

基于 GCN 模型的 DDoS 攻击检测技术研究

姜舒颖¹ 黄迎春¹

JIANG Shuying HUANG Yingchun

摘要

如何高效检测出分布式拒绝服务（distributed denial of service, DDoS）攻击是目前互联网领域中存在的一个亟待解决的问题。在 DDoS 攻击检测领域，考虑到固有的复杂性，尤其是系统包含的网络节点间复杂的交互，为了捕捉和建模这些节点间的关系，提出了一种基于图注意力机制的图卷积神经网络（graph convolutional network, GCN）DDoS 攻击检测模型。通过图注意力机制，模型能够自适应地为不同节点之间的关系分配重要性权重，从而更准确地识别出潜在的 DDoS 攻击行为。将 DDoS 攻击视为一个图结构，网络节点表示网络设备或主机，边表示节点之间的连接关系，能够从节点和边的特征中提取有用的信息，利用节点的邻居信息来推断节点特征，更好地捕捉 DDoS 攻击的上下文信息。实验结果证明，所设计的模型的精度极其出色，不仅提高了检测的准确性，还有助于人们更深入地理解 DDoS 攻击在网络中的传播和演变规律。

关键词

分布式拒绝服务；图卷积神经网络；图注意力机制；网络节点；图结构的建模

doi: 10.3969/j.issn.1672-9528.2024.10.020

0 引言

分布式拒绝服务攻击是一种针对计算机系统或网络的攻击行为，利用客户/服务器架构，集结多计算机资源成攻击网络，对目标系统协同攻击，导致其资源耗尽、服务中断，从而增强攻击的威力^[1]。DDoS 颠覆了传统的点对点攻击方式，展现了一种无显著统计特征的攻击方式。此类攻击利用了广泛存在的协议和服务作为掩护，使得仅凭协议/服务的

类型来区分攻击行为与正常网络活动变得极具挑战性，导致分布式拒绝服务攻击不易检测^[2]。DDoS 攻击技术的持续升级，导致防御工作变得艰巨且有挑战性。那么如何提高 DDoS 攻击检测在实际网络中应用的准确率和精确度，则有非常重要的价值和意义^[3]。

GCN 算法是图卷积神经网络研究领域的一个热点，深入研究了使用图卷积网络^[4]进行 DDoS 攻击检测，主要专注于处理由节点和边组成的网络结构，即图数据。本文提出将融入了图注意力机制的 GCN 模型应用于 DDoS 攻击检测领域，

1. 沈阳理工大学信息科学与工程学院 辽宁沈阳 110159

[5] YANG Z, TANG K, YAO X. Large scale evolutionary optimization using cooperative coevolution[J]. Information sciences, 2008, 178(15):2985-2999.

[6] LI X, TANG K, OMIDVAR M N, et al. Benchmark functions for the CEC 2013 special session and competition on large-scale global optimization [J]. Gene, 2013, 7(33):1-23.

[7] HENLEY S. Principles and procedure of statistics: a biometrical approach[J]. Computers & geosciences, 1983, 9(2):275.

[8] CHENG R, JIN Y. A competitive swarm optimizer for large scale optimization[J]. IEEE transactions on cybernetics, 2015, 45(2): 191-204.

[9] CHENG R, JIN Y. A social learning particle swarm optimization algorithm for scalable optimization[J]. Information sciences, 2015, 291:43-60.

[10] FALCO I D, CIOPPA A D, TRUNFIO G A. Investigating surrogate-assisted cooperative coevolution for large-scale global optimization[J]. Information sciences, 2019, 482:1-26.

