基于双重图神经网络的计算机网络入侵检测方法探讨

孙浩源　赵　奇*
河北石油职业技术大学　河北承德　067000

摘　要：随着计算机网络应用的普及，计算机安全技术也在不断发展。其中，网络入侵检测技术是目前应对网络安全问题的有效技术措施，在网络安全检测中应用比较普遍。而传统计算机网络入侵检测过度依赖手动操作，所以无法应对全部的入侵行为，对此，提出基于双重图神经网络的计算机网络入侵检测方案，借助网络结构对于传统时序数据进行高效处理。能够在双重图神经网络检测中，不断对特征进行更新，有效检测网络入侵行为。这种检测方法的准确性和全面性更高，对于提升计算机网络安全管理水平具有重要应用价值。

关键词：双重图神经网络；计算机；网络入侵检测；网络安全

前言

在计算机网络的应用发展过程中，网络安全威胁问题成为企业和个人用网中都高度关注的问题。通过计算机网络入侵检测，能够及时发现计算机网络中的潜在威胁和攻击，及时采取措施来应对，减少因为入侵导致的信息安全和经济损失。而双重图神经网络作为一种创新方案横空出世。它融合了传统图神经网络的强项与注意力机制的精髓，既能全面把握网络的全局结构特性，又能细致入微地关注节点间的局部联系。这种双重优势使得双重图神经网络在处理复杂网络数据时展现出更强的鲁棒性和出色的泛化能力。因此，本文提出了一种基于双重图神经网络的全新计算机网络入侵检测方案，力求实现对入侵行为的精准识别，并有效发掘潜在的网络安全隐患。

一、双重图神经网络在计算机网络入侵检测中的应用原理和优势

（一）原理

双重图神经网络通过结合传统图神经网络（GNN）的全局结构捕捉能力和注意力机制的局部关系聚焦能力，实现了对网络数据的全方位解析。GNN擅长于利用节点特征和边关系来构建网络的全局视图，而注意力机制则能够强化关键节点和边的信息，使模型更加关注于那些可能对入侵检测有重要影响的局部区域。再者，计算机网络往往具有复杂的拓扑结构和节点间关系，这使得传统的入侵检测方法难以全面捕捉所有潜在的威胁。双重图神经网络通过其强大的图处理能力，能够有效地分析这些复杂结构，识别出异常的节点行为或流量模式，从而提高检测的准确性和效率[1]。图1（计算机网络入侵检测系统）

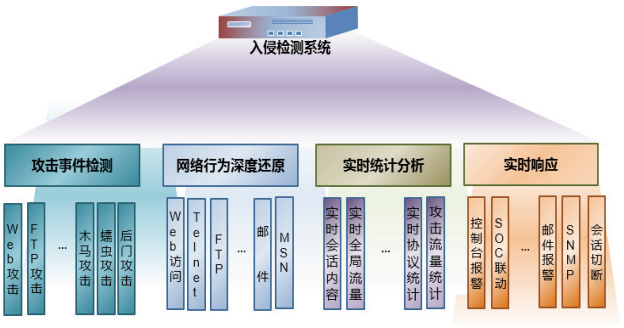

图1　计算机网络入侵检测系统

可见，随着网络环境和攻击手段的不断变化，入侵检测系统需要具备动态学习和更新的能力。双重图神经网络通过其自学习和优化机制，能够不断从新的网络数据中学习新的特征模式，并更新其内部模型参数，以适应不断变化的网络环境。

（二）应用优势

就双重图神经网络在计算机网络入侵检测中的应用优势来看，主要表现在以下几方面：

第一，更高的检测准确性。由于双重图神经网络能够同时考虑网络的全局结构和局部关系，因此能够更准

第一作者简介：孙浩源（1994.06-），男，汉族，河北承德人，研究生学历，助教，专业：计算机系统结构。
通讯作者：赵奇*（1992.01-），男，汉族，河北承德县人，研究生学历，助教，专业：计算机技术。

确地识别出潜在的入侵行为。与传统的特征匹配方法相比，DGNN在复杂网络环境下的检测性能显著提升。

第二，更强的鲁棒性[2]。面对网络中的噪声和异常数据，双重图神经网络通过其强大的图处理能力和注意力机制，能够有效地过滤掉这些干扰因素，保持检测结果的稳定性和可靠性。

