**文章编号**:1007-5321(2021)05-0094-07 **DOI**:10.13190/j.jbupt.2021-007

# 基于内外卷积网络的网络入侵检测

王艺霏[1], 莫 爽[2], 吴文睿[2], 范少华[2], 肖 丁[2]
(1. 国网冀北电力有限公司信息通信分公司, 北京 100054;
2. 北京邮电大学 计算机学院(国家示范性软件学院), 北京 100876)

**摘要**: 网络入侵检测通过分析流量特征来区分正常和异常的网络行为以实现入侵流量的检测,是网络安全领域的重要研究课题. 针对已有入侵检测模型特征提取过程复杂、信息提取不足等问题,提出了一种基于内外卷积网络的入侵检测模型. 首先使用一维卷积神经网络提取流量数据的内部特征,然后通过对内部特征计算相似度建模得到无向同质图,此外将流量在外部网络侧的通信行为建模为有向异质图,并对两图使用图卷积网络学习包含网络流量多种交互行为的嵌入向量,最后将学习到的流量嵌入向量输入到分类器中用于最终的分类. 实验结果表明,所提模型的检测准确率和误报率均优于对比模型.

**关 键 词**: 入侵检测; 深度学习; 图卷积网络; 卷积神经网络
**中图分类号**: TP393 **文献标志码**: A

# Internal-External Convolutional Networks for Network Intrusion Detection

WANG Yi-fei[1], MO Shuang[2], WU Wen-rui[2], FAN Shao-hua[2], XIAO Ding[2]
(1. State Grid Jibei Information and Telecommunication Company, Beijing 100054, China;
2. School of Computer Science (National Pilot Software Engineering School), Beijing University of Posts and Telecommunications, Beijing 100876, China)

**Abstract**: Network intrusion detection is an important research topic in the field of network security which is used to distinguish normal and abnormal network behaviors by analyzing traffic characteristics to realize intrusion traffic detection. To solve the problems of the complex feature extraction process, and insufficient information extraction in existing intrusion detection models, an intrusion detection model based on internal and external convolutional networks is proposed. Firstly, an one-dimensional convolutional neural network is used to extract the internal features of the traffic data. Then, an undirected homogeneous graph is obtained by calculating the similarity of the internal features. In addition the communication behavior of the traffic on the external network side is modeled as a directed heterogeneous graph, and graph convolutional network is used to learn embedding containing multiple interactive behaviors of network traffic from two graghs. Finally, the learned flow embedding is input into the classifier for final classification. Experimental results show that compared with existing methods, the detection accuracy and false alarm rate of the proposed model are better than those of the compared models.

**Key words**: intrusion detection; deep learning; graph convolutional network; convolutional neural network

**收稿日期**: 2021-07-07
**基金项目**: 基于全业务统一数据中心的数据融合及可视化关键技术研究项目(52018E18006N)
**作者简介**: 王艺霏(1988—), 女, 工程师.
**通信作者**: 肖 丁(1966—), 男, 讲师, dxiao@bupt.edu.cn.

近来网络空间安全问题受到人们越来越多的关注，网络安全保护指的是如何针对各种类型的网络攻击制定有效的防御措施来确保网络设备的安全和信息安全. 入侵检测模型通过分析网络流量中关键节点的特征来识别恶意攻击行为，是网络安全保护体系结构的重要组成部分.

入侵检测模型按照实现方式的不同可以分为基于签名的检测和基于异常的检测. 基于签名的检测模型首先分析已知的攻击，并提取它们的区别特征和签名，随后将提取到的签名和新的流量进行对比来实现入侵流量的检测. 这类模型对于已知的攻击具有高检测率和低误报率，但不能检测任何新型攻击. 基于异常的检测模型主要与机器学习的模型相结合，首先需要设计网络流量特征，然后对模型进行训练使其能够检测出入侵流量[1]. 相比于基于签名的检测模型，该模型的优势是可以检测出未知的攻击，因此吸引了越来越多学术界和工业界学者的关注[2]；然而，该模型因需要领域专家进行特征设计，导致模型的泛化性较差[3]，而且目前没有设计网络流量特征集的统一标准[4]. 其次，该模型误报率较高，这也限制了其在实际中的应用[5].

已有的入侵检测模型往往只考虑如何学习流量的内部特征，忽略了通信时在外部网络侧进行交互的信息，导致检测效果不佳. 为了解决该问题，提出了一种内外卷积网络（IECNet，internal-external convolutional network）的入侵检测模型，该模型首先使用一维卷积神经网络（1D-CNN，one-dimension convolutional network）提取流量数据的内部特征，然后将不同流量作为顶点构建一个无向同质图，将流量数据的网际互连协议（IP，internet protocol）地址和端口作为顶点构建一个有向异质图. 随后，使用不同的图卷积网络（GCN，graph convolutional network）学习包含网络流量的嵌入向量并输入到分类器中用于最终的分类. 实验结果表明，所提模型的检测准确率和误报率均优于对比模型.

