•人工智能安全•

DOI:10.15961/j.jsuese.202100784

本刊网刊

基于图神经网络的P2P僵尸网络检测方法

林宏刚[1,2,3], 张运理[1,2], 郭楠馨[1,2], 陈　麟[3*]

(1.成都信息工程大学 网络空间安全学院, 四川 成都 610225; 2.先进密码技术与系统安全四川省重点实验室, 四川 成都 610225;
3.网络空间安全态势感知与评估安徽省重点实验室, 安徽 合肥 230037)

摘　要:P2P僵尸网络因具有较高的隐蔽性和健壮性, 已经成为新型的网络攻击平台, 对网络空间安全造成的威胁越来越大, 但现有基于规则分析或流量分析的检测方法不能有效检测。为了解决P2P僵尸网络隐蔽性强、难以识别等问题, 提出了一种基于图神经网络(graph neural network, GNN)的P2P僵尸网络检测方法。该方法不依赖流量协议特征, 而是基于P2P僵尸网络节点交互特征及网络拓扑结构信息实现检测。首先, 该方法先提取P2P僵尸网络流量中的源IP、目的IP、出度、入度和节点介数中心性, 构建成拓扑图、出入度图和介数中心性图; 其次, 通过元素积对3种特征图的邻接矩阵加权求和进行图融合, 得到检测模型的输入; 然后, 利用基于注意力机制的图卷积神经网络提取节点间特征, 使用神经协同过滤算法实现中心节点注意力概率分配, 完成节点状态更新; 最后, 利用多层图卷积层之间的紧密连通性实现对交互特征的降维抽取和对高阶结构信息的挖掘, 自动学习僵尸网络的内在特征, 并通过节点分类模块判别分类, 完成僵尸网络检测。使用ISCX–2014僵尸网络数据集对该方法进行对比验证, 实验结果表明, 在训练样本包含僵尸网络节点规模较大时本文提出的深层图神经网络方法的检测准确率和模型稳定性优于其他两类对比方法, 所提方法能有效提高P2P僵尸网络检测能力和泛化能力, 降低误报率。

关键词:P2P僵尸网络; 深度学习; 图卷积神经网络; 图融合; 注意力机制

中图分类号:TP309.5　　**文献标志码**:A　　**文章编号**:2096-3246(2022)02-0065-08

P2P Botnet Detection Method Based on Graph Neural Network

LIN Honggang[1,2,3], *ZHANG Yunli*[1,2], *GUO Nanxin*[1,2], *CHEN Lin*[3*]

(1.School of Cyberspace Security, Chengdu Univ. of Info.Technol., Chengdu 610225, China;
2.Advanced Cryptography and System Security Key Lab. of Sichuan Province, Chengdu 610225, China;
3.Anhui Province Key Lab. of Cyberspace Security Situation Awareness and Evaluation, Hefei 230037, China)

Abstract: P2P botnet has become a new network attack platform because of its high concealment and robustness, which poses an increasing threat to cyberspace security. However, the existing detection methods based on rule analysis or traffic analysis can't detect it effectively. In order to solve the problems of strong concealment and difficult identification of P2P botnets, a P2P botnet detection method based on graph neural network (GNN) was proposed. The method was based on the information of P2P botnet node interaction and network topology to realize detection and did not rely on the characteristics of traffic protocol. Firstly, the source IP, the destination IP, the outdegree, the indegree and the node betweenness centrality in P2P botnet traffic were extracted to construct a topology graph, an out-degree and in-degree graph and a betweenness centrality graph; Then, the weighted sum of adjacency matrices of the three feature graphs was fused by element-wise product to input into the detection model; Then, a graph convolution neural network based on attention mechanism was used to extract the features between nodes, and the neural collaborative filtering algorithm was used to realize the attention probability distribution of the central node and complete the node state update; Using the close connectivity between multi-layer graph convolution layers, the dimension reduction extraction of interactive features and the

