一、个人小结

1、思想品德和科研诚信

自进入研究生阶段以来，我在思想品德和科研诚信方面不断提升自我，力求在学术道路上成为一名有责任感和社会担当的研究者。作为一名研究生，我深知这一阶段不仅仅是知识积累和技能提升的过程，更是个人品德和学术诚信建设的关键时期。这段时间的学习和实践，使我在思想道德修养、社会责任感以及科研诚信意识方面得到了深刻的锻炼和成长。

首先，在思想品德方面，我始终以严谨的态度和高尚的道德标准要求自己。研究生阶段是学术生涯的重要起点，我深刻意识到，作为一名学者，不仅要具备扎实的专业知识，更要具备良好的思想品德和道德修养。在学习过程中，我注重培养自己的社会责任感，始终将个人的发展与国家和社会的进步紧密联系在一起。我认为一个合格的研究生不仅应该追求个人学术成就，更应该以服务社会、贡献国家为己任。在思想品德的修养过程中，我特别注重加强自律意识和道德自觉。研究生阶段的学习生活相对自由，如何合理安排时间，如何在面对诱惑时保持初心，都是对个人品德和意志力的重大考验。为了在学术和生活中保持高标准的道德操守，我制定了严格的自我约束机制，时刻提醒自己保持良好的道德风范。在学术活动中，我严格遵守学术规范，尊重他人劳动成果，绝不容忍任何形式的学术不端行为。在日常生活中，我注重言行一致，待人接物真诚友善，力求在日常小事中践行高尚的道德准则。

其次，在科研诚信方面，我始终坚持严谨治学、实事求是的科研态度，力求在学术研究中做到诚实、透明和公正。科研诚信是学术研究的基石，是确保研究成果真实可靠的基本保障。自研究生入学以来，我不断学习并遵循科研诚信的各项要求，严格恪守学术道德。在科研工作中，我始终坚持以事实为依据，以数据为支撑，绝不弄虚作假。在撰写学术论文时，我仔细核对每一个数据和每一个结论，确保所发表的研究成果真实可信。此外，我严格按照学术规范进行文献引用，尊重他人的知识产权，坚决杜绝抄袭、剽窃等不端行为。在科研实践中，我始终遵循科学研究的客观规律，尊重事实和数据，拒绝一切可能影响研究公正性的行为。例如，在进行实验数据的采集和分析时，我严格按照既定的实验方案操作，确保数据的真实性和可靠性。对于实验中出现的意外情况，我会如实记录并分析原因，而不是为了追求理想结果而进行数据篡改或选择性忽略。我深知，任何学术研究都应该经得起时间和同行的检验，只有坚持科研诚信，才能为学术界贡献真正有价值的知识和成果。在参与科研项目的过程中，我始终保持严谨和诚信的科研态度。在课题的设计和执行阶段，我认真思考每一个实验步骤，反复推敲每一个理论假设，确保研究设计的科学性和合理性。在数据分析和结果解读阶段，我坚持实事求是的原则，尊重实验数据的客观性，避免主观偏见的影响。在撰写学术论文时，我注重详细记录研究的全过程，并严格按照学术规范进行引用和致谢，尊重他人的知识贡献，确保论文的学术质量和诚信度。

最后，我深刻认识到，科研诚信不仅仅是学术研究中的要求，更是一个研究生应当具备的基本品质和职业素养。随着信息时代的到来，学术界面临着前所未有的挑战和机遇，如何在复杂多变的环境中坚守科研诚信，如何在利益诱惑面前保持初心，是每一个研究生都必须面对的考验。在今后的学习和科研工作中，我将继续坚定不移地践行科研诚信，保持对知识的敬畏和对真理的追求，为学术界的健康发展贡献自己的一份力量。