# 1　相关研究

## 1.1　入侵检测技术

在入侵检测领域，最近出现了设计特征集进行入侵检测的模型. 例如，Ma 等[6]应用深度神经网络在 1999 年国际知识发现和数据挖掘竞赛数据集（KDD99，international knowledge discovery and data mining cup 1999 data）上进行入侵行为检测. Javaid 等[7]研究了使用深度置信网络进行入侵检测的研究. 但是这些模型使用的数据集是经过预先计算得到的流统计特征，特征集的选择无统一有效的标准.

## 1.2　深度学习技术

深度学习因为能够直接从原始数据中提取特征，近年来已逐渐用于网络流量分类任务中. Tan 等[8]将计算机视觉的技术用于拒绝服务（DoS，denial of service）攻击的检测并取得了一定的效果. Torres 等[9]首先将网络流量特征转换为字符序列，然后使用循环神经网络（RNN，recurrent neural network）学习其时间特征，并将其进一步应用于检测恶意软件流量. Zhang 等[10]提出了基于多尺度卷积神经网络和长短期记忆的入侵检测模型来学习网络流量数据的多个维度的特征，实现了较好的检测效果. Lotfollahi 等[11]使用堆叠自编码器（SAE，stack auto-encoder）和 CNN 相结合的模型对加密流量进行分类，在流量分类的粒度上既能实现流量特征分类也能实现应用类型识别. Yao 等[12]提出了一种基于高斯混合模型和隐马尔可夫模型（MGHMM，Gaussian mixture models and hidden Markov models）的流量分类模型和一种新的模型参数选择方法.

然而，上述基于深度学习的模型往往只考虑了流量的内部特征，忽略了进行通信时网络侧的交互信息，从而面临着分类性能的瓶颈. 一些学者提出了一种基于图的流量分类模型[13]，该方法将流量数据构建成一个图结构，其中 IP 地址作为图中的顶点，任何 2 个进行通信的 IP 地址之间都会有边相连. 随后，对图的属性进行分类. 然而，由于该图的顶点是 IP 地址，并没有细致地考虑到网络侧的行为信息存在的多样性以及异质性.

综上，在已有文献中尚无同时考虑流量级别的特征和网络侧的行为信息来进行网络入侵检测的研究. 为了充分利用这 2 种类型的信息，使用基于 CNN 和 GCN 的模型来同时学习原始网络流量数据的流量特征和行为信息，以开发更有效的入侵检测模型.

# 2　基于 GCN 的入侵检测模型

## 2.1　问题描述

网络流被定义为具有相同的源 IP、源端口、目的 IP、目的端口和传输层协议[14]的五元组的数据包集合. 网络入侵检测任务的目的是对网络通信中的流量进行二分类，将流量分为正常流量或攻击流量. 它可以定义为一个有向二部图的边分类问题. 该图

有2类节点:源端节点和目的端节点,网络流作为图的边. 受到了先前异质图嵌入工作[15]的启发,所提模型将终端在网络中的通信行为构建为一个异质图$G(S,D,E)$,其中$S$为由源IP和源端口表示的一组源端节点;$D$为一组目的端节点,由目的IP地址和目的端口组成;$E$为从源端节点传输到目的端节点的一组网络流(边). 如果$s \in S$向$d \in D$发送流,则存在从源端节点到目的端节点的边$e \in E$. 这种异质图也称为通信图,如图1左部分所示.

### 2.2 数据处理

根据网络流定义将流量数据分为多个网络流,网络流具有方向性(正向和反向). 此外,对于每个网络流,还需要进行填充或截断的操作,其目的是使得每个样本都具有固定大小的图像结构,图像中的每个像素代表流量中的一个字节. 之后将图像输入到1D-CNN中进行学习,得到流量$e$的嵌入向量为

$$\boldsymbol{h}_e^0 = C(\boldsymbol{x}) \tag{1}$$

其中:$\boldsymbol{x} \in \mathbf{R}^n$为表示流量样本的向量,$C(\cdot)$为1D-CNN的卷积函数.