【作者简介】

付国霞（1995—），女，山西原平人，硕士，助教，研究方向：进化算法、智能计算。

（收稿日期：2024-07-08）

将 DDoS 攻击建模为图的形式，每个节点代表现实世界中的一个独立的 IP 地址，可以增强节点之间的信息传递和聚合过程，更加灵活地适应复杂的图结构，提高了模型的表达能力，并且减少了信息丢失。引入图注意力机制的 GCN 模型能够更好地捕捉图结构中的复杂关系，提高模型的性能和泛化能力，以及降低误报率，提高准确率。

1 数据预处理

本文以入侵检测公开数据集为分析源，CIC-IDS2017 数据集是由加拿大网络安全研究所于 2017 年发布^[5]，数据集包含一周网络流量，涵盖正常行为和多种攻击。实验选取 83 个特征（除 ID 和标签外），来自 8 个 CSV 文件的有效载荷数据。为了更有效地进行 DDoS 攻击检测，对收集到的数据集进行了深入的分析，基于分析结果，进行数据预处理，旨在优化数据质量，为后续的攻击检测工作奠定坚实的基础。

1.1 数据清洗

在数据预处理阶段，为了提高数据分析的准确性，降低错误率，本文首先对输入的数据文件进行合并，其次解决缺失值和异常值的问题，并剔除不必要的脏数据，包括第一行特征名称和含有 Nan、Infinity 等异常值的行，但遇到了样本数据极度不平衡的问题，直接影响了模型训练的效果。采用了 SMOTE（synthetic minority oversampling technique）采样方法对训练数据集进行预处理。这种策略有助于减轻因数据不平衡可能导致的过拟合问题，进而提升模型的整体性能和稳定性。

1.2 特征选择

特征选择的目标是从原始特征集合中选择出与学习任务最相关、对模型性能有贡献的特征子集，同时去除那些不相关、冗余或噪声特征，从而简化模型，提高模型的泛化能力，并减少计算复杂度。

采用 Pearson 相关系数进行数据分析，旨在判断两个数据集是否沿着同一线性趋势变动，从而衡量它们之间线性关系的紧密程度。Pearson 相关系数的公式为：

$$\gamma = \frac{\sum (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum (x_i - \bar{x})^2 \sum (y_i - \bar{y})^2}} \quad (1)$$

为了优化特征集，利用随机森林算法，将包含正常与攻击流量的 7 个 CSV 文件逐一引入模型框架中，并借助决策树技术快速评估各特征的重要性，实现特征的有效筛选与排序。基于特征选择的结果进行标准化，确保数据符合正态分布，旨在消除量纲差异，提升模型的稳定性和准确性，从而增强对训练特征重要性的鲁棒性，才能全面评估模型的性能。这

样就能够充分利用数据，保证检测的稳定性。经过 Lasso 线性回归算法的特征降维和交叉验证操作，RF 模型在每轮训练中都会对特征重要性进行评估。最后将数据集中的维度降低到最具信息量的特征，减少了数据集的复杂度和计算成本。

2 引入图注意力机制的 DDoS 攻击检测

DDoS 攻击颠覆了传统单点攻击，采用多点并发模式，无固定统计特征，且利用协议和服务作为掩护，使区分攻击与正常流量极具挑战性。随着 DDoS 攻击的数量激增、频率加快日益复杂以及造成的影响不断深化，正确辨识并区分出正常的流量与恶意的 DDoS 攻击流量成为网络安全领域的艰巨任务。

GCN 算法主要专注于处理由节点和边组成的网络结构，即图数据。将数据流元素映射为图节点，利用源 IP 与目的 IP 的关系来构成图数据的边，得到基于 IP 关联的无向图^[6]，如图 1 所示。

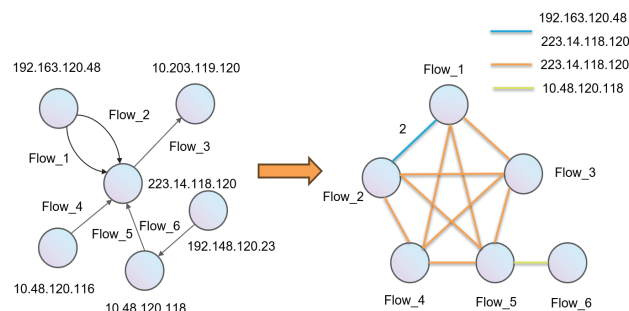


图 1 图数据转换规则

2.1 GCN 模型

针对 GCN 模型，节点信息的重要性常超过边，但都是图数据的关键组成部分。图卷积神经网络在 2017 年被提出，相较于传统神经网络，GCN 模型显著不同，它能够直接在图结构上进行高效计算，无需对图数据进行向量化，克服了传统方法在图结构数据处理上的缺陷。GCN 的核心运算精准表达公式为：

