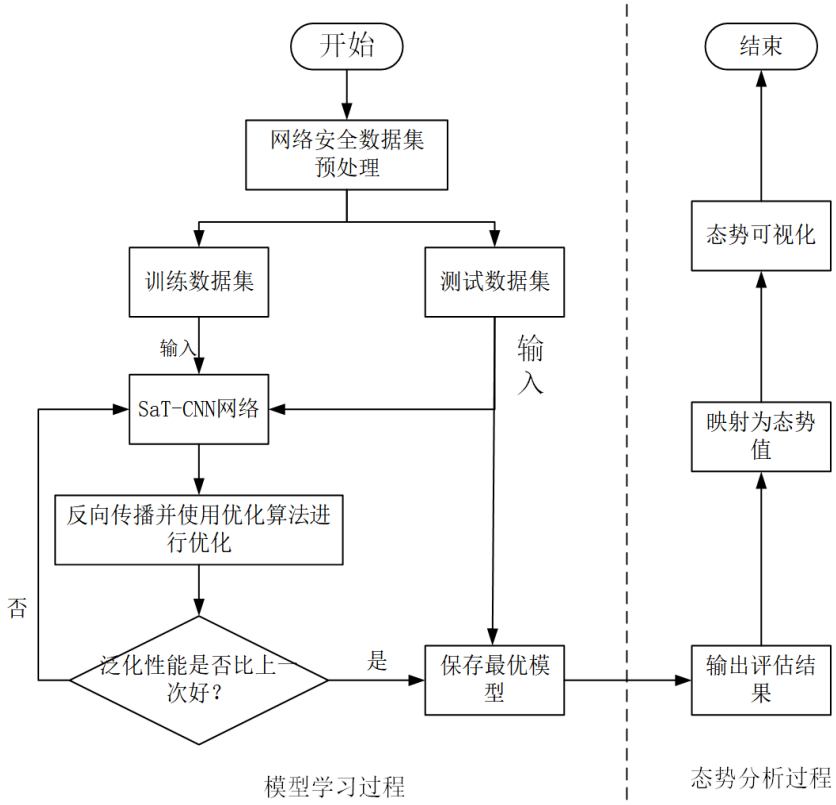


图 4.5 基于 SaT-CNN 网络安全态势评估流程图

步骤 1：选取合适的网络安全流量相关数据集，对其进行特征分析，观察它的数据结构和基本信息。之后进行数据预处理。这一步骤在第二章已经详细论述。

步骤 2：把处理好的数据集分为训练集和测试集。

步骤 3：将经过处理的训练集送进搭建的 SaT-CNN 模型进行训练。在训练过程中，模型对输入数据的特征分布进行学习，重点关注具有辨识度的特征，从而帮助更好地分辨攻击类型。模型学习之后利用真实标签和预测标签之间的误差，反向传播更新模型中的参数。将测试集输入训练模型进行预测，输出预测结果，观察是否达到最优。如果没有达到最优标准，那么将继续进行新一轮的学习，直到模型获得最优参数，达到最优结果。将模型参数进行保存，用于后续的使用。

步骤 4：将测试集的预测结果导出，将预测标签进行态势量化，按照态势评估指标进行计算，将最终态势值输出并进行可视化分析。

4.3 实验结果与分析

4.3.1 实验环境及训练过程

(1) 实验环境和实验分析指标

本章节模型实验仍旧在一台远端服务器上进行，系统版本为 Ubuntu18.04.1 版本，GPU 型号为 NVIDIA GeForce RTX 2080Ti，利用 Pytorch1.7.0 GPU 版深度学习框架，使用 Python 语言进行程序编写。

实验在 UNSW-NB15 数据集中进行，具体的实验指标是依据混淆矩阵的准确率、精确率和 F1 值，原理在第三章中已经详细论述。关于态势评估值量化的问题依据第三章介绍的态势值量化对照表，按照攻击类型造成危害范围的影响差异，对这些攻击进行排序，对其赋予一个定量态势值。

(2) 训练过程

在模型进入学习前，应设置一系列的参数。为保留数据间的时间关联，采用滑动时间窗口，这里时间窗口大小设置为 5，所以每个数据时间帧转换为尺寸（1，5，196）的单通道特征图输入，设置 Batch 为 256，Epoch 设置为 200 次。模型优化采用 Adam 优化器，采用交叉熵损失函数计算训练误差，dropout 设置为 0.2。详细的训练流程如下表所示：