2、学位论文中期进展情况（根据学位论文选题，说明已取得的阶段性成果、下一步的工作计划和研究内容，如与选题报告内容不符，必须进行论证说明）

物联网（IoT）边缘计算的迅猛发展为各种智能应用提供了前所未有的机会，但与此同时，也带来了日益复杂的安全威胁。入侵检测作为保障边缘计算环境安全的关键技术，近年来成为研究的热点。然而，由于物联网环境的异构性、资源限制以及动态性，传统的入侵检测方法在边缘计算场景下面临诸多挑战和局限。在过去几年中，物联网网络攻击的频率和复杂程度都显著增加，网络犯罪分子可以危害和利用物联网网络来执行恶意活动，例如物联网勒索软件、僵尸网络DDoS攻击。网络入侵检测系统（NIDS）位于物联网内的战略点，用于监控流量，是检测和缓解基于网络的网络攻击的重要工具。本课题经过对现有研究的调研发现，传统的机器学习和深度学习方法在进行复杂的网络攻击检测时，尚未充分挖掘和利用网络流数据中固有的结构化特征和拓扑信息。这种信息包含了网络节点之间的关系、流量的路径模式以及数据包的相互依赖性，如果能够有效利用，将有助于提高检测的精度和对高级威胁的识别能力。然而，目前大多数现有的方法仍然侧重于数据的平面特征，未能充分整合网络流中的复杂拓扑关系与动态交互，导致在面对高级持续性威胁（APT）等复杂攻击时，检测的准确性和鲁棒性仍有待提升。在边缘计算环境中进行负载异常检测时，现有的方法主要依赖于传统的统计分析和机器学习技术，然而这些方法在应对边缘节点复杂的负载特性和动态环境时仍然存在局限性。边缘计算节点通常具有异构性和分布式特性，其负载不仅受到本地任务处理的影响，还会因为网络延迟、资源分配、数据传输等多方面的动态变化而波动。这些因素使得负载数据呈现出非线性、非平稳性等复杂特征，给异常检测带来了挑战。然而，目前大多数现有的方法仍然主要侧重于单点或局部的负载分析，未能充分捕捉和利用节点之间的协同工作关系和全局负载模式。缺乏对负载数据中固有的时序相关性和空间关联性的综合分析，使得这些方法在应对负载突发性波动以及长期趋势变化时，检测的准确性和实时性仍有待提升。对此，本课题针对以上问题将研究内容分为三个方面：1）通过改进的图神经网络（GNN）提取图数据的边缘特征，并借助Kolmogorov-Arnold网络（KAN）优化模型的表示能力，使得模型能更准确地识别边缘计算节点的网络入侵行为，提高网络入侵威胁的检测效率；2）通过引入快速傅里叶变换（FFT）的尺度学习与转换层，结合Inception模块与自适应图卷积网络的双分支多尺度卷积方法，并集成改进的注意力机制，以增强边缘计算节点的负载异常检测能力；3）为整合上述技术并提升用户交互体验，本课题拟开发一个智能化的可视化入侵检测系统，该系统通过实时监控和分析网络流量及设备状态，协同网络入侵检测与节点负载异常检测方法，以直观的用户界面有效呈现潜在的入侵行为与异常负载情况，从而进一步提升系统在边缘计算环境中的应用效率与实用性。以下章节将详细介绍本课题已完成的主要工作内容。2.4节将介绍下一步工作计划，旨在进一步优化模型性能并扩展实验验证，确保系统在多样化场景下的广泛适用性。

2.1 基于改进的GNN边缘计算节点网络入侵检测方法研究

2.1.1 网络图的构建

网络流（例如，Net-Flow）是记录生产网络中通信的常见格式，在网络入侵检测系统（NIDS）的背景下，它也是最常见的格式。流记录通常包括用于标识通信源和目的地的字段，而记录的其他字段则提供有关流的进一步信息，如数据包数、字节数、流持续时间等。因此，图结构为建模此类数据提供了一种非常自然的方式。本课题采用了以下四个流字段来确定图的边缘：源IP地址、源（L4）端口、目标IP地址和目标（L4）端口。前两个字段形成一个二元组，用于标识源节点，而后两个字段则标识

流的目标节点。额外的流字段则提供与相应图边关联的特征。例如，源节点（172.26.185.48：52962）与目标节点（192.168.1.152：80）交换数据，相应的流可以表示为网络边。由于在我们的图构建过程中，所有剩余的流记录字段都被分配给了边，因此图节点是无特征的。在此算法中，我们为所有节点分配一个一向量，即所有值均为一的向量。接着，将数据划分为训练集和测试集，前者用于模型训练，后者用于性能评估。在数据集划分过程中，确保数据分布的 一致性。最后，将类别特征转换为数值特征，并应用StandardScaler函数进行归一化，以确保特征值在均值为 0 且方差为 1 的标准正态分布中均匀分布。

2.1.2 面向边分类的SK-EGraphSAGE算法

传统图神经网络，如GraphSAGE，虽已在广泛应用中取得显著成果，但其主要聚焦于节点特征进行节点分类，仅有少数方法探索了边特征在边分类中的应用。为此，本研究提出了SK-EGraphSAGE算法，旨在嵌入过程中更有效地提取边缘信息，从而实现网络流分类，即区分正常流量与攻击流量。这一算法为边嵌入和边分类提供了坚实基础。

网络入侵检测系统的核心目标是检测并识别恶意流量与网络流。在本研究的网络流图表示中，边分类问题的关键信息作为边特征提供。因此，现有的NIDS基准数据集通常将网络流信息表示为边特征，而非节点特征，从而仅支持边分类。相比之下，大多数现有的GNN研究仍然集中于节点分类，提出的解决方案难以应用于NIDS背景下的边分类问题。为克服这一局限性，SK-EGraphSAGE通过捕捉边特征与拓扑信息，将有效增强网络入侵检测能力。