收稿日期:2021 – 08 – 11

基金项目:网络空间安全态势感知与评估安徽省重点实验室开放课题(CSSAE–2021–002); 国家242信息安全计划项目(2021–037)

作者简介:林宏刚(1976—), 男, 博士, 教授. 研究方向: 网络空间安全. E-mail: linhg@cuit.edu.cn

* **通信作者**:陈　麟, E-mail: chenlin@cuit.edu.cn

网络出版时间:2022 – 03 – 11 14 : 08 : 15　　**网络出版地址**:https://kns.cnki.net/kcms/detail/51.1773.TB.20220310.1115.001.html

mining of high-order structure information were realized. The internal characteristics of botnet were automatically learned, and the botnet detection was completed through the node classification module. The proposed method was validated on the ISCX–2014 botnet dataset. The experimental results showed that the proposed deep graph neural network method outperforms the other two comparative methods in terms of detection accuracy and model stability when the training sample contains botnet nodes of large size. The model can effectively improve the detection ability and generalization ability of P2P botnets, as well as reduce the false positive rate.

Key words: P2P botnet; deep learning; graph convolution neural networks; graph fusion; attention mechanism

僵尸网络是指被黑客集中控制的计算机群，其核心特点是黑客能够通过一对多的命令与控制信道操纵感染木马或僵尸程序的主机执行相同的恶意行为[1]，如分布式拒绝服务攻击、发送垃圾邮件、虚拟货币挖掘等。2020年网络安全报告显示，中国境内僵尸程序受控主机IP地址数量高达5百万，受控服务器数量为12 810个，僵尸网络侵害事件情况依旧严峻。早期基于IRC和HTTP的僵尸网络易被检测发现，目前攻击者更青睐于采用隐蔽性和威胁性更大的P2P技术创建僵尸网络，P2P僵尸网络检测成为当前热门研究课题。

目前，僵尸网络检测相关工作主要应用机器学习算法（例如，随机森林、SVM、k–means等）[2]。此类方法采用监督学习方法建立基于人为标记的网络流量特征的模型检测僵尸流量。近年来，研究者也开始采用一些深度学习算法（例如，CNN、LSTM、RNN等）检测僵尸网络流量，并取得了一些很好的效果，应用基于深度学习的大数据分析技术能够实现数据特征的快速自动抽取，解决建模过程中对专家知识的依赖[3]。根据检测所依赖特征的不同，僵尸网络检测方法主要分为基于网络流量协议特征和基于网络流量通信图特征两类。

基于网络流量协议特征的检测方法利用机器学习或者深度学习算法提取僵尸网络流量协议特征来检测僵尸网络。Algelal等[4]使用集成分类器对僵尸网络流量特征进行提取，进而区分正常流量和僵尸流量。吴迪等[5]设计实现BotCatcher，可以提取僵尸网络流量的时间和空间两项特征，无需依赖流量相关协议特征，进而实现对僵尸网络的检测。牛伟纳等[6]研究相似性来提取僵尸网络流量会话特征，并使用基于决策树的随机森林算法来检测P2P僵尸网络。Wang等[7]提出一种基于卷积神经网络（convolutional neural network, CNN）的恶意软件流量分类方法，采用CNN算法提取网络流量的空间特征，将流量数据转换为2维图像作为CNN的输入，进而进行特征学习，实现自动检测。罗扶华等[8]提出一种基于深度学习的检测方法，先将原始流量转化为2维图像样本，再利用卷积神经网络学习样本的空间特征、长短期记忆网络（long short-term memory, LSTM）学习样本的时序特征，完成对僵尸网络的检测。基于网络流量协议特征的僵尸网络检测技术主要依赖于检测通信流的统计特征，但在真实网络环境下，网络流量数据量大，计算量大，导致检测效率较低。此外，检测经过混淆加密的僵尸网络流量时，此类方法将会失效。