$$H^{(l+1)} = \sigma \left(D^{(-1/2)} A D^{(-1/2)} H^{(l)} W^{(l)} \right) \quad (2)$$

此公式详尽描述了 GCN 中一层的前向传播流程，不仅融合了图的结构信息，还集成了节点的固有特征。所有邻居节点特征的加权汇总生成节点的新特征，其权重由邻接矩阵与可学习的权重矩阵共同决定，并利用非线性激活函数进行加权和操作。整个过程可以看成是图上进行的一种卷积操作^[7]。该模型实际是由输入层、隐藏层（图卷积层，类似全连接层的作用）、SoftMax 以及输出层构成的。

2.2 图注意力机制

图注意力机制的原理就是对汇聚到中心节点的邻居节点

学习权重，使其能够按照权重进行邻域特征的加权和，应用了 SoftMax 进行归一化，计算注意力系数的公式为：

$$\alpha_{i,j} = \frac{\exp\left(\alpha \left(\alpha^T [W_{x_i} \parallel W_{x_j}] \right)\right)}{\sum_{k \in N(i), k \neq j} \exp\left(\alpha \left(\alpha^T [W_{x_i} \parallel W_{x_k}] \right)\right)} \quad (3)$$

根据计算好的注意力系数，将特征加权求和，其公式为：

$$h'_i = \sigma \left(\sum_{j \in N_i} \alpha_{ij} W h_j \right) \quad (4)$$

因为衡量相似度的方法不同，多用几个相似性度量方法，来进化增强一下，即运用多头注意力机制，其公式为：

$$h'_i(K) = \parallel \sigma \left(\sum_{j \in N_i} \alpha_{ij}^k W^k h_j \right) \quad (5)$$

本研究的实验结果表明，将图注意力机制融入 GCN 模型中，显著增强了模型在捕捉网络节点间复杂相互作用方面的精确度，同时赋予了模型更强的泛化潜能。这意味着，即便面对与训练集图结构不完全一致的新数据，该模型也能有效工作，无需严格匹配训练集的图结构。这一改进直接提升了模型的整体表现，从而提高了检测的准确性和可靠性。

3 实验与分析

3.1 实验数据集

本文所提出的框架，在 CIC-IDS2017 数据集上进行全面评估与验证，此数据集包含了 DDoS 攻击相关的数据包信息，包含每个数据包的源 IP 地址、目标 IP 地址、长度、协议类型，以及数据包到达的精准时间戳等。将总流量数据集分成 80% 和 20% 进行训练和测试。

3.2 实验过程

本文使用的软件环境参数为：Python 3.8.10，PyTorch 1.10.0。硬件环境为：Intel Core i7-9700 K，八核 16 GB 内存，512 GB NV Me SSD，操作系统为 Ubuntu 20.04 LTS。

(1) 在 GCN 模型设置中，由两个 GCNConv 图卷积层组成，第一个 GCNConv 层输出 16 维的特征；第二个 GCNConv 层从 16 维的特征接收输入，并输出特征。为了确保模型能够捕获数据中的复杂非线性关系，同时避免过度依赖特定的神经元组合导致的过拟合问题，本文在模型训练阶段采取了双重策略，引入 ReLU 激活函数，并实施 dropout 技术，设定丢弃率为 0.5；采用 Adam 优化算法来自适应地调整学习率。