为了有效纳入边特征，必须对图中的边信息进行采样和聚合。此外，算法的最终输出应生成边嵌入，而非原始算法所提供的节点嵌入。鉴于基于流量的NIDS数据集仅包含流量（即边）特征而不包含节点特征，因此我们仅利用提供的边特征。使用向量$\mathbf{x}_v = \{1, \ldots, 1\}$来初始化节点特征（以及初始节点嵌入），并且全一向量的维度与边特征的数量相同。本课题设计的邻域聚合函数在第k层生成采样邻域边的聚合嵌入，而不再采用标准的GraphSAGE节点聚合函数，如下所示：

$$\mathrm{h}^{\mathrm{k}}_{\mathcal{N}(v)} \leftarrow \mathrm{AGG}_k\left(\left\{\mathrm{SKAtten}(\mathrm{e}^{k-1}_{uv}), \forall u \in \mathcal{N}(v), uv \in \mathscr{E}\right\}\right),$$

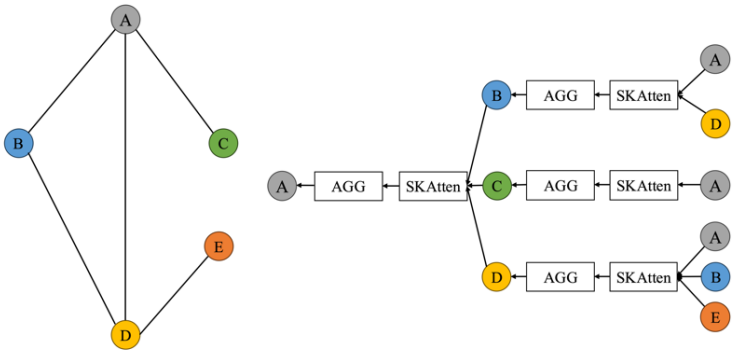

图1 节点聚合过程

其中$\mathrm{h}^{\mathrm{k}}_{\mathcal{N}(v)}$表示第$k$层中节点$v$的邻域聚合嵌入，该嵌入是通过对节点$v$邻域中所有边的特征进行聚合后获得的；$\mathrm{AGG}_k$代表第$k$层的聚合函数，该函数负责对邻域内边的特征进行聚合操作，以生成第k层的嵌入；SKAtten代表选择性注意力机制（Selective Kernel Attention），用于对边特征进行自适应处理，提升聚合过程的有效性；e^{k-1}_{uv}是第$k-1$层中连接节点u和节点v的边uv的特征，该特征在第k层的聚合计

算中被使用。最终的节点嵌入表示为$z_v = h_v^K$。随后，通过门控融合的方式将节点u和节点的节点v嵌入来获取每条边uv的边嵌入z_{uv}^K，如下所示：

$$z_{uv}^K = \text{GatedFusion}\left(z_u^K, z_v^K\right), uv \in \mathcal{E}。$$

2.1.3 SK-EGraphSAGE模型训练

本研究在实现中采用了包含两个SK-EGraphSAGE层的神经网络模型，这意味着邻域信息通过从两跳邻域中聚合而得。聚合函数选择了均值函数，即对采样邻域中的边特征进行逐元素求均值，以完成聚合操作。边缘嵌入的输出通过Kolmogorov-Arnold网络（KAN）进行处理，从而使算法的输出能够与NIDS数据集提供的标签进行对比，而非通过传统的多层感知机（MLP）。相比于MLP，KAN网络在逼近复杂函数方面具有更高的效率和理论保证，从而提升了模型的表达能力和分类精度。KAN网络的这种非线性组合函数的灵活性，尤其在处理高维度和非线性边嵌入时，展现出更强的适应性，从而显著增强了整体模型的性能。