第三，更好地泛化能力。由于DGNN具备动态学习和更新的能力，因此能够适应不同网络环境和攻击手段的变化。这使得DGNN在应用于不同的计算机网络时具有更好的泛化能力，无需针对每个特定网络进行大量的定制化调整。

第四，实时性保障。在计算机网络入侵检测中，实时性是一个至关重要的指标。双重图神经网络通过其高效的计算和优化算法，能够在保证检测准确性的同时实现快速的响应和报警，为网络安全提供及时有效的保障。

二、网络入侵检测结构设计

在探索构建高效智能的计算机网络入侵检测体系时，设计了一种创新的网络入侵检测结构，此结构致力于精确识别并即时响应网络中的潜在威胁。该结构的核心在于引入了一个灵活且自适应的多层感知网络（Multi-Layer Perceptron，MLP），它不仅能显著提升检测的准确性，还具备强大的学习能力，以有效应对网络攻击的不断演变。

此网络入侵检测结构的设计亮点在于其多层次感知器的配置。具体来说，构建了一个包含输入层、两个隐藏层以及输出层的深度神经网络架构。输入层作为数据处理的起点，负责接收并初步处理从网络中捕获的多样化数据，这些数据覆盖了网络流量、日志信息等多个方面，共计41个特征输入，确保了信息的全面性和精确性[3]。

随后，数据进入第一个隐藏层，该层配置了256个神经元。这一设计的目的在于通过复杂的非线性变换，深入挖掘数据中的隐含模式和特征，为后续的入侵行为识别提供有力支持。紧接着，数据流经第二个隐藏层，其中包含128个神经元，进一步对特征进行提炼与优化[4]。通过采用逆向完全连通的方式，即增加隐藏层神经元的数量，加强了网络各层之间的信息交互与整合能力，从而提升了模型的整体性能。

尤为值得一提的是，两个隐藏层之间实施了一种自适应过滤机制。这一机制能够自动筛选并剔除无关或冗余的信息，仅保留对入侵检测至关重要的特征。这种机制不仅显著提高了检测效率，还大大降低了误报和漏报的风险，确保了检测的准确性和可靠性。

此外，该网络入侵检测结构还注重节点数量的合理配置。在输入层设有41个神经元，第一个隐藏层设有256个神经元，第二个隐藏层设有128个神经元。这样的节点数量配置不仅保证了网络的性能，还提高了检测系统的效率。通过优化节点数量和隐藏层设计，该结构实现了对网络攻击的高效识别与防御，同时赋予了检测系统强大的自适应性和学习能力。

可见，这种创新的网络入侵检测结构通过精心规划的节点数量与隐藏层布局，能够有效实现对网络攻击的精确识别与有效防御，该检测结构还具备强大的自适应性和学习能力。这一方案不仅能够应对当前已知的网络威胁，还能对未来可能出现的未知攻击行为进行实时监测与预警，为计算机网络的安全稳定运行提供有力保障[5]。

三、基于双重图神经网络的计算机网络入侵检测方法

（一）利用双重图神经网络提取入侵特征

在图模型的网络入侵检测场景中，传统分类与聚类方法显现出其在精准识别入侵行为上的不足，且普通神经网络在处理图结构数据时亦显得力不从心。针对这一挑战，本文创新性地提出一种基于双重图神经网络的入侵特征提取策略。该策略旨在通过深入挖掘通信数据包中的信息，对由数据包划分出的子图进行点属性和边属性的全面特征提取，并将这两类特征融合，以精确捕捉子图的属性和结构特点，进而实现对网络入侵行为的高效识别。

此策略的实施包含两个核心步骤：预处理与特征提取。预处理步骤是整个流程的先决条件，它负责对原始样本集进行系统的处理。借助开源的CICFlowmeter工具，从海量的流量包中提取出关键特征，为后续的样本处理奠定基础。在样本处理过程中，开展数据筛选、数值转换以及归一化等关键操作，以确保数据的准确性和可靠性。在子图划分阶段，对样本集进行图模型构建，根据节点特征和属性特征，生成全图的邻接矩阵，并依据科学的子图划分原则，将大图拆解为多个子图，从而形成子图数据集。