基于网络流量通信图特征的检测方法是研究人员为克服模型对数据依赖性高、通用性不足等问题而采取的手段。由于节点间交互可以映射到图模型，因此可用图的异常检测方法对动态网络异常进行检测，例如AddGraph[9]、Graph–TR[10]、GDN[11]、Spotlight[12]。在此基础上，研究人员常采用图的异常点检测和拓扑图交互特征提取方法来检测僵尸网络。Chowdhury等[13]根据通信图的网络拓扑结构，提取七大类图结构特征，采用自组织映射（self-organizing maps, SOM）算法检测僵尸网络。Lagraa等[14]提出BotGM，将网络流量行为转换为事件序列，构建有向图，采用图编辑距离来检测异常点。Wang等[15]提出Botcapturer，基于图异常检测和网络流量聚类的两层僵尸网络检测框架，采用传统k–means算法聚类标记出可疑聚合流。Wang等[16]提出BotMark，该框架基于相似性模型、稳定性模型以及图模型采用投票机制来识别僵尸流量。基于通信图特征的检测方法需要大量人工定义拓扑特征，执行多个预过滤步骤，并且大多需要依赖数据的特征工程和参数调优。

随着网络结构数据（图）的应用越来越广泛，传统方法已无法满足挖掘动态网络中异常元素的需求。图神经网络作为一种深度学习技术，能同时结合图的属性特征和结构特征来对图的异常数据挖掘[17–19]。刘杰等[20]提出了一种基于图神经网络的工控网络异常检测算法，融合网络节点自身属性及网络拓扑结构中邻域节点的信息实现对网络异常的检测。曲强等[21]针对现有社交网络Spammer检测方法仅能提取浅层特征与计算复杂度高的问题，提出了一种基于图卷积网络（GCN）的社交网络Spammer检测技术。郭嘉琰等[22]提出一种基于图神经网络的异常检测算法，将图结构、属性以及动态变化的信息引入模型中，学习进行异常检测的表示向量。

本文提出基于图神经网络的P2P僵尸网络检测方法用于解决现有的检测方法存在的不能检测加密

流量、数据量大、计算复杂等问题。首先，该方法对数据集进行预处理工作，提取节点多个特征生成特征图，并通过图融合方法得到模型输入权重图；然后，将此图作为多层图卷积神经网络模型的输入，通过多层叠加的基于注意力机制的图卷积网络提取节点间特征，完成节点状态更新；最后，对僵尸网络特征进行学习，并通过节点分类完成僵尸网络的检测。该方法不依赖流量协议特征，而是融合P2P僵尸网络节点交互特征及网络拓扑结构的信息实现僵尸网络的检测。基于ISCX–Bot–2014僵尸网络数据集将本文方法与两种已有方法进行对比试验与分析，实验结果表明本文方法对P2P僵尸网络的检测效果更好。

1　基于图神经网络的P2P僵尸网络检测模型

图神经网络是为了在图结构的数据上进行深度学习而发展兴起的一种神经网络模型，可以自动识别图中的节点依赖关系，不需要显式过滤器、显式特性定义或手动调优，在提取图特征方面应用效果极佳。本文基于节点交互特征及网络拓扑结构的信息构建特征图以表征P2P僵尸网络，因此可利用GNN识别图中的节点特征来检测P2P僵尸网络。本文提出的基于图神经网络的P2P僵尸网络检测方法如图1所示，下面对图生成、基于图神经网络的特征提取模型、节点分类3个主要模块进行介绍。