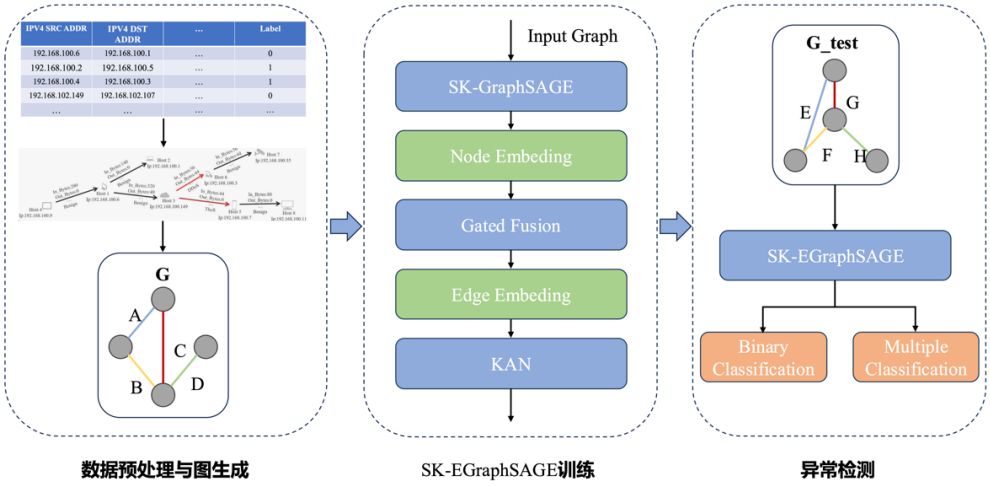

图2 SK-EGraphSAGE架构图

2.1.4 边分类

在训练过程中调整模型参数后，模型就可以通过对未见过的测试样本进行分类来进行评估。测试流记录也被转换为图形，通过训练的E-GraphSAGE层，从中计算边缘嵌入。然后将它们转换为最终softmax层中的类概率，并最终与真实的类标签进行比较，以计算分类评估性能指标。

表1 SK-EGraphSAGE二分类实验数据

数据集指标	NF-BoT-IoT			NF-ToN-IoT		
	P	R	F1	P	R	F1
E-GraphSAGE	96.92	97.57	97.15	97.19	97.12	97.03
Ours	98.09	98.15	98.12	99.02	99.01	99.00

2.1.5 公开数据集实验

本课题使用了公开的数据集NF-BoT-IoT和NF-ToN-IoT来测试SK-EGraphSAGE模型的性能。这两个数据集广泛用于网络流量分析和入侵检测研究，提供了丰富的网络流数据，包括正常流量和恶意流量的标签信息。通过实验，我们评估了SK-EGraphSAGE模型在这两个数据集上的分类精度、召回率和F1分数，进一步验证了模型在处理高维度、非线性网络流数据时的有效性和适应性。实验结果将展示SK-EGraphSAGE在公开数据集上的优越性能，并证明其在网络入侵检测任务中的潜在应用价值。

表2 SK-EGraphSAGE多分类实验数据

数据集指标	NF-BoT-IoT			NF-ToN-IoT		
	P	R	F1	P	R	F1
E-GraphSAGE	96.02	77.43	80.62	69.88	56.37	59.14
Ours	86.78	82.36	83.97	71.77	58.92	62.30

2.2 基于多尺度跨序列相关性分析的边缘计算节点负载异常检测

2.2.1 嵌入输入与集成残差连接

对输入的时间序列进行嵌入，以得到一个统一的输入表示。这一过程通过一维卷积层来实现，然后将嵌入后的特征与位置嵌入和时间嵌入相加，得到最终的输入嵌入表示：

$$\boldsymbol{X}_{emb} = \alpha \mathrm{Conv1}D\left(\widehat{\boldsymbol{X}}_{t-L:t}\right) + \boldsymbol{PE} + \sum_{p=1}^{P} \boldsymbol{SE}_p,$$

其中，α是用于平衡卷积层输出与其他嵌入的权重，**PE**是位置嵌入，$\mathbf{SE}_p$是可学习的时间戳嵌入。本课题的模型ADMSConvNet的实现采用了残差方法。开始我们设定$\mathbf{X}_0 = \mathbf{X}_{emb}$，其中 $\mathbf{X}_{emb}$ 表示通过嵌入矩阵将原始输入数据转换为丰富特征后的表示。

$$X_l = \mathrm{ADMSConvBlock}(X_{l-1}) + X_{l-1},$$

其中，ADMSConvBlock 表示 ADMSConvNet 层的主要功能所必需的操作和计算。

2.2.2 尺度分析

本课题旨在通过利用不同时间尺度下的时间序列相关性来提高异常检测的准确性。选择合适的时间尺度是该方法的关键因素之一。我们认为周期性作为一种重要的时间尺度，具有特别的价值。周期性在时间序列数据中起着基础性作用，它捕捉数据中的重复模式，为异常检测提供关键信息。例如，在夏季和冬季的高峰期，电力需求与温度通常呈现强正相关性，而在春秋两季的温和时期，这种相关性会减弱。时间尺度的选择会影响相关性的测量结果。采用日周期或月周期进行分析可能会得出不同的相关系数。模型使用快速傅里叶变换（FFT）来识别输入时间序列的显著周期性模式，以此作为时间尺度的依据。FFT的振幅值被平均并选择前k 个最高的振幅值对应的频率，以此来定义时间尺：

$$F = \mathrm{Avg}\left(\mathrm{Amp}(\mathrm{FFT}(\mathrm{X_{emb}}))\right), f_1,\cdots,f_k = \arg\ \mathrm{Topk}(F), s_i = \left[\frac{\mathrm{T}}{f_i}\right], i \in 1,\cdots,k..,$$