表 4.1 SaT-CNN 模型训练测试过程

SaT-CNN 模型训练测试过程	
模型输入：	网络安全态势训练数据集 输入数据时间帧尺寸：（1，5，196） 批数量：Batch size=256 轮次：epoch=200
模型训练：	将经过预处理的数据时间帧随机选择样本输入到模型中，经过前向传播抵达输出层，计算误差；根据误差进行参数寻优，调整模型参数，直到模型结果最优
模型测试：	每一轮次运行完毕时，对测试集进行预测
模型输出：	最优模型预测的测试集攻击类别标签

4.3.2 UNSW-NB15 数据集实验结果分析

本章提出的 SaT-CNN 网络安全态势评估模型由时空信息联合提取模块堆叠而成，该模块则又包含时间特征提取单元、空间特征提取单元和门控融合注意力机制。为验证本章提出的卷积结构的有效性，引入决策树、LSTM、ResNet 进行准确率等指标对比。同时为了验证模型内部结构的有效性，将时间特征提取单元、空间提取单元以及联合提取模块进行对比分析，分别命名为 SaT-CNN、SFEU-CNN、TFEU-CNN。实验设置二分类和十分类两组实验，二分类用于对模型效果进行初步分析，但是由于二分类标签类别较少，并且正常和异常标签数量差距较大，因此后续在十分类实验中进一步对模型效果进行验证。

(1) 基于 SaT-CNN 的二分类态势评估实验分析

1) 关于测试集的准确率、精确率、F1 值对比

表 4.2 实验指标对比

模型	卷积	时间特征提取单元	空间特征提取单元	时空信息联合提取模块	准确率（%）	精确率（%）	F1 值（%）
DT					91.23	91.32	91.17
LSTM					98.15	98.14	98.14
ResNet					98.74	98.72	98.73
CNN	√				98.95	98.96	98.96
TFEU-CNN	√	√			99.12	99.13	99.12
SFEU-CNN	√		√		**99.15**	**99.14**	**99.15**
SaT-CNN	√			√	**99.16**	**99.15**	**99.16**

如表 4.2 所示，在相同实验环境中，本文所提出的结构在准确率、精确率和 F1 值中均优于决策树、LSTM、ResNet、CNN 模型，证明本章模型在网络安全态势评估中具有不错的效果。其中空间信息提取单元（SFEU）和时间信息提取单元（TFEU）的各项指标均高于基础 CNN，证明本模型从时间和空间角度对流量数据进行处理是有效的。关于 SaT-CNN 中的时空信息联合提取模块与单独的 SFEU 和 TFEU 相比，各项指标均有所提高，SaT-CNN 模型的准确率是 99.16%，精确率是 99.15%，F1 值是 99.16%，说明时空特征融合提取有助于提高网络安全态势评估准确度。

2) 与改进 Res2Net 模型的对比分析

通过表 4.3 可发现，SaT-CNN（模型 2）在准确率、精确率、F1 值等方面均略高于改进 Res2Net 模型（模型 1），差距在 0.01~0.02%之间浮动，并且在训练时间方面模型 2 比模型 1 显著减少，说明模型 2 在保有较高分类精度的情况下，训练速度有所提高，减少了训练成本。

表 4.3　SaT-CNN 与改进 Res2Net 对比

模型	准确率（%）	精确率（%）	F1 值（%）	时间（/10^2s）
改进 Res2Net（模型 1）	99.14	99.13	99.14	1.96
SaT-CNN（模型 2）	99.16	99.15	99.16	0.97