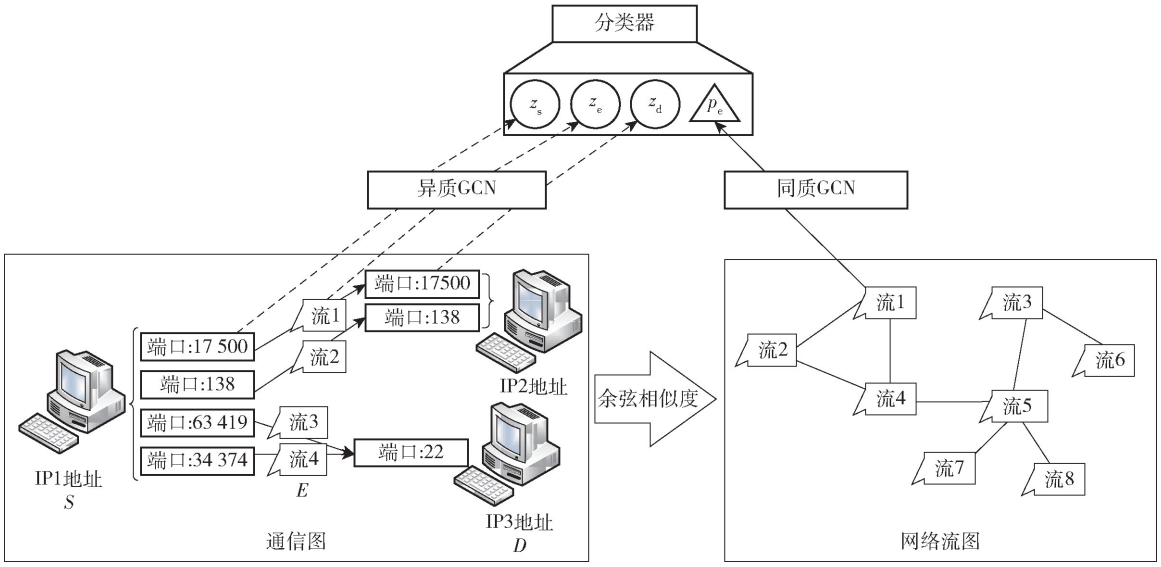



图1 IECNet模型架构

### 2.3 模型总览

提出了IECNet模型进行入侵流量分类,模型框架如图1所示. 提出的模型主要包括GCN和流量分类2个部分. 对流量数据分别建立通信图和网络流图,并将自设计的GCN对这2个图进行学习以捕获网络流量的外部网络侧交互信息. 最终将得到的流量嵌入向量进行分类,随后的小节将详细描述上述过程.

### 2.4 GCN

GCN的典型结构由多个传播层组成,一般来说,传播层可以分为2个子层. 给定一个带有节点和其邻居节点$v,v' \in V$,$(v,v') \in E$的图$G=(V,E)$,每个节点$v \in V$的节点特征为$\boldsymbol{x}_v = \boldsymbol{h}_v^0$. 对于具有$L$层的GCN,其在第$l$层($l=1,2,\cdots,L$)的聚合子层和组合子层学习到的嵌入向量可以表示为

$$\boldsymbol{h}_{N(v)}^l = \sigma(\boldsymbol{W}^l \cdot A(\{\boldsymbol{h}_{v'}^{l-1}, \forall v' \in N(v)\})) \tag{2}$$

$$\boldsymbol{h}_v^l = C_{\text{com}}(\boldsymbol{h}_v^{l-1}, \boldsymbol{h}_{N(v)}^l) \tag{3}$$

其中:$\sigma(\cdot)$为激活函数,$\boldsymbol{W}^l$为在第$l$层的所有节点之间共享的可训练矩阵,$A(\cdot)$为从相邻节点聚合嵌入向量的函数,$N(v)$为$v$的邻点集,$C_{\text{com}}(\cdot)$为用于聚合自身和邻点嵌入向量的函数.

#### 2.4.1 通信图上的GCN

在基于GCN的异质图节点分类任务中,需要利用最后一层传播层的节点嵌入向量,最后一个传播层的边嵌入向量和由这条边连接的2个顶点的嵌入向量. 最后,将上述3个嵌入向量拼接起来,用于最终的边分类任务. 如图1所示,$\boldsymbol{z}_e$,$\boldsymbol{z}_s$和$\boldsymbol{z}_d$表示边、源端节点和目的端节点的嵌入向量,即$\boldsymbol{z}_e = \boldsymbol{h}_e^l$,$\boldsymbol{z}_s = \boldsymbol{h}_{S(e)}^l$和$\boldsymbol{z}_d = \boldsymbol{h}_{D(e)}^l$,$S(e)$为边$e$的源端节点,$D(e)$为边$e$的目的端节点.