在特征提取环节，引入图卷积神经网络这一先进技术。图卷积神经网络是卷积神经网络在图数据领域的拓展，它摒弃了传统卷积神经网络中固定大小的卷积核，而是采用权重共享机制，对同一子集内的节点应用相同

的卷积核进行处理。在模型中，采用双重图卷积神经网络架构，分别针对子图的点集和边集进行特征提取。通过对提取出的节点特征和边特征进行线性变换，并将这两类特征进行巧妙的融合，得到能够全面反映图属性和结构特征的完备特征向量[6]。

（二）更新特征检测计算机网络入侵

在构建模型的过程中，首先着眼于时间序列中的时序关系，为此设计了第一重图。在这一层中，我们选择了一维卷积神经网络（CNN）作为核心工具。CNN以其出色的一维数据处理能力，特别是通过卷积操作提取时间上的局部特征，而广受青睐。这种设计能够让模型能够捕捉到数据随时间变化的细微规律，为后续的入侵检测提供了坚实的时序基础。紧接着，为了更深入地揭示时间序列中特征之间的复杂关系，构建第二重图。与第一重图不同，这里采用图卷积神经网络（GCN）。GCN在处理图结构数据时具有显著优势，能够捕捉到节点之间的非线性关系。通过GCN，深入挖掘特征之间的内在联系，为入侵检测提供更加全面、深入的特征信息。

在构建了双重图结构之后，利用双重图神经网络对这两个图进行联合训练。这种训练方式使得网络能够同时学习到时间序列中的时序和特征关系，为后续的入侵检测任务打下了坚实的基础。在训练过程中，网络通过反向传播算法不断优化参数，以最小化预测结果与真实值之间的误差。这种优化过程能够有效提高模型的准确性，增强其对未知攻击的识别能力。

当模型训练完成后，将其应用于实际的时间序列数据中，进行入侵检测。网络通过分析数据中的异常模式，能够准确地检测出潜在的入侵行为。这种基于时间序列建模的入侵检测方法，提高检测的准确性，降低误报率和漏报率。

四、实验结果分析

为验证提出的基于双重图神经网络的入侵检测法，本文与基于规则及统计学的检测方法进行了对比实验。在模拟平台上，随机选取一周的网络数据，共采集1000组样本，通过三种方法对入侵行为进行实时监测，并记录结果。实验前，对原始数据预处理，包括去除异常值、缺失值处理及特征标准化。设置异常值和缺失值阈值以确保数据质量。实验结果显示，如表1所示：

表1　不同检测方法结果对比

组别	双重图神经网络法	规则检测法	统计学检测法
实验1 F1值	0.938	0.782	0.727
实验2 F1值	0.955	0.776	0.708
实验3 F1值	0.949	0.790	0.735
实验4 F1值	0.927	0.783	0.790
实验5 F1值	0.981	0.785	0.719
实验6 F1值	0.931	0.731	0.729
平均F1值	0.947	0.777	0.734

可见，基于双重图神经网络的检测方法在六个实验组中F1分数均最高，平均F1分数也优于其他两种方法。因此，本文提出的方法在检测准确性上具有显著优势，能更有效地识别计算机网络入侵。

总结

基于双重图神经网络的计算机网络入侵检测方法应用对于提升检测的精准性具有重要应用价值，本文对于这种入侵检测方法进行了分析，就具体的操作流程进行探究，旨在为计算机网络安全检测技术的应用和发展提供一些参考。

参考文献

[1]王雪妍，温蜜，李晋国，熊赟.一种卷积神经网络结合特征融合的网络入侵检测方法[J].计算机应用与软件，2024，41（08）：359-366.

[2]张璐，胡静，王旭.基于大数据分析的网络入侵检测与防御技术研究[J].网络安全和信息化，2024，（08）：132-134.

[3]王玮琳.基于双重图神经网络的计算机网络入侵检测方法[J].现代工业经济和信息化，2024，14（07）：74-76.

[4]伍均玺，林峰，高红云.基于改进深度学习的主动式通信网络入侵行为自适应识别算法[J].微型电脑应用，2024，40（04）：9-12.