3)　SaT-CNN 的 loss 损失和训练集测试集准确率对比

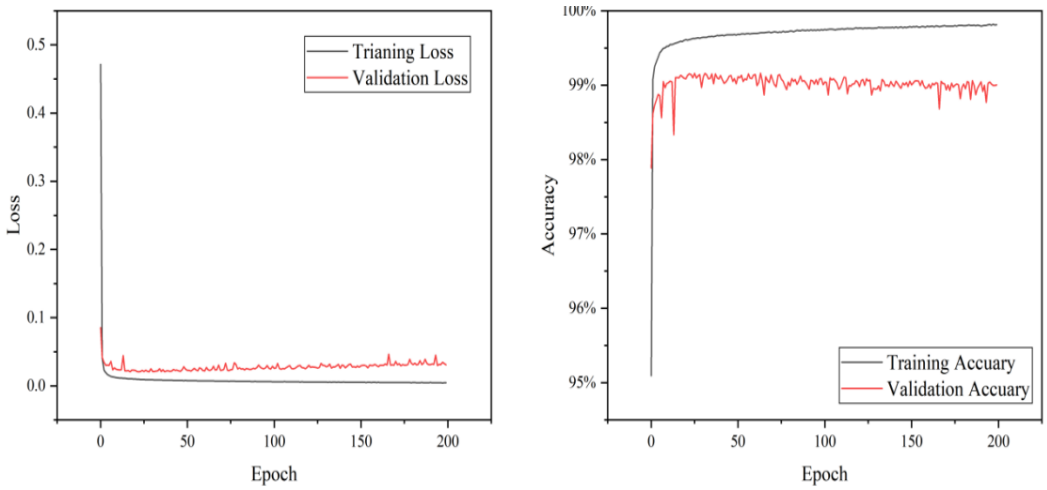


图 4.6　训练集和测试集 loss 值（左）和准确率（右）曲线

图 4.6 中分别为训练集和测试集在 SaT-CNN 模型的 loss 损失和准确率随着 Epoch 的增加而变化的过程。由图左可观察到本文模型在训练集和测试集上的损失值逐渐下降并趋于平缓，在 Epoch 为 25 之后逐渐稳定，训练集的损失值逐渐稳定之后无较大波动，测试集的损失虽然趋于稳定但存在些微波动。图中可观察到训练集和测试集的准确率随着轮次的增加的变化情况，可观察到训练集和测试集的准确率在 Epoch 为 25 之后逐渐稳定，训练集由于模型学习能力的逐渐加强不断提升准确率，测试集伴随出现一些过拟合现象。

4)　SaT-CNN 模型预测态势值可视化

如图 4.7 所示，该图是在测试集中随机抽取 5000 条数据，根据其预测类别标签，按照态势值评估对照表进行转换。经过观察，发现红色曲线覆盖大多数蓝色曲线，说明 SaT-CNN 的模型提取能力较为不错，能够有效辨别攻击类型。

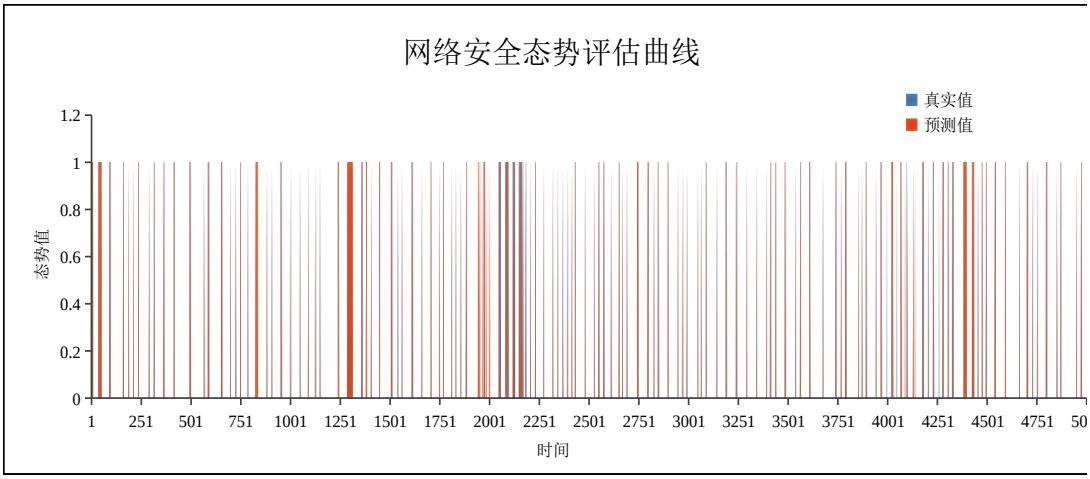


图 4.7　测试集态势评估曲线

(2)　基于 SaT-CNN 的十分类态势评估实验分析

1)　关于测试集的准确率、精确率、F1 值对比

表 4.4 展示的是针对同一数据集进行的十分类实验评价指标，其中本文所提出的模型和模块各项指标均高于决策树、LSTM、ResNet、CNN，证明本章模型结构从时间、空间角度综合考虑有助于提升态势评估准确率。时间信息提取单元和空间信息提取单元分别结合 CNN 进行实验，可发现，准确率、精确率和 F1 值，均有一些提升，证明本章所提模块对时间和空间信息具有适用性。SaT-CNN 模型的准确率、精确率和 F1 值分别是 96.95%，96.89%，96.74%，对比单独的两个信息提取单元分类效果更好，说明本模型可以将时空特征更好地进行提取，提升了模型的准确性。