其中，F是经过FFT变换后得到的振幅向量，$f_1,\cdots,f_k$是选择的个最显著的频率，s_i是对应的时间尺度。

2.2.3 双分支多尺度卷积

本课题提出了一种具有双分支的多尺度卷积方法，用于收集详细和广泛的序列间及序列内依赖关系。第一分支采用了Inception模块，通过不同大小的卷积核捕捉多尺度特征，能够有效地提取序列内和序列间的属性。第二个分支采用了Mixhop图卷积方法，更有效地捕捉复杂的序列间关系。Inception模块侧重于局部和全局的时空特征，而Mixhop图卷积通过自适应邻接矩阵来提取各时间序列之间的动态连接。通过整合两个分支的输出，我们的方法结合了Inception和Mixhop图卷积的优势，确保了从时间序列数据中进行稳健且全面的特征提取。

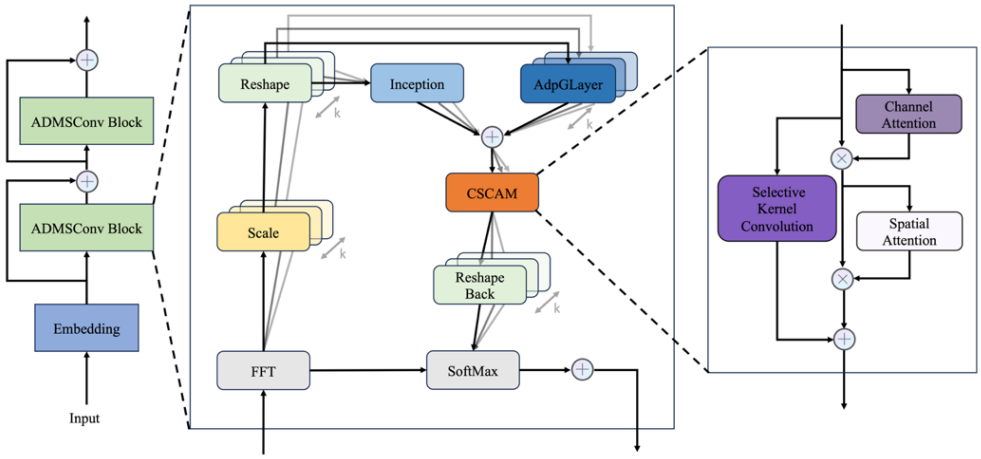

图3 ADMSConvNet架构图

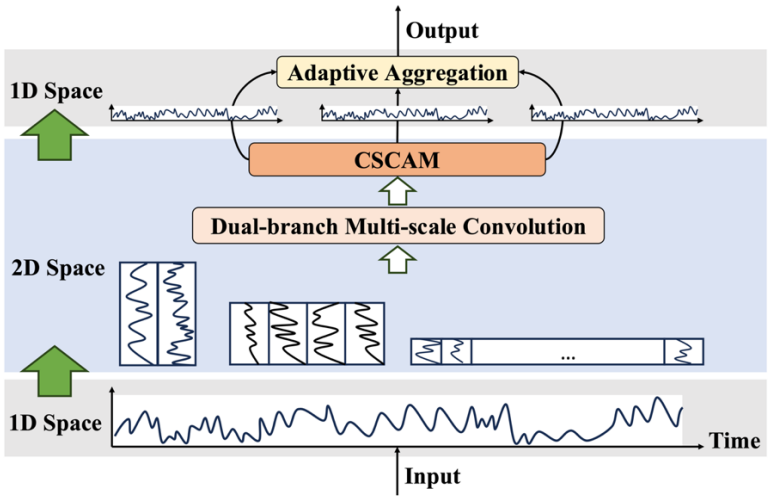

图4 ADMSConvBlock流程图

2.2.4 选择性核注意力和卷积块注意力并行机制

在计算机视觉领域，已经开发了多种先进方法来增强神经网络中的特征表示。在这些方法中，注意力机制展现了显著的效果。借鉴这些进展，我们设计了CSCAM模块，它并行集成了两个组件，以增强神经网络的特征表示。第一个组件是一个顺序的通道和空间注意力模块。第二个组件是自适应卷积注意力机制。该机制动态选择不同大小的卷积核，以调整感受野的范围。通过整合这两种注意力机制，该模块实现了动态且全面的特征表示。自适应卷积注意力机制根据输入特征动态调整其感受野，使网络能够灵活地捕捉多尺度信息。同时，顺序通道和空间注意力模块沿通道和空间轴依次计算注意力矩阵，并将这些注意力矩阵与输入特征矩阵相结合进行响应式增强，全面捕捉关键信息，逐步突出有意义的特征。结合这些注意力机制，使网络能够高效地捕捉并强调关键特征，通过利用有效的多尺度和精细特征表示，提升模型性能，进而实现更为稳健和精确的模型。