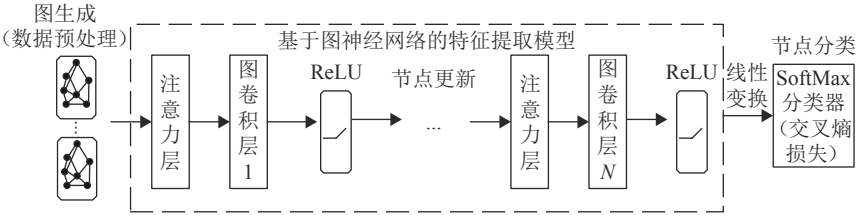

图 1　基于图神经网络的P2P僵尸网络检测模型

Fig. 1　P2P botnet detection model based on graph neural networks

1.1　图生成

数据预处理过程如下：模型输入为图数据，本文选用的僵尸网络流量数据集文件格式为pcap，为保证特征提取的正确有效，需要进行数据预处理。数据集中数据流量包含除P2P僵尸网络之外的各类数据，数据流存在建立不完全的情况，此类数据包对检测没有实际意义，需要进行数据清洗。完成上述工作后，从pcap数据包文件中提取出构建特征图所需的源IP、目的IP、节点入度、节点出度、节点介数中心性，绘制相关特征图作为图融合的输入。

采用图数据作为模型输入时，如果模型输入的图不能对节点间的有效关系进行编码，不仅不利于网络参数的学习，还会降低检测性能。为避免图上节点信息丢失过多，影响检测结果，本文构建3种节点特征图，采用图融合方法将3个不同图权重融合为1个图权重。根据P2P僵尸网络中节点的源IP、目的IP、节点入度、节点出度、节点介数中心性几项属性分别构建拓扑图、出入度图和介数中心性图，具体实现方法如下。

1）根据源IP、目的IP两项属性，基于NetworkX图分析算法，将pcap数据包中互相通信的主机作为图的节点，主机之间的连接关系作为图的边，构造拓扑图$\boldsymbol{G}_{\mathrm{e}}=(V,\boldsymbol{E})$，其中，$V$为图中节点集合$\{v_1,v_2,\cdots,v_n\}$；$\boldsymbol{E}\in\boldsymbol{R}^{n\times n}$为节点邻接矩阵，其元素$e_{ij}=1$为节点$v_i$与$v_j$之间存在直接通信。

2）根据节点出度、节点入度两项属性，基于拓扑图将出入度作为图中节点间的权重，构造出入度图$\boldsymbol{G}_d=(V,\boldsymbol{D})$，其中，$\boldsymbol{D}=\mathrm{diag}(d_1,d_2,\cdots,d_n)$节点出入度矩阵表示相应节点的度。

3）根据节点介数中心性这项属性，基于拓扑图将节点介数中心性作为节点间的权重，构造介数中心性图$\boldsymbol{G}_b=(V,B)$，介数中心性体现两个非邻接的节点间的依赖关系，是检测P2P僵尸网络的一项有用特征。用$B_v=\sum_{i\neq j\neq v\in V}\frac{\sigma_{ij}(v)}{\sigma_{ij}}$表示节点$v$的中心性系数，其中，$\sigma_{ij}$为从节点$v_i$到节点$v_j$的最短路径总数，$\sigma_{ij}(v)$为通过节点$v$的最短路径总数。

4）图融合过程中，先对每个图的邻接矩阵$\boldsymbol{A}$进行标准化，再通过元素积对不同图的邻接矩阵加权求和来组合不同的图。为了使加权和运算后的融合结果保持归一化，在加权矩阵中增加一个SoftMax运算，图融合过程可表示为：

$$\boldsymbol{G}=\sum_{i=1}^{3}w_i'\circ\boldsymbol{A}_i' \tag{1}$$

式中：w_i'为一条边上的i个权重，$w_i'=\mathrm{SoftMax}(w_i)$；“$\circ$”表示元素积运算；$\boldsymbol{G}$为图融合得到的图，用作模型输入；$\boldsymbol{A}_i'$为标准化后的邻接矩阵。