1) 聚合子层

GCN的聚合子层同等对待所有类型的节点,而忽略了边的属性. 为了适应上述通信图,此处为3种实体(源端节点、目的端节点和流)定义了3个聚合函数. 对于一个流(即一个边),它的隐藏状态通

过连接前一个边本身和它连接的 2 个节点的隐藏状态来更新. 因此,聚合子层定义为

$$\boldsymbol{h}_e^l=\sigma(\boldsymbol{W}_e^l\cdot\boldsymbol{A}_e^l(\boldsymbol{h}_e^{l-1},\boldsymbol{h}_{S(e)}^{l-1},\boldsymbol{h}_{D(e)}^{l-1})) \tag{4}$$

其中,

$$\boldsymbol{A}_e^l(\boldsymbol{h}_e^{l-1},\boldsymbol{h}_{S(e)}^{l-1},\boldsymbol{h}_{D(e)}^{l-1})=C_{\text{con}}(\boldsymbol{h}_e^{l-1},\boldsymbol{h}_{S(e)}^{l-1},\boldsymbol{h}_{D(e)}^{l-1}) \tag{5}$$

其中 $C_{\text{con}}(\cdot)$ 为拼接函数.

对于节点 $s\in S$ 和 $d\in D$,除了来自相邻节点的信息外,还聚合连接它们的边的属性. 聚合的邻居嵌入向量 $\boldsymbol{h}_{N(s)}^l$,$\boldsymbol{h}_{N(d)}^l$ 计算为

$$\boldsymbol{h}_{N(s)}^l=\sigma(\boldsymbol{W}_s^l\cdot\boldsymbol{A}_s^l(\boldsymbol{H}_s^{l-1})) \tag{6}$$

$$\boldsymbol{h}_{N(d)}^l=\sigma(\boldsymbol{W}_d^l\cdot\boldsymbol{A}_d^l(\boldsymbol{H}_d^{l-1})) \tag{7}$$

其中,

$$\boldsymbol{H}_s^{l-1}=\{C_{\text{con}}(\boldsymbol{h}_s^{l-1},\boldsymbol{h}_e^{l-1}),\forall e=(s,d)\in E(s)\} \tag{8}$$

$$\boldsymbol{H}_d^{l-1}=\{C_{\text{con}}(\boldsymbol{h}_d^{l-1},\boldsymbol{h}_e^{l-1}),\forall e=(s,d)\in E(d)\} \tag{9}$$

其中 $E(s)$ 和 $E(d)$ 分别为节点 $s$ 和 $d$ 的邻边集.

边和节点分别维护不同的参数 $(\boldsymbol{W}_s^l,\boldsymbol{W}_d^l)$,不同的聚合矩阵 $(\boldsymbol{A}_s^l,\boldsymbol{A}_d^l)$. 对于 $\boldsymbol{A}_s^l$ 和 $\boldsymbol{A}_d^l$ 的具体形式,采用注意力机制:

$$\boldsymbol{A}_s^l(\boldsymbol{H}_s^{l-1})=A_{\text{att}}(\boldsymbol{h}_{S(e)}^{l-1},\boldsymbol{H}_s^{l-1}) \tag{10}$$

$$\boldsymbol{A}_d^l(\boldsymbol{H}_d^{l-1})=A_{\text{att}}(\boldsymbol{h}_{D(e)}^{l-1},\boldsymbol{H}_d^{l-1}) \tag{11}$$

其中:$A_{\text{att}}$ 为函数 $F:\boldsymbol{h}_{\text{key}}\times\boldsymbol{H}_{\text{val}}\rightarrow\boldsymbol{h}_{\text{val}}$,它将一个特征向量 $\boldsymbol{h}_{\text{key}}$ 和一组候选特征向量 $\boldsymbol{h}_{\text{val}}$ 映射到 $\boldsymbol{H}_{\text{val}}$ 中元素的加权和. 求和的权重(即注意力分数),由缩放点乘注意力计算得到[16].

2) 组合子层

在聚合了邻居信息之后,对源端节点和目的端节点进行如下处理:

$$\boldsymbol{h}_s^l=C_{\text{con}}(\boldsymbol{V}_s^l\cdot\boldsymbol{h}_{S(e)}^{l-1},\boldsymbol{h}_{N(s)}^l) \tag{12}$$

$$\boldsymbol{h}_d^l=C_{\text{con}}(\boldsymbol{V}_d^l\cdot\boldsymbol{h}_{D(e)}^{l-1},\boldsymbol{h}_{N(d)}^l) \tag{13}$$

其中:$\boldsymbol{h}_s^l$ 和 $\boldsymbol{h}_d^l$ 为源端节点和目的端节点在第 $l$ 层的隐藏状态,$\boldsymbol{V}_s^l$ 和 $\boldsymbol{V}_d^l$ 为源端节点和目的端节点的可训练权重矩阵.

2.4.2　网络流图上的 GCN

网络流图是一个无向同质图,通过连接具有一定相似度的网络流来构建,从而通信图中的边(网络流)现在成为网络流图中的顶点,具体如图 1 右侧所示. 相似度使用余弦距离.

对于一条一般化的网络流 $\boldsymbol{f}_i$,可以表示为

$$\boldsymbol{f}_i=(\boldsymbol{x}_0,\boldsymbol{x}_1,\boldsymbol{x}_2,\cdots,\boldsymbol{x}_n) \tag{14}$$

其中 $n$ 为每个网络流样本的特征数.