2.2.5 多尺度聚合与异常检测

在进入下一层时，整合 k 个不同尺度的张量是至关重要的。每个张量首先被重新调整为二维矩阵的形式。接着，我们根据各个尺度的幅度对这些尺度进行组合。具体来说，通过快速傅里叶变换获取的各尺度对应的幅度值，使用SoftMax函数来计算这些幅度，以便根据各自的特定幅度来集中处理来自不同尺度的数据。这种“专家混合”（MoE）策略确保了多尺度特征能够有效整合到后续层中。为了有效地检测异常，本课题的模型在时间和属性维度上应用了线性投影，将二维矩阵转换为适合后续处理的形式。为了识别时间数据中的异常，利用重构误差来获取异常评分。通过将模型的输出重构回原始输入并测量其差异，从而有效地识别异常点。

2.2.6 公开数据集实验

本课题将模型的精确率（Precision）、召回率（Recall）和F1得分与15种基线方法在两个数据集上的表现进行了对比。各数据集的具体结果如下所示：

SMD数据集：在SMD数据集上，我们的模型在异常检测中表现出色，精确率达到了88.16%，仅略低于Anomaly Transformer的88.91%。更为重要的是，我们的模型召回率为84.40%，相比Anomaly Transformer（82.23%）提升了2.17%，相比TimesNet（82.63%）提升了1.77%。这一显著的召回率提升表明了我们模型在有效识别真正正例方面的增强能力。此外，我们模型的F1得分为86.24%，超过了Anomaly Transformer的85.49%（提高0.75%）和TimesNet的85.12%（提高1.12%）。这些结果显示了我们模型在精确率和召回率之间取得了显著的平衡，性能优于其他模型。

PSM数据集：在PSM数据集上，我们的模型在检测异常方面表现出色，精确率达到了98.63%，在基线模型中名列前茅。虽然精确率比FEDformer的99.31%低0.68%，但我们的模型召回率为92.93%，显著高于许多其他模型。例如，超越了DLinear的召回率89.26%（提升了3.67%）和TimesNet的召回率92.21%（提升了0.72%）。我们的模型取得了95.70%的F1得分，显著超过了其他基线模型，例如Anomaly Transformer的79.40%（提升了16.30%）和TimesNet的95.21%（提升了0.49%）。尽管精确率略低于FEDformer，但总体上的平衡性和较高的召回率突显了我们模型在异常检测中的稳健性和高效性。

表3 ADMSConvNet对比实验数据

数据集指标	SMD			PSM		
	P	R	F1	P	R	F1
LSTM	78.52	65.47	71.41	69.24	99.53	81.67
Transformer	83.58	76.13	79.57	62.75	96.56	76.07
LogTrans	83.46	70.13	76.21	63.06	98.00	76.74
TCN	84.06	79.07	81.49	54.59	99.77	70.57
Reformer	82.58	69.24	75.32	59.93	95.38	73.61
Informer	86.60	77.23	81.65	64.27	96.33	77.10
AnomalyTrans	88.91	82.23	85.49	68.35	94.72	79.40

Pyraformer	85.61	80.61	83.04	71.67	96.02	82.08
Autoformer	88.06	82.35	85.11	96.75	77.97	86.35
DLinear	83.62	71.52	77.10	98.28	89.26	93.55
ETSformer	87.44	79.23	83.51	99.31	85.28	91.76
LightTS	87.10	78.42	82.53	38.37	95.97	91.85
FEDformer	87.95	82.39	85.08	99.31	82.42	90.08
TimesNet	87.76	82.63	85.12	98.22	92.21	95.21
iTransformer	87.33	77.77	82.28	98.07	93.14	95.54
Ours	88.16	84.40	86.24	98.63	92.93	95.70

2.3 智能化可视化入侵检测系统的构建

本课题已在入侵检测可视化系统的开发中，完成了登录模块、首页大屏、网络入侵检测和节点负载检测等核心页面的前端设计与实现。这些页面的开发基于现代前端框架Vue.js，确保了系统在用户交互过程中的高响应性和动态数据展示能力。系统通过清晰且用户友好的界面设计，实现了高效的交互操作，用户可以根据实际需求自由配置和调整监控视角，实时跟踪和分析网络安全状态。这种高度定制化的监控视角使安全团队能够灵活地聚焦于网络流量的关键部分，提升了异常事件的发现和处理效率。

图5 入侵检测平台登录页

首页大屏模块提供了全面的网络状态概览，能够实时展示关键的网络性能指标、入侵事件的分布情况、以及历史数据的可视化对比。通过对网络流量、攻击类型和节点负载的综合分析，系统可以为安全管理人员提供全面的安全态势感知，从而快速识别潜在的安全风险。

网络入侵检测模块深入分析网络中的入侵行为，能够识别多种类型的攻击事件，如DDoS攻击、SQL注入、中间人攻击、XSS攻击等。系统通过实时采集网络流量并对其进行分类，可以快速检测出网络中的异常流量，并生成直观的可视化图表。不同类型的攻击事件通过颜色编码和数据图形直观展