1.2　基于图神经网络的特征提取模型

针对P2P僵尸网络的高混合率和传播率等相关特征，基于Kipf等[23]提出的图神经网络框架，本文引入图融合及注意力机制，设计了一个包含多个图卷

积层的图神经网络特征提取模型，如图1虚线框中内容所示，主要包含注意力机制层和图卷积层。下面将对改进的图神经网络特征提取模型进行介绍。

1.2.1 注意力机制层

图卷积模型中对节点权重参数的解释采用切比雪夫多项式方案，在一个领域阶次内所有邻节点所对应的权值相同，无法体现中心节点受邻节点影响力的差异。同时在节点数量较小的情况下，图卷积模型容易达到过拟合的状态。因此。引进注意力机制，改进了图卷积模型更新中心节点特征状态的方法，能更好地提取节点特征，得到的权重参数有更好的解释能力。注意力概率分配的实现流程如下：首先，利用神经协同过滤算法（neural collaborative filtering algorithm, NCF）[24]，计算得到邻节点到中心节点的相似性概率分布；本文在原始NCF模型的基础上进行了调整，在NeuMF层上添加了tanh激活函数，并将其输出固定为注意力概率，如图2所示。然后，将每个节点与其邻居的相似性向量进行均一化操作，获得加权计算的权重。最后，对邻节点特征进行加权求和，其公式表示如式（2）所示，通过神经网络框架下反向传播学习，能更好地适用于未在训练集中出现过的图数据。

$$\boldsymbol{X}_i^{(l)} = \sum_i \frac{\mathrm{attn}(v_{\mathrm{center}}, v_{\mathrm{neigh}}^i) \times v_{\mathrm{neigh}}^i}{\sum_i \mathrm{attn}(v_{\mathrm{center}}, v_{\mathrm{neigh}}^i)} \tag{2}$$

式中，$\boldsymbol{X}_i^{(l)}$为加权求和得到的邻节点特征矩阵，$\mathrm{attn}(v_{\mathrm{center}}, v_{\mathrm{neigh}}^i)$为中心节点与邻节点的相似性度量。

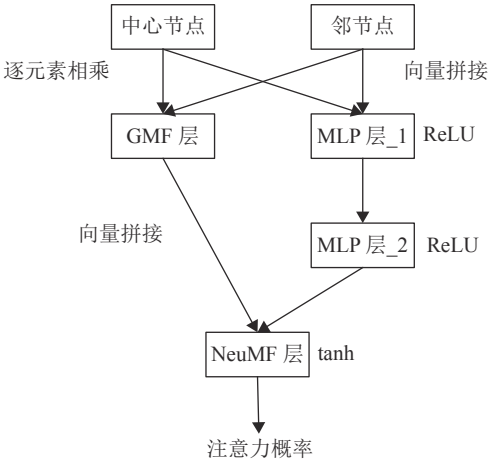

图 2 改进的神经协同过滤算法实现注意力概率挖掘

Fig. 2 Improved attention probability mining realized by neural collaborative filtering algorithm

1.2.2 图卷积层

一次图卷积操作得到的1阶邻居信息，在节点数量较少的情况下，无法充分体现节点间的依赖关系。为解决该问题，图卷积过程使用多层隐藏层进行训练，使用多层邻居的信息，实现对高阶邻域结构信息的捕获。本文设计的图神经网络通过多层图卷积的堆叠将节点向量特征构造为大小为h的向量，该向量用于表示节点与其邻节点的联系。每个节点特征描述在每一个图卷积层上，将图映射到频率空间，在频率空间进行卷积操作之后，再将其转换回节点空间，公式表示如下：

$$\boldsymbol{X}^{(l+1)} = \sigma(\widetilde{\boldsymbol{D}}^{-\frac{1}{2}}\widetilde{\boldsymbol{A}}\widetilde{\boldsymbol{D}}^{-\frac{1}{2}}\boldsymbol{X}^{(l)}\boldsymbol{W}^{(l)}) \tag{3}$$