构建网络流图后使用同质 GCN 学习流量在同质图中的嵌入向量,得到该样本在网络流图的最终嵌入向量:

$$\boldsymbol{p}_e=G(C_{\text{con}}(\boldsymbol{f}_1,\boldsymbol{f}_2,\cdots,\boldsymbol{f}_m)) \tag{15}$$

其中:$G(\cdot)$ 为 GCN 的卷积函数,$m$ 为该样本在网络流图中网络流的总数.

### 2.5　流量分类

IECNet 模型得到的最终嵌入向量是上述 $\boldsymbol{p}_e$ 和从通信图中学习嵌入向量的拼接,并输入到 softmax 层中进行最终的分类:

$$y=C_{\text{cla}}(C_{\text{con}}(\boldsymbol{z}_s,\boldsymbol{z}_d,\boldsymbol{z}_e,\boldsymbol{p}_e)) \tag{16}$$

其中 $C_{\text{cla}}(\cdot)$ 为分类器函数

## 3　实验及结果分析

### 3.1　数据集

实验使用 1998 年美国国防部高等研究计划局数据集[17](DARPA1998, defense advanced research projects agency 1998 data)和 2012 年信息安全卓越中心数据集[18](ISCX2012, the information security centre of excellence 2012 data),它们的发布年份和流量类型差异很大,有助于评估模型的普遍性.

DARPA1998 数据集中,流量的类型包括正常流量和 DoS 攻击、端口攻击、远程用户(R2L, remote to login)攻击、提权(U2R, user to root)攻击 4 种恶意流量. 数据集按时间跨度分割为训练集和测试集,如表 1 所示.

**表 1　分割后的 DARPA1998 数据集**

| 流量类型 | 训练集 | | 测试集 | |
|---|---|---|---|---|
| | 数量 | 百分比/% | 数量 | 百分比/% |
| 正常流量 | 849 991 | 34.45 | 459 547 | 41.79 |
| DoS 攻击 | 1 561 231 | 63.29 | 591 619 | 53.79 |
| 端口攻击 | 48 984 | 1.99 | 40 317 | 3.67 |
| R2L 攻击 | 6 494 | 0.26 | 8 041 | 0.73 |
| U2R 攻击 | 229 | 0.01 | 207 | 0.02 |
| 总计 | 2 466 929 | 100.00 | 1 099 731 | 100.00 |

相比于 DARPA1998 数据集,ISCX2012 数据集的攻击流量占比极小,约为 2.8%. 流量的类型包括正常流量和暴力破解(BFSSH, brute force secure shell)攻击、渗透攻击、超文本传输协议拒绝服务(HttpDoS, hyper text transfer protocol denial of service)攻击和分布式拒绝服务(DDoS, distributed

denial of service)攻击4种恶意流量. 按照一定比例将数据集分割为训练集和测试集,如表2所示.

**表2 分割后的ISCX2012数据集**

| 流量类型 | 训练集 | | 测试集 | |
|---|---|---|---|---|
| | 数量 | 百分比/% | 数量 | 百分比/% |
| 正常流量 | 890 726 | 97.27 | 593 811 | 97.27 |
| BFSSH攻击 | 4 179 | 0.46 | 2 785 | 0.46 |
| 渗透攻击 | 6 027 | 0.66 | 4 017 | 0.66 |
| HttpDoS攻击 | 2 090 | 0.23 | 1 392 | 0.23 |
| DDos攻击 | 12 673 | 1.38 | 8 448 | 1.38 |
| 总计 | 915 695 | 100.00 | 610 453 | 100.00 |

### 3.2 对比模型和评价指标

为了评估模型的有效性,使用如下对比模型:基于支持向量机(SVM, support vector machine)的模型、基于多层感知机(MLP, multilayer perceptron)的模型、基于1D-CNN的模型和基于分层时空特征的入侵检测系统(HAST, hierarchical spatial-temporal features-based intrusion detection system)模型,模型参数分别参照文献[4],文献[19-21]进行设置. 评价指标选取了入侵检测领域常用的4个指标,即准确率(ACC, accuracy)、正常流量检测率(NDR, normal detection rate)、攻击流量检测率(ADR, attack detection rate)和误报率(FAR, false alarm rate),定义分别为

$$R_{\mathrm{ACC}}=\frac{N_{\mathrm{tp}}+N_{\mathrm{tn}}}{N_{\mathrm{tp}}+N_{\mathrm{tn}}+N_{\mathrm{fp}}+N_{\mathrm{fn}}} \tag{17}$$

$$R_{\mathrm{NDR}}=\frac{N_{\mathrm{tn}}}{N_{\mathrm{tn}}+N_{\mathrm{fp}}} \tag{17}$$