示，使用户能够一目了然地掌握当前网络的安全状态。

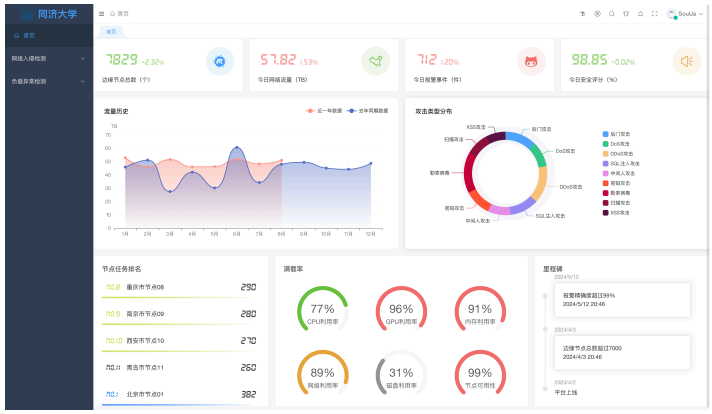

图7 入侵检测平台首页

节点负载检测模块专注于对边缘计算节点的资源使用情况进行监控。该模块能够实时显示各个节点的CPU、GPU、内存、网络和磁盘的利用率，并结合历史数据分析，帮助用户识别可能导致系统负载过高的风险点。对于负载异常的节点，系统将自动生成警报，并提供详细的资源使用分析报告，支持用户快速定位问题所在。

所有前端模块与后端服务无缝对接，后端通过Django框架和MySQL数据库实现高效的数据存储与管理，确保了大规模数据处理的稳定性和响应速度。系统中的实时数据通过优化后的接口进行传输和处理，保证了数据的持续更新和快速响应。此外，系统的告警功能能够及时通知管理员，处理潜在的网络入侵行为与节点负载异常，进一步增强了系统的安全防护能力。

图8 边缘节点网络监测页

图9 边缘节点负载监测页

系统的开发不仅着眼于功能实现，还特别注重用户体验优化和安全事件的高效可视化展现。通过引入ECharts.js等图形库，系统能够生成高度自定义的图表，支持多种数据类型的可视化，包括折线图、饼图、柱状图等，为用户提供多样化的数据分析工具。用户可以通过可视化仪表盘实时查看网络行为、负载情况和告警事件，极大提高了安全团队的工作效率和决策能力。

2.4 下一阶段工作计划

虽然本研究已在NF-BoT-IoT和NF-ToN-IoT数据集上初步验证了SK-EGraphSAGE模型的性能，但为了更全面、严谨地评估模型的适应性和泛化能力，后续工作将扩展至更多公开数据集。这些数据集将涵盖多种类型的网络流量和入侵模式，确保模型在不同场景中的鲁棒性和稳定性得到充分验证。此外，我们计划引入更丰富的对比实验，以更准确地评估SK-EGraphSAGE相较于其他主流模型的性能优势。这些对比实验将包括经典的GNN模型、其他边分类方法以及不同的入侵检测系统，以探讨SK-EGraphSAGE在分类精度、召回率和F1分数等关键指标上的相对表现。通过与不同模型的对比，我们将深入分析SK-EGraphSAGE在处理高维度、非线性网络流数据时的优势与不足。同时，消融实验也是后续工作中的重点。我们将逐步剔除模型中的各个关键组件，如SKAttention机制、FFT尺度学习层和KAN网络，评估其各自对整体模型性能的独立贡献。通过这些消融实验，可以更加清晰地了解各个模块在提升模型表达能力、特征提取和分类准确度方面的具体作用，从而为模型的进一步优化提供科学依据。

尽管本课题在入侵检测可视化系统的前端开发中已经取得了显著进展，但后续工作仍需进一步完善系统的功能与性能优化。首先，数据采集部分将是后续开发的重点，我们计划构建一个高效、稳定的数据采集模块，以确保系统能够实时、准确地收集和更新网络流量及节点负载数据。该模块将支持多种数据源的接入，以满足复杂网络环境下的多维度监控需求。此外，各种后端API接口的实现也是下一步的关键任务之一。通过开发一系列功能完善的API接口，我们将进一步增强前后端的通信效率，确保前端能够及时获取到后端处理的最新数据，支持系统的实时分析与动态展示。同时，API接口的扩展还将支持多样化的功能，包括安全告警的触发、日志记录、以及历史数据的查询与分析。最后，系统的告警事务处理将被进一步优化，旨在提高系统的自动化处理能力。当检测到潜在的入侵行为或异常负载时，系统将能够通过完善的告警处理机制，快速响应并采取相应的应对措施。该机制不仅将实现告警的实时推送，还将支持安全事件的分类与优先级管理，确保安全团队能够快速做出决策，提升整体安全响应的效率。