(2) Attention-GCN 模型引入图注意力机制，由两个 GATConv 图卷积层组成，第一个 GATConv 层输出 768 维的特征；第二个 GATConv 图卷积层从 768 维的特征接收输入，并输出特征。本文在模型训练中采用的 ELU 激活函数和 dropout 技术，并使用 Adam 优化算法来调整学习率。

(3) 这两个模型在训练过程中均对 CIC-IDS2017 数据集进行前向传播得到输出，通过交叉熵进行损失计算并用于反向传播，两个模型的损失曲线如图 2 ~ 3 所示。将训练周期设置为 1000，其他超参数设定未进行特别调整，采用模型的默认值。

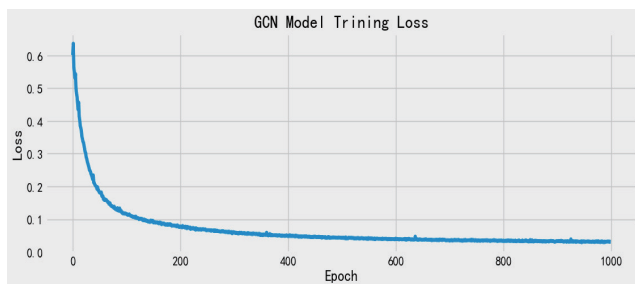


图 2 GCN 模型的损失曲线

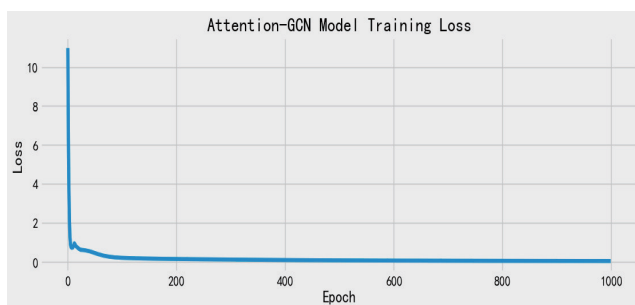


图 3 Attention-GCN 模型的损失曲线

3.3 评价标准

为了全面剖析模型性能，采用四个评价标准来验证模型性能。混淆矩阵 (confusion matrix) [8]：在二分类模型的评估中，包含四个关键指标的工具来全面衡量模型的性能：真正例 (true positive, TP)：本身为正例并被预测为正例的数目；负正例 (false positive, FP)：本身为负例但被预测为正例的数目；真负例 (true negative, TN)：本身为负例并被预测为负例的数目；负负例 (false negative, FN)：本身为正例但被预测为负例的数目。

准确率 (accuracy, A)：

$$A = \frac{TP + TN}{TP + TN + FP + FN} \quad (6)$$

召回率 (recall, R)：

$$R = \frac{TP}{TP + FN} \quad (7)$$

F_1 得分 (F_1 -score, F_1)：

$$F_1 = \frac{2 \times P \times R}{P + R} \quad (8)$$

3.4 检测结果

在对比先前研究的实验结果后，可以观察到，利用本文所提出的方法对 CIC-IDS2017 数据集进行测试，不仅提高了

检测的准确率、召回率，而且在 F_1 得分上也有显著提升。如表 1 所示^[9]，相较于前人提出的各种模型，本文的 Attention-GCN 模型的结果有提升，表明本文模型在类别判断方面有明显优势，检测结果较高。

表 1 不同模型之间的检测性能对比

方法	评价标准		
	$A/\%$	$R/\%$	$F_1/\%$
RF-SVM	85.6	86.4	86.0
RNN	95.52	95.51	95.52
SRNN	98.28	98.28	98.28
GCN	99.17	99.21	99.56
Attention-GCN	99.31	99.42	99.64