表 4.4　实验指标对比

模型	卷积	时间特征提取单元	空间特征提取单元	时空信息联合提取模块	准确率（%）	精确率（%）	F1 值（%）
DT					87.63	88.32	87.51
LSTM					90.31	90.15	90.28
ResNet					94.05	93.67	93.86
CNN	√				96.50	96.75	96.34
TFEU-CNN	√	√			96.79	**96.85**	**96.69**
SFEU-CNN	√		√		**96.88**	96.76	96.63
SaT-CNN	√			√	**96.95**	**96.89**	**96.74**

2)　与改进 Res2Net 模型的对比分析

表 4.5　SaT-CNN 与改进 Res2Net 对比

模型	准确率（%）	精确率（%）	F1 值（%）	时间（/10^2s）
改进 Res2Net（模型 1）	96.83	96.86	96.61	1.67
SaT-CNN（模型 2）	96.95	96.89	96.74	0.93

观察表 4.5 发现，SaT-CNN 模型（模型 2）对比改进 Res2Net 模型（模型 1）在准确率、精确率、F1 值等方面均有提升，并且减少了训练时间，模型 2 相比模型 1 每一轮次的训练时间减少 74s，说明有效缩短了训练时间，训练成本也有所降低。

3)　关于训练集和测试集的 loss 损失和准确率对比

通过观察图 4.8 中左图，发现训练集和测试集在 Epoch 为 15 时损失值逐渐趋于稳定，并且保持平稳状态，其中训练集随着学习能力的加强，损失值逐渐减小，测试集趋于稳定，并偶有波动。观察图右发现，训练集和测试集的准确率随着 Epoch 的变化逐渐增加，训练集的准确率不断上升，并逐渐平稳；而测试集的准确率在经过最高值之后趋于稳定，并且通过两张图对比发现，测试集损失值和准确率在同一训练轮次存在波动曲线，说明当测试集损失函数值发生波动时，准确率也会受到影响。