3、学术素养（包括专业理解能力、专业批评能力、知识运用能力、问题分析能力、参加国际交流和会议、在学期间取得成果等）

在过去两年的研究生学习生涯中，我的学术素养得到了显著提升。在程斌老师的悉心指导下，通过对课题方向的深入研究，我逐渐掌握了扎实的专业知识和技术技能，为我在学术道路上的进一步发展奠定了坚实的基础。

首先，在专业理解能力方面，我专注于选修如计算机网络安全、软件工程、机器学习理论与应用等核心课程。这些课程不仅为我提供了扎实的理论基础，也使我掌握了领域内最新的研究工具和方法。通过系统的学习，我能够深刻理解这些课程中的关键概念，并能够将其与我的研究方向相结合。每一门课程都帮助我更好地理解复杂的技术原理，并培养了我独立解决问题的能力。在学术研究的过程中，我不仅仅停留在课堂学习的层面，而是将理论知识延展至实际应用中。我结合所学内容，主动系统地研读了大量相关文献，涉及领域包括异常检测中的经典算法、入侵检测技术的最新进展以及时间序列分析的前沿研究。这些文献的阅读不仅开阔了我的视野，也帮助我掌握了该领域内的核心研究方法和当前的技术趋势。在此基础上，我积极参与了多项与课题相关的实验和项目，实践中遇到的问题促使我进一步巩固和加深了对理论知识的理解。通过这些努力，我逐渐形成了全面的专业理解能力，能够从理论到实践再到创新的全过程中，提出具有前瞻性和实际应用价值的研究成果。这不仅为我当前的课题研究奠定了坚实的基础，也为我未来在学术领域的持续发展提供了有力的支持。

在专业批评能力方面，我始终坚持培养和运用批判性思维，积极参与学术讨论和团队合作，并在此过程中不断提升自己的学术鉴别力。在研究生阶段，我深刻认识到，批判性思维不仅是学术研究的重要工具，更是推动个人和集体进步的关键力量。在参与的学术讨论中，我不仅仅停留于理论知识的积累，而是更加注重将所学知识与实际应用相结合。我会主动发起或参与讨论，针对课题研究中的难点和前沿问题，提出自己的见解和分析。在这些讨论中，我力求从不同角度深入剖析问题，通过与导师和同学们的互动，不断完善自己的思考路径。批判性思维不仅是学术研究的关键能力之一，更是促进自我提升的重要力量。通过不断挑战已有的理论和观点，我能够更加清晰地识别研究中的不足和改进空间。同时，批判性思维也促使我保持谦逊和开放的态度，接受他人的建议和批评，进而在学术道路上不断进步。

在知识运用能力方面，我始终强调将所学的理论知识灵活应用于实际研究中，力求通过理论与实践的紧密结合来解决课题中的实际问题。在研究生阶段，我深刻认识到，理论知识只有在实践中得到有效应用，才能真正转化为具有实用价值的研究成果。因此，我在每一个研究环节中，都尽力将理论与实践相结合，推动课题研究向更高层次发展。在研究过程中，我注重从多角度、多层次思考问题，以确保提出的解决方案不仅具备科学性，还具有较强的实际可行性。每当面对复杂的研究问题时，我会首先从理论层面进行全面分析，明确相关的理论依据和研究框架。在此基础上，我结合实际情况，设计了多个实验以验证研究假设。通过实验设计，我能够将抽象的理论具体化，检验其在实际应用中的有效性。例如，在某一项实验中，我通过调整实验参数和条件，逐步验证了不同变量对结果的影响，从而找到了最优的实验方案。这种方法不仅提高了研究的精确度，也增强了研究成果的科学性和可信度。

在学术成果方面，我在研究生期间以第一作者身份撰写了一篇具有一定学术价值的小论文，并已将其投稿至IEEE Transactions on Neural Networks and Learning Systems期刊。撰写论文的过程中，我经历了从选题、文献调研、实验设计到数据分析和结果讨论的完整研究流程。这一过程让我更加深入地理解了如何将学术研究与实际应用相结合。在确定研究课题时，我充分考虑了课题的创新性和实际应用价值，选择了一个在技术前沿具有挑战性和现实意义的研究方向。为确保论文的科学性和严谨性，

我在广泛阅读相关领域文献的基础上，提出了自己的研究假设和方法。通过精心设计实验并进行数据收集与分析，我验证了提出的方法，并将研究成果转化为可应用的技术方案。此外，通过与导师和同行的讨论和反馈，我对学术写作的规范和要求有了更为深刻的理解。这不仅帮助我提高了论文的质量，也让我在学术交流中更加自信和从容。通过在以上方面能力的提升，不仅让我在研究能力和学术表达上取得了长足进步，也让我更加坚定了将学术研究与实际应用紧密结合的信念。我深知，学术研究的最终目标是推动技术创新和社会进步。因此，在未来的研究工作中，我将继续秉持这一理念，努力将更多的研究成果转化为具有实际应用价值的技术方案，为学术界和产业界的发展贡献自己的力量。