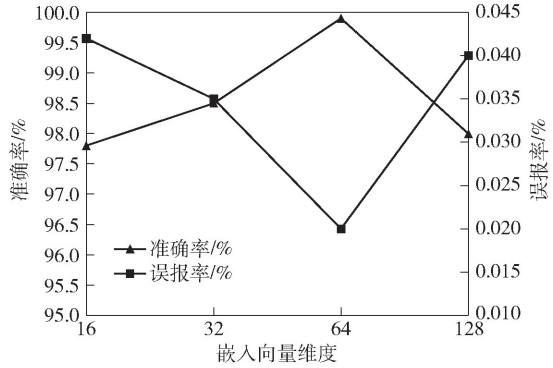
$$R_{\mathrm{ADR}}=\frac{N_{\mathrm{tp}}}{N_{\mathrm{tp}}+N_{\mathrm{fn}}} \tag{18}$$

$$R_{\mathrm{FAR}}=\frac{N_{\mathrm{fp}}}{N_{\mathrm{tn}}+N_{\mathrm{fp}}} \tag{19}$$

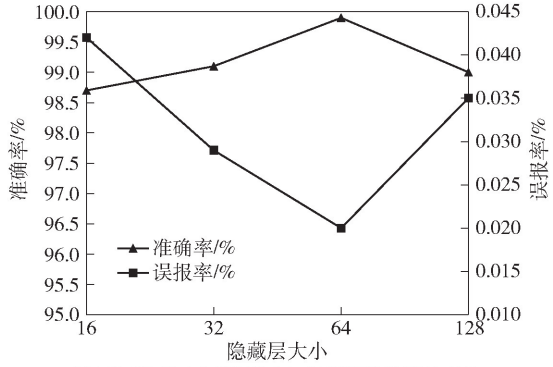
其中:$N_{\mathrm{tp}}$为正确分类为攻击流量的实例数,$N_{\mathrm{tn}}$为正确分类为正常流量的实例数,$N_{\mathrm{fp}}$为将正常流量错误分类为攻击流量的实例数,$N_{\mathrm{fn}}$为将攻击流量错误分类为正常流量的实例数.

### 3.3 参数实验

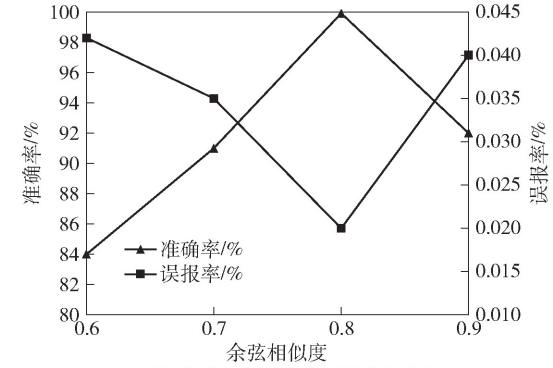
在本节中,将探讨不同参数对模型性能的影响. 模型的关键参数包括异质GCN的嵌入向量维度、注意力层的隐藏层大小和余弦相似度的阈值,所有参数实验均在ISCX2012数据集上进行. 实验结果如图2所示. 由图2(a)可知,异质GCN的嵌入向量维数的最佳值为64. 该现象说明嵌入向量维度为64时刚好合适,当小于64时,模型未拟合;大于64时,模型变为过拟合,都无法很好地学习到样本空间的特征表示. 由图2(b)可知,注意力层的隐藏层大小为64时效果最好,可以认为此时注意力层能够更好地学习到嵌入向量的上下文信息并加以编码. 余弦相似度的选取如图2(c)所示,相似度为0.8时,模型性能最好. 余弦相似度的选取间接影响了后续构建网络流图时每个邻点边的数目:当选取该值过大时,因邻点数目过少而无法提取足够特征;而当选取该值过小时,每个顶点的邻点过多,为模型引入了噪声,反而使模型提取到错误的特征.




(a) 不同嵌入向量维度下模型性能的变化




(b) 不同注意力层隐藏层大小下模型性能的变化




(c) 不同余弦相似度下模型性能的变化

图2 ISCX2012数据集上的不同参数下模型性能的变化

### 3.4　实验分析

3.4.1　性能对比

为验证模型的有效性，在 2 个不同数据集上进行了实验，并分别使用训练集的 20%，40%，60% 和 80% 的子集进行训练. 实验参数基于 3.3 节的实验最优结果进行设置，异质 GCN 的隐藏层数为 2，嵌入向量维度为 64，注意力层的隐藏层大小为 64，余弦相似度为 0.8，梯度算法的动量为 0.5，学习率为 0.001. 实验结果如表 3 和表 4 所示. 所提出的 IECNet 模型在不同的子集中，ACC，NDR，ADR 和 FAR 指标绝大部分都优于对比模型，这表明了所提模型的有效性. IECNet 模型有效地使用 CNN 提取流量的内部特征，并使用 GCN 提取流量网络侧的行为信息，最终实现了最优的流量识别效果.