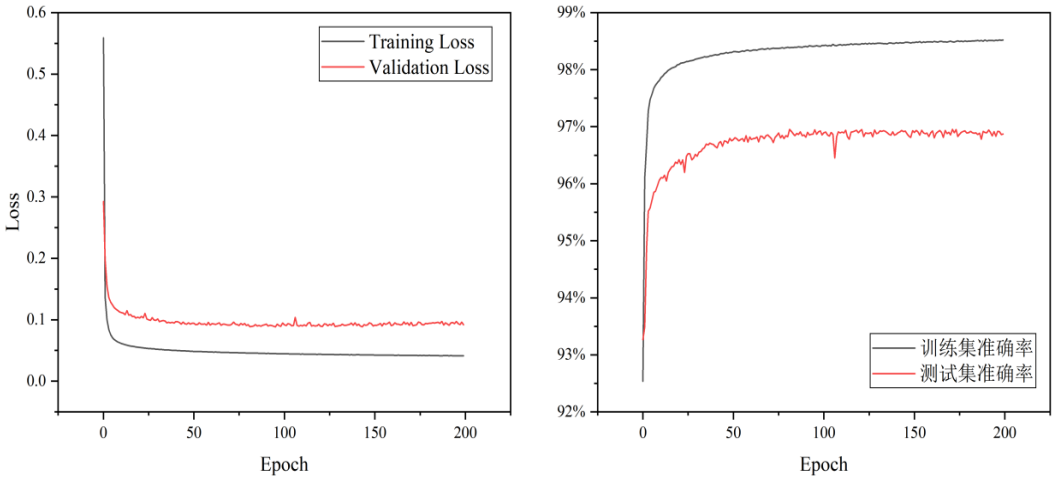


图 4.8　训练集和测试集 loss 值（左）和准确率（右）曲线

4)　测试集经过 SaT-CNN 模型预测的态势值可视化

通过观察图 4.9 的评估曲线，可发现红色值遮盖住大部分蓝色面积，输出的态势值可以与真实值进行有效拟合，证明本章模型对攻击类型可以进行有效判断。

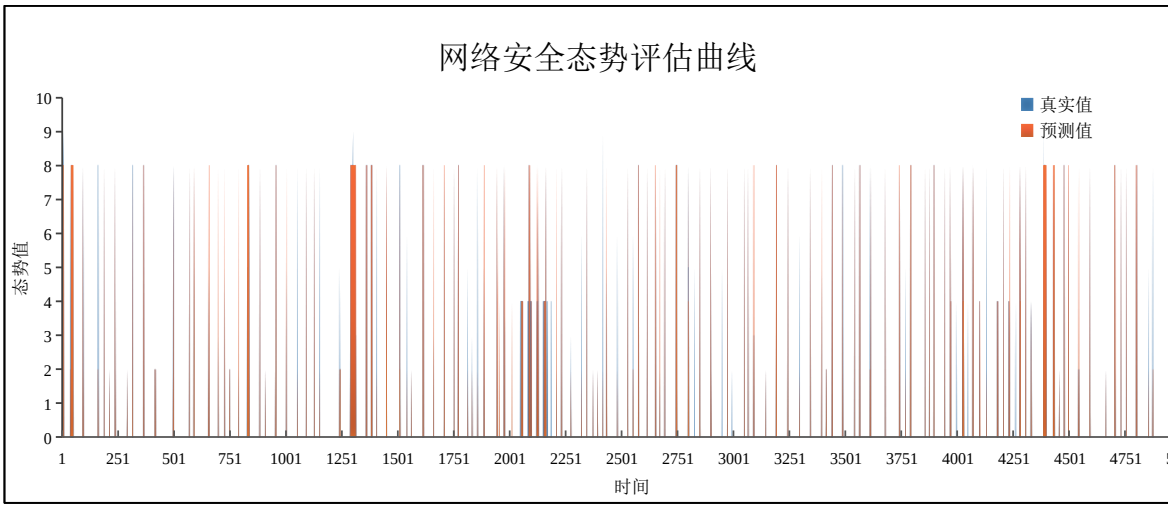


图 4.9　测试集态势评估曲线

4.4　本章小结

本章介绍一种基于 SaT-CNN 的网络安全态势评估模型，以 CNN 为基础模型，从网络流量数据的时间和空间角度出发，经由时空信息联合特征提取模块堆叠而成。该模块主要结构为并联而成的时间信息提取单元和空间信息提取单元，对输入特征进行时空特征提取，之后经由一个门控融合机制对时空特征进行自适应融合，从而提升模型对攻击类别的识别能力。空间信息提取单元利用卷积可加性对提取的特征进行加强，并且减少计算量，可以较好匹配输入流量数据的结构；时间信息提取单元利用非对称卷积设计双重窗口，对流量数据包含的长时和短时时间信息进行提取，两个窗口提取的信息相互补充，有助于时间信息的深度提取。

本章节在 UNSW-NB15 数据集中进行实验，通过对比实验表明，本章提出的网络安全态势评估模型具有较高的准确率，有效识别网络中的攻击，为网络防御提供正向支持。

5 总结与展望

5.1 工作总结

随着互联网基础设施规模的扩大，逐渐复杂的网络数据对维护网络安全增加了难度。为了应对日益复杂和层出不穷的网络威胁，一些学者将态势感知引入网络安全领域，希望利用它从大量的噪声数据中识别出网络。为了尽可能减少攻击造成的损失，帮助网络管理人员从宏观上把握整个网络的安全状况，合理有效地进行应对，提高网络系统的监测和应急响应能力。本文提出两种基于卷积神经网络的网络安全态势评估模型，主要工作如下：

(1) 提出了一种基于改进 Res2Net 的网络安全态势评估模型。针对深层神经网络特征表达力强的优点，结合流量数据具有时空特征，引入 Res2Net 作为基础模型。通过构建一种通道-空间模块对特征图的通道和空间维度建模，避免单一维度造成信息损失。通道模块采用 GCT 通道变换注意力机制，通过对特征的显示计算得到通道间的关系，促成通道间的竞争和合作关系。空间模块通过条带池化时空全局特征融合单元，利用条带池化产生的特殊形状窗口可以对网络流量数据的形状进行契合的特点，将时间维度和空间维度的全局特征进行提取，数据矩阵中每个元素所在的时间维度和空间维度会形成独一无二的权重值，该值代表此元素信息在特征图上的重要性。本模型在 UNSW-NB15 数据集中进行验证，各项指标证明模型可以对流量信息有效检测。