式中：$\boldsymbol{X}^{(l)}$为第l层节点矩阵；$\widetilde{\boldsymbol{A}}$为引入的节点自连接特征，$\widetilde{\boldsymbol{A}} = \boldsymbol{A} + \boldsymbol{I}$；$\widetilde{\boldsymbol{D}}$为$\widetilde{\boldsymbol{A}}$的度数矩阵，其元素$\widetilde{d}_{ii} = \sum_j^n \widetilde{a}_{ij}$；$\sigma$为ReLU激活函数；$\boldsymbol{W}^{(l)}$为上一层特征$\boldsymbol{X}^{(l-1)}$的权值矩阵。此外，应用一个非线性函数来对当前层的隐藏节点特征属性进行更新，矩阵更新如式（4）所示：

$$\boldsymbol{X}^{(l)} = \sigma(\overline{\boldsymbol{A}}\boldsymbol{X}^{(l-1)}\boldsymbol{W}^{(l)}) \tag{4}$$

式中，$\overline{\boldsymbol{A}} = \boldsymbol{D}^{-\frac{1}{2}}\boldsymbol{A}\boldsymbol{D}^{-\frac{1}{2}}$为标准化邻接矩阵，为了更好地将上述图神经网络模型用于僵尸网络图特征学习，本文使用基于随机游走的标准邻接矩阵$\overline{\boldsymbol{A}} = \boldsymbol{D}^{-1}\boldsymbol{A}$进行归一化。基于随机游走的标准邻接矩阵能更好地利用P2P僵尸网络拓扑结构具有的混合分布属性，并使得仅包含源节点度的标准邻接矩阵和与之相对应的概率变换矩阵保持一致。同时，本文还设计了一个单独的线性变换层来映射最后一层的预测输入，线性变化如式（5）所示：

$$\boldsymbol{X}^{(l)} = \sigma(\boldsymbol{X}^{(l-1)}\boldsymbol{U}^{(l)} + \sigma(\overline{\boldsymbol{A}}\boldsymbol{X}^{(l-1)}\boldsymbol{W}^{(l)})) \tag{5}$$

式中，$\boldsymbol{U}^{(l)}$为第l层的可学习变换矩阵。经过l层堆叠图卷积神经网络后，每个节点的最终特征属性将包含L-hop邻域内有用的局部属性，输入到线性层中进行线性变换。

1.3 节点分类模块

节点特征属性经过线性变换后，再映射到分类函数进行最后的节点分类，本文选用SoftMax分类函数判断节点是否在僵尸网络中。SoftMax分类器在机器学习中有非常广泛的应用，每个节点的SoftMax值S_i为：

$$S_i = \frac{\mathrm{e}^i}{\sum_j \mathrm{e}^j} \tag{6}$$

式中，S_i为SoftMax分类器对输入的节点是否存在于僵尸网络内的判定值，e为自然常数。

通过最小化损失函数，使神经网络模型达到收敛状态，减少模型预测值的误差。本文采用交叉熵作为损失函数计算单次训练的损失值。交叉熵损失函

数通过缩小两个概率分布的差异，使得预测概率分布尽可能达到真实概率分布[25]，计算式如下：

$$L = -[y \cdot \lg(\hat{y}) + (1-y) \cdot \lg(1-\hat{y})] \quad (7)$$

式中：L为损失熵值；$\hat{y}$为模型预测样本是正例的概率；y为样本标签，如果样本属于正例则其取值为1，否则取值为0。

2　实验评估

2.1　数据来源

为了更好地模拟真实的网络环境，本文采用ISCX–Bot–2014僵尸网络数据集，该数据集为了保证僵尸网络符合真实环境的情况，混合了ISOT dataset、ISCX 2012 IDS dataset、Botnet traffic generated by the malware capture facility project的子集。ISCX–Botnet–2014数据集通用性强，包含了已知的多种P2P僵尸网络，同时，在构造数据集的过程中采用的都是真实的僵尸网络流量轨迹，以保证数据集真实性。该数据集分为训练集和测试集，训练数据集大小为5.3 GB，测试数据集大小为8.5 GB，测试集包含训练集没有的多种僵尸网络，可用于评价学习模型对未知僵尸网络的检测效果。