**表 3　所提模型和其他模型在 DARPA1998 数据集上的性能对比**　%

| 模型 | 训练集 20% 子集 | | | | 训练集 40% 子集 | | | | 训练集 60% 子集 | | | | 训练集 80% 子集 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | ACC | NDR | ADR | FAR | ACC | NDR | ADR | FAR | ACC | NDR | ADR | FAR | ACC | NDR | ADR | FAR |
| SVM | 76.10 | 73.20 | 75.40 | 0.20 | 78.90 | 75.30 | 78.60 | 0.15 | 81.30 | 76.70 | 80.40 | 0.09 | 84.80 | 80.10 | 82.30 | 0.08 |
| MLP | 94.10 | 94.90 | 90.10 | 0.54 | 95.10 | 96.30 | 93.20 | 0.50 | 97.10 | 97.40 | 95.60 | 0.30 | 97.90 | 98.70 | 96.30 | 0.30 |
| 1D-CNN | 95.10 | 94.30 | 91.36 | 0.18 | 96.30 | 96.39 | 93.90 | 0.12 | 98.12 | 97.45 | 96.00 | 0.09 | 98.90 | 98.90 | 97.43 | 0.07 |
| HAST | 96.70 | 95.20 | 93.25 | 0.13 | 98.30 | 97.10 | 95.14 | 0.10 | 99.69 | 99.10 | 97.78 | 0.07 | 99.70 | 99.30 | 98.20 | 0.07 |
| IECNet | 97.31 | 96.10 | 95.00 | 0.10 | 98.30 | 98.20 | 97.10 | 0.06 | 99.70 | 99.70 | 98.60 | 0.04 | 99.67 | 99.75 | 99.10 | 0.03 |

**表 4　所提模型和其他模型在 ISCX2012 数据集上的性能对比**　%

| 模型 | 训练集 20% 子集 | | | | 训练集 40% 子集 | | | | 训练集 60% 子集 | | | | 训练集 80% 子集 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | ACC | NDR | ADR | FAR | ACC | NDR | ADR | FAR | ACC | NDR | ADR | FAR | ACC | NDR | ADR | FAR |
| SVM | 96.40 | 96.10 | 66.70 | 0.10 | 98.30 | 98.50 | 67.30 | 0.05 | 99.50 | 99.90 | 68.20 | 0.03 | 99.60 | 99.80 | 70.10 | 0.02 |
| MLP | 95.60 | 94.20 | 96.80 | 2.60 | 97.80 | 96.30 | 98.20 | 2.40 | 99.00 | 97.70 | 99.70 | 2.20 | 99.50 | 98.40 | 99.80 | 1.90 |
| 1D-CNN | 95.87 | 95.15 | 96.30 | 0.09 | 97.93 | 96.79 | 96.81 | 0.07 | 98.20 | 98.84 | 97.30 | 0.04 | 98.90 | 98.35 | 97.90 | 0.01 |
| HAST | 97.80 | 96.70 | 94.20 | 0.08 | 98.90 | 98.80 | 95.29 | 0.04 | 99.89 | 99.97 | 96.96 | 0.02 | 99.91 | 99.90 | 97.10 | 0.02 |
| IECNet | 98.00 | 98.32 | 97.21 | 0.05 | 98.90 | 99.00 | 98.30 | 0.03 | 99.90 | 99.97 | 99.83 | 0.02 | 99.90 | 99.92 | 99.70 | 0.01 |

3.4.2　耗时实验

本节基于 3.4.1 节列出的参数展开模型的训练和测试时间的耗时实验，结果如表 5 所示. 由表可知，在 DARPA1998 数据集上 IECNet 模型的训练和测试时间分别为 46.5 min（2790 s）和 2.9 min（174 s），相比耗时最少的 1D-CNN 模型，IECNet 模型在增加少许训练时间和测试时间的代价下，实现了最优的识别性能，这清楚地表明了所提方案的高效率.

**表 5　所提模型在 DARPA1998 数据集上的耗时实验结果对比**　min

| 模型 | 训练时长 | 测试时长 |
|---|---|---|
| SVM | 124 | 18 |
| MLP | 1 083 | 3 |
| 1D-CNN | 39 | 1.2 |
| HAST | 43 | 1.3 |
| IECNet | 46.5 | 2.9 |

## 4　结束语

提出了一种基于 IECNet 的入侵检测模型用以解决网络入侵检测的问题. 所提模型通过将流量数据建模为图结构，并使用 CNN 和 GCN 捕获流量数据的内部特征和网络侧行为信息，实现了模型性能的提升. 实验结果证明了该模型的有效性，并优于对比模型. 但存在的问题是模型虽然分类准确率高，但只限于二分类的场景，无法检测出特定的攻击类型（即多分类场景），需要进一步改进，这也是未来的研究方向.