(2) 为了提高训练速度，并且保持高准确率，提出了一种基于 SaT-CNN 的网络安全态势感知评估模型。针对网络流量数据具有的时间特征和空间特征，设计一种时空信息联合提取模块，通过对时间特征和空间特征的分支并行提取，得到具备时空信息的流量特征图，之后通过门控融合机制将时间特征图和空间特征图进行融合，将时空信息进行筛选，对更加关注的信息进行加权，筛选出的信息有益于攻击类别分类。时空信息联合提取模块包含空间信息提取单元和时间信息提取单元。前者利用卷积对整张特征图蕴含的特征进行全局提取，其中非对称卷积利用卷积的可加性对提取的特征增强表达能力；后者利用不同尺寸的非对称卷积对特征图的时间信息进行提取，不同尺度的卷积组成双重窗口对时间信息提取长时和短时特征，增加时间维度特征的多样性。最后通过 UNSW-NB15 数据集对模型进行验证，证明该模型可以对攻击类别进行有效识别。

5.2 局限性与展望

本文针对流量数据蕴含的时空特征，结合卷积神经网络的特征表达能力构建两种网络安全态势感知评估模型，借此提高模型对攻击类别的辨别度。但是本文的模型仍然存在一些不足，未来将从以下几个方面进一步完善：

(1) 网络安全原始的数据来自各种基础设施中收集的信息，包括网络拓扑结构、网络流量、操作系统、日志信息等多种不同结构的信息，只单独分析网络流量存在一定的局限性，因此在后续研究中将寻求更好的融合方式对多源数据进行处理 ，完整有效地分析网络中的态势信息。

(2) 虽然本文模型在十分类实验中证明了有效性，但是由于数据集在二分类标签中正常和异常标签数量差距过大，导致本文实验模型在二分类实验中存在的指标差距并不明显，未来将会继续对二分类实验进一步改进提升。

(3) 本文提出的态势评估模型采取 UNSW-NB15 数据集学习是考虑到随机划分的数据集将会存在时间连续性上的影响，但是仅仅单一数据集不能证明模型在多种环境中的泛用性，因此在后续研究中将会寻找更多合适的数据集进一步验证本文模型的性能。

(4) 针对现今存在的深度学习模型均是对于已经存在的攻击类型进行学习，对于新型攻击的识别度有待考证，后续工作中可以结合无监督、自监督等方法结合本文模型进一步研究，提高攻击识别度。

参考文献

[1] 中国网络空间研究院.中国互联网发展报告 2022[M].北京:电子工业出版社,2022.

[2] 中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要[N].人民日报,2021-03-13(001).DOI:10.28655/n.cnki.nrmrb.2021.002455.

[3] 桂畅旎.2021 年全球网络空间安全态势回眸[J].中国信息安全,2021,No.145(12):32-38.

[4] 黄志雄,陈徽.供应链安全国际法保护的困境与出路——以“太阳风”事件为切入点[J].厦门大学学报(哲学社会科学版),2022,72(01):62-76.

[5] 赵子鹏,张奇.解读重大勒索攻击事件下的网络安全态势及应对[J].中国信息安全,2021(06):64-67.

[6] 李恒阳.俄乌冲突网络对抗及其对网络空间安全的影响[J].中国信息安全,2022(06):83-86.

[7] 瑞星 2020 年中国网络安全报告[J].信息安全研究,2021,7(02):102-109.

[8] Bass T. Multisensor data fusion for next generation distributed intrusion detection systems[C]//Proceedings of the IRIS National Symposium on Sensor and Data Fusion. Citeseer, 1999, 24(28): 24-27.

[9] 陈秀真,郑庆华,管晓宏,林晨光.层次化网络安全威胁态势量化评估方法[J].软件学报,2006(04):885-897.

[10] Wang H, Chen Z, Feng X, et al. Research on network security situation assessment and quantification method based on analytic hierarchy process[J]. Wireless Personal Communications, 2018, 102: 1401-1420.

[11] 韩晓露, 刘云, 张振江, 等. 基于直觉模糊集的网络安全态势评估方法[J]. 吉林大学学报: 工学版, 2019 (1): 261-267.

[12] Fan Z, Tan C, Li X. A hierarchical method for assessing cyber security situation based on ontology and fuzzy cognitive maps[J]. International Journal of Information and Computer Security, 2021, 14(3-4): 242-262.

[13] Zhao X, Zhang Y, Xue J, et al. Research on network risk evaluation method based on a differential manifold[J]. IEEE Access, 2020, 8: 66315-66326.