GCN 模型以及 Attention-GCN 模型的混淆矩阵如图 4、图 5 所示。

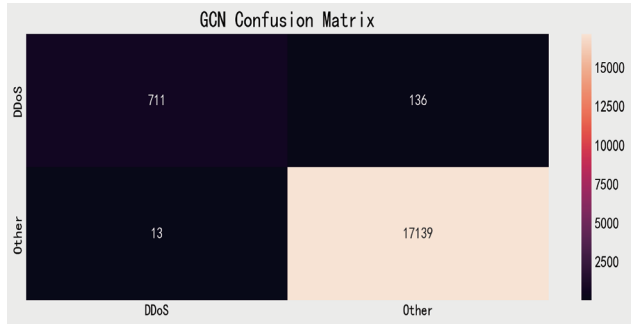


图 4 GCN 模型的混淆矩阵

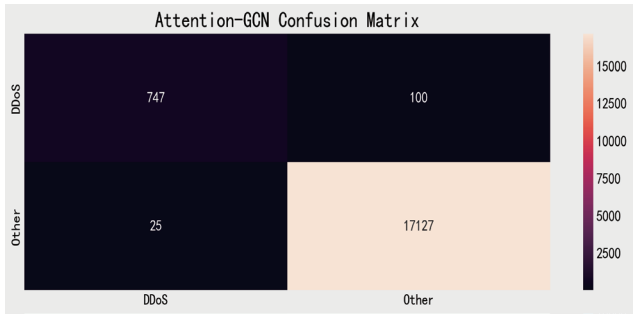


图 5 Attention-GCN 模型的混淆矩阵

4 结论

本文融合了图数据结构的固有特性与 GCN 的高效处理能力，并成功将其应用于 DDoS 攻击的检测领域。初始阶段，借助随机森林算法实施特征选择以及特征重要性评估；随后，融入图注意力机制，旨在实现检测效果的最大化。经过一系列调整与优化，此方法展现出了卓越的成效。实验数据表明，该方法在多个评估维度上均实现了显著提升，特别是在 DDoS 攻击的精准识别上表现较佳。这一突破性成果不仅验证了本文方法的高效性与实用性，更深刻地揭示了 GCN 在 DDoS 攻击检测领域的巨大潜力和在防御策略构建上的可行性与价值。

参考文献：

[1]ZARGAR S T, JOSHI J, TIPPER D. A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks[J].IEEE communications surveys & tutorials, 2013, 15(4):2046-2069.

[2]WANG B, ZHENG Y, LOU W, et al. DDoS attack protection in the era of cloud computing and software-defined networking[J]. Computer networks, 2015,81(4):308-319.

[3]FERRAG M A, SHU L, DJALLEL H, et al. Deep learning-based intrusion detection for distributed denial of service attack in Agriculture 4.0[J].Electronics,2021,10(11):1257.

[4]KIPF T N, WELING M.Semi-supervised classification with graph convolutional networks[EB/OL].(2016-09-09)[2024-03-24]. <https://arxiv.org/abs/1609.02907>.

[5]SHARAFALDIN I, LASHKARI A H, GHORBANI A A.To-ward generating a new intrusion detection dataset and intrusion traffic characterization[C]//4th International Conference on Information Systems Security and Privacy (ICISSP).[S.l.]: Science and Technology Publications, Lda, 2018:108-116.

[6]REN G, CHENG G, FU N. Accurate encrypted malicious traffic identification via traffic interaction pattern using graph convolutional network[J].Applied sciences, 2023, 13(3):1483.

[7]葛睿博,路新喜,董凌鹤.基于图卷积神经网络的网络安全全态势感知研究 [J]. 网络安全技术与应用, 2024(5): 35-38.

[8]戴俭,唐勇,张婷婷,等.基于 RF-SVM 的应用层 DDoS 攻击检测方法 [J]. 软件导刊,2023,22(3):62-67.

[9]邱志文.基于深度学习的 DDoS 攻击流量检测算法设计与实现研究 [D]. 武汉:长江大学,2023.

【作者简介】

姜舒颖（2000—），女，山东聊城人，硕士，研究方向：计算机应用技术。

黄迎春（1976—），通信作者（email: 1365153370@qq.com），男，辽宁瓦房店人，硕士，副教授，硕士生导师，研究方向：网络服务与信息安全。

（收稿日期：2024-07-08）