**参考文献：**

[1] 焦宏宇. 基于 Openstack 的新型蜜场系统[D]. 南京：南京邮电大学，2018：2-3.

[2] Liao H J, Lin C H R, Lin Y C, et al. Intrusion detection system: a comprehensive review[J]. Journal of Network and Computer Applications, 2013, 36(1): 16-24.

[3] Wang Wei, Sheng Yiqiang, Wang Jinlin, et al. HAST-

IDS: learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection[J]. IEEE Access, 2017, 6: 1792-1806.

[4] Zhang Fengli, Wang Dan. An effective feature selection approach for network intrusion detection[C]//2013 IEEE Eighth International Conference on Networking, Architecture and Storage. Piscataway: IEEE, 2013: 307-311.

[5] Hubballi N, Suryanarayanan V. False alarm minimization techniques in signature-based intrusion detection systems: a survey[J]. Computer Communications, 2014, 49: 1-17.

[6] Ma Tao, Wang Fen, Cheng Jianjun, et al. A hybrid spectral clustering and deep neural network ensemble algorithm for intrusion detection in sensor networks[J]. Sensors, 2016, 16(10): 1701.

[7] Javaid A, Niyaz Q, Sun Weiqing, et al. A deep learning approach for network intrusion detection system[J]. EAI Endorsed Transactions on Security and Safety, 2016, 3(9): e2.

[8] Tan Zhiyuan, Jamdagni A, He Xiangjian, et al. Detection of denial-of-service attacks based on computer vision techniques[J]. IEEE Transactions on Computers, 2014, 64(9): 2519-2533.

[9] Torres P, Catania C, Garcia S, et al. An analysis of recurrent neural networks for botnet detection behavior[C]// 2016 IEEE Biennial Congress of Argentina (ARGENCON). Piscataway: IEEE, 2016: 1-6.

[10] Zhang Jianwu, Ling Yu, Fu Xingbing, et al. Model of the intrusion detection system based on the integration of spatial-temporal features[J]. Computers & Security, 2020, 89: 101681.

[11] Lotfollahi M, Siavoshani M J, Zade R S H, et al. Deep packet: a novel approach for encrypted traffic classification using deep learning[J]. Soft Computing, 2020, 24(3): 1999-2012.

[12] Yao Zhongjiang, Ge Jingguo, Wu Yulei, et al. Encrypted traffic classification based on Gaussian mixture models and hidden Markov models[J]. Journal of Network and Computer Applications, 2020, 166: 102711.

[13] Iliofotou M, Kim H, Faloutsos M, et al. Graption: a graph-based P2P traffic classification framework for the internet backbone[J]. Computer Networks, 2011, 55(8): 1909-1920.

[14] Moore A W, Papagiannaki K. Toward the accurate identification of network applications[C]// International Workshop on Passive and Active Network Measurement. Berlin: Springer, 2005: 41-54.

[15] Li Ao, Qin Zhou, Liu Runshi, et al. Spam review detection with graph convolutional networks[C]//28th ACM International Conference on Information and Knowledge Management. New York: ACM, 2019: 2703-2711.

[16] Vaswani A, Shazeer N, Parmar N, et al. Attention is all you need[C]// Advances in Neural Information Processing Systems. New York: Curran Associates, 2017: 5998-6008.

[17] Lippmann R, Cunningham R K, Fried D J, et al. Results of the DARPA 1998 offline intrusion detection evaluation[C]// Recent Advances in Intrusion Detection. Berlin: Springer, 1999: 829-835.

[18] Shiravi A, Shiravi H, Tavallaee M, et al. Toward developing a systematic approach to generate benchmark datasets for intrusion detection[J]. Computers & Security, 2012, 31(3): 357-374.

[19] Xu Xin. Adaptive intrusion detection based on machine learning: feature extraction, classifier construction and sequential pattern prediction[J]. International Journal of Web Services Practices, 2006, 2(1-2): 49-58.

[20] Farid D M, Harbi N, Rahman M Z. Combining naive Bayes and decision tree for adaptive intrusion detection[J]. International Journal of Network Security & Its Applications, 2010, 2(2): 12-25

[21] Wang Wei, Zhu Ming, Wang Jinlin, et al. End-to-end encrypted traffic classification with one-dimensional convolution neural networks[C]//2017 IEEE International Conference on Intelligence and Security Informatics (ISI). Piscataway: IEEE, 2017: 43-48.