[14] Zhao D, Wang H, Wu Y. Situation Element Extraction Based on Fuzzy Rough Set and Combination Classifier[J]. Computational Intelligence and Neuroscience, 2022, 2022.

[15] Alali M, Almogren A, Hassan M M, et al. Improving risk assessment model of cyber security using fuzzy logic inference system[J]. Computers & Security, 2018, 74: 323-339.

[16] Doynikova E, Kotenko I. CVSS-based probabilistic risk assessment for cyber situational awareness and countermeasure selection[C]//2017 25th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP). IEEE, 2017: 346-353.

[17] Liao Y, Zhao G, Wang J, et al. Network Security Situation Assessment Model Based on Extended Hidden Markov[J]. Mathematical Problems in Engineering, 2020, 2020: 1-13.

[18] Hu J, Guo S, Kuang X, et al. I-HMM-Based Multidimensional Network Security Risk Assessment[J]. IEEE Access, 2019, 8: 1431-1442.

[19] 张恒巍,张健,韩继红.基于非合作博弈攻击预测的防御策略选取方法[J].计算机科学,2016,43(01):195-201.

[20] Niazi R A, Faheem Y. A bayesian game-theoretic intrusion detection system for hypervisor-based software defined networks in smart grids[J]. IEEE Access, 2019, 7: 88656-88672.

[21] Lin P, Chen Y. Dynamic network security situation prediction based on bayesian attack graph and big data[C]//2018 IEEE 4th Information Technology and Mechatronics Engineering Conference (ITOEC). IEEE, 2018: 992-998.

[22] Li Y, Yao S, Zhang R, et al. Analyzing host security using D‐S evidence theory and multisource information fusion[J]. International Journal of Intelligent Systems, 2021, 36(2): 1053-1068.

[23] Banerjee J, Maiti S, Chakraborty S, et al. Impact of machine learning in various network security applications[C]//2019 3rd International Conference on Computing Methodologies and Communication (ICCMC). IEEE, 2019: 276-281.

[24] Chen Y, Yin X, Sun A. Network security situation assessment model based on GSA-SVM[C]//Proceedings of 2018 International Conference on Computer, Communication and Network Technology (CCNT). 2018: 414-420.

[25] Hu J, Ma D, Liu C, et al. Network security situation prediction based on MR-SVM[J]. IEEE Access, 2019, 7: 130937-130945.

[26] Zhao D, Ji G, Zeng S. A Network Security Situation Assessment Method Based on Multi-attention Mechanism and HHO-ResNeXt[C]//Security and Privacy in Social Networks

and Big Data: 8th International Symposium, SocialSec 2022, Xi'an, China, October 16–18, 2022, Proceedings. Singapore: Springer Nature Singapore, 2022: 199-211.

[27] Wang G. Comparative study on different neural networks for network security situation prediction[J]. Security and Privacy, 2021, 4(1): e138.

[28] 程家根,祁正华,陈天赋.基于 RBF 神经网络的网络安全态势感知[J].南京邮电大学学报(自然科学版),2019,39(04):88-95.

[29] 王金恒,单志龙,谭汉松等.基于遗传优化 PNN 神经网络的网络安全态势评估[J].计算机科学,2021,48(06):338-342.

[30] Haider N, Baig M Z, Imran M. Artificial Intelligence and Machine Learning in 5G Network Security: Opportunities, advantages, and future research trends[J]. arXiv preprint arXiv:2007.04490, 2020.

[31] Nikoloudakis Y, Kefaloukos I, Klados S, et al. Towards a machine learning based situational awareness framework for cybersecurity: an SDN implementation[J]. Sensors, 2021, 21(14): 4939.

[32] Dong Z, Su X, Sun L, et al. Network security situation prediction method based on strengthened LSTM neural network[C]//Journal of Physics: Conference Series. IOP Publishing, 2021, 1856(1): 012056.

[33] Hernández A, Amigó J M. Attention mechanisms and their applications to complex systems[J]. Entropy, 2021, 23(3): 283.

[34] Li Z, Zhao D, Li X, et al. Network security situation prediction based on feature separation and dual attention mechanism[J]. EURASIP Journal on Wireless Communications and Networking, 2021, 2021(1): 1-19.

[35] 何春蓉,朱江.基于注意力机制的 GRU 神经网络安全态势预测方法[J].系统工程与电子技术,2021,43(01):258-266.

[36] Yao C, Yang Y, Yang J, et al. A Network Security Situation Prediction Method through the Use of Improved TCN and BiDLSTM[J]. Mathematical Problems in Engineering, 2022, 2022.

[37] 张任川,张玉臣,刘璟等.应用改进卷积神经网络的网络安全态势预测方法[J].计算机工程与应用,2019,55(06):86-93.

[38] Nirmala P, Manimegalai T, Arunkumar J R, et al. A Mechanism for Detecting the Intruder

in the Network through a Stacking Dilated CNN Model[J]. Wireless Communications and Mobile Computing, 2022, 2022.

[39] Wang W, Sheng Y, Wang J, et al. HAST-IDS: Learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection[J]. IEEE access, 2017, 6: 1792-1806.

[40] Cao B, Li C, Song Y, et al. Network Intrusion Detection Model Based on CNN and GRU[J]. Applied Sciences, 2022, 12(9): 4184.

[41] Endsley M R. Design and evaluation for situation awareness enhancement[C]//Proceedings of the Human Factors Society annual meeting. Sage CA: Los Angeles, CA: Sage Publications, 1988, 32(2): 97-101.

[42] Hall D L, Llinas J. An introduction to multisensor data fusion[J]. Proceedings of the IEEE, 1997, 85(1): 6-23.

[43] Krizhevsky A, Sutskever I, Hinton G E. Imagenet classification with deep convolutional neural networks[J]. Communications of the ACM, 2017, 60(6): 84-90.

[44] Szegedy C, Liu W, Jia Y, et al. Going deeper with convolutions[C]//Proceedings of the IEEE conference on computer vision and pattern recognition. 2015: 1-9.

[45] He K, Zhang X, Ren S, et al. Deep residual learning for image recognition[C]//Proceedings of the IEEE conference on computer vision and pattern recognition. 2016: 770-778.

[46] Alzubaidi L, Zhang J, Humaidi A J, et al. Review of deep learning: Concepts, CNN architectures, challenges, applications, future directions[J]. Journal of big Data, 2021, 8: 1-74.

[47] Bala R, Nagpal R. A review on kdd cup99 and nsl nsl-kdd dataset[J]. International Journal of Advanced Research in Computer Science, 2019, 10(2).

[48] Brown C, Cowperthwaite A, Hijazi A, et al. Analysis of the 1999 darpa/lincoln laboratory ids evaluation data with netadhict[C]//2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications. IEEE, 2009: 1-7.

[49] 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.

[50] Gao S H, Cheng M M, Zhao K, et al. Res2net: A new multi-scale backbone

architecture[J]. IEEE transactions on pattern analysis and machine intelligence, 2019, 43(2): 652-662.

[51] Yang Z, Zhu L, Wu Y, et al. Gated channel transformation for visual recognition [C]//Proceedings of the IEEE/CVF conference on computer vision and pattern recognition. 2020: 11794-11803.

[52] Hou Q, Zhang L, Cheng M M, et al. Strip pooling: Rethinking spatial pooling for scene parsing[C]//Proceedings of the IEEE/CVF conference on computer vision and pattern recognition. 2020: 4003-4012.

[53] Woo S, Park J, Lee J Y, et al. Cbam: Convolutional block attention module[C]//Proceedings of the European conference on computer vision (ECCV). 2018: 3-19.

[54] Doynikova E, Fedorchenko A, Kotenko I. Ontology of metrics for cyber security assessment[C]//Proceedings of the 14th International Conference on Availability, Reliability and Security. 2019: 1-8.

[55] Li S, Zhao D, Li Q. A framework for predicting network security situation based on the improved LSTM[J]. EAI Endorsed Transactions on Collaborative Computing, 2020, 4(13).

[56] Kim J, Koh J, Kim Y, et al. Robust deep multi-modal learning based on gated information fusion network[C]//Computer Vision–ACCV 2018: 14th Asian Conference on Computer Vision, Perth, Australia, December 2–6, 2018, Revised Selected Papers, Part IV. Cham: Springer International Publishing, 2019: 90-106.

[57] Ding X, Guo Y, Ding G, et al. Acnet: Strengthening the kernel skeletons for powerful cnn via asymmetric convolution blocks[C]//Proceedings of the IEEE/CVF international conference on computer vision. 2019: 1911-1920.

[58] Liu M, Ren S, Ma S, et al. Gated transformer networks for multivariate time series classification[J]. arXiv preprint arXiv:2103.14438, 2021.