2.2　评估指标

为了分析模型在不同情况下的检测效果，本文采用准确率（ACC）、F1值（F1–score）、误报率（FPR）、漏报率（FNR）4种度量标准作为评价指标。准确率指正确判别僵尸网络节点占总体节点数的比例；F1–score是分类问题的一个衡量指标，是精确率和召回率的加权调和平均数，最大为1，最小为0；误报率用于评估正常流量误报为僵尸流量的概率；漏报率用于评估僵尸流量误报为正常流量的概率。4种指标的具体计算式如式（8）～（11）所示：

$$P_{\mathrm{acc}} = \frac{V_{\mathrm{TP}} + V_{\mathrm{TN}}}{V_{\mathrm{TP}} + V_{\mathrm{TN}} + V_{\mathrm{FP}} + V_{\mathrm{FN}}} \quad (8)$$

式中，P_{acc}为准确率，V_{TP}表示正样本判断为正向的概率，V_{TN}表示负样本判断为负向的概率，V_{FP}表示负样本判断为正向的概率，V_{FN}表示正样本判断为负向的概率。

$$F_1 = 2 \cdot \frac{P_{\mathrm{precision}} \cdot P_{\mathrm{recall}}}{P_{\mathrm{precision}} + P_{\mathrm{recall}}} \quad (9)$$

式中：$P_{\mathrm{precision}}$为精确率（precision, PPV），指检测为僵尸节点样本中实际也为僵尸节点的比例；P_{recall}为召回率（recall），指所有僵尸节点中被判为僵尸节点的比例。

$$P_{\mathrm{FPR}} = \frac{V_{\mathrm{FP}}}{V_{\mathrm{FP}} + V_{\mathrm{TN}}} \quad (10)$$

式中，P_{FPR}为误报率。

$$P_{\mathrm{FNR}} = \frac{V_{\mathrm{FN}}}{V_{\mathrm{TP}} + V_{\mathrm{FN}}} \quad (11)$$

式中，P_{FNR}为漏报率。

2.3　实验参数和内容

2.3.1　实验环境

本文模型输入为多个特征图，特征提取过程需要良好的硬件运算性能。实验环境配置如下：采用PyTorch作为神经网络框架；计算机硬件配置CPU为i5−10400f 6核，16 GB内存，显卡为NVIDIA GTX 1660s，搭载Windows10专业版64位操作系统，编译环境为python3.8，编译器采用PyCharm。

2.3.2　参数配置

本文设计的GNN模型输入为不包含任何流量协议特征的特征图，层与层之间的非线性激活函数采用ReLU函数，并且在每一层输出后加上偏差向量，设置所有层的嵌入大小为32，最后一层作为节点输出的线性层。本文使用Adam优化器[26]对训练模型进行优化。Adam优化算法相关参数设置如下：

P_l指学习速率或步长，更大的值在速率校正之前会加快初始学习速度，较小的值在模型训练期间降低学习速度，本文模型中设置为0.005；$P_{\beta 1}$为第1次估计的指数衰减率，本文模型中设置为0.9；$P_{\beta 2}$为第2次估计的指数衰减率，在稀疏梯度问题上，其取值应该接近1.0，本文模型中设置为0.999。P_ε为一个非常小的数字，可以防止任何情况下出现分母为0，保证算法稳定，本文模型中设置其为1e − 08。此外，还需设置与Adam算法无直接关系的参数$V_w = 5\mathrm{e}-4$，该参数的作用是L2正则化，表示当前可学习参数p的权值衰减；g_t为待更新的学习参数p的偏导数，公式如下：

$$g_t = g_t + (p \cdot V_w) \quad (12)$$

2.3.3　实验内容

为了从多个角度对本文提出的方法进行评估，根据以下因素设置了对比实验。

1）为研究GNN模型层数对学习训练检测效果的影响，本文采用包含2、4、8、12层的图卷积层模型进行对比学习验证。为研究训练集中僵尸节点规模大小对检测未知小型僵尸网络效果的影响，本文在包含100、1 000、10 000僵尸网络节点的训练集上进行模型训练的对比实验。

2）本文方法与其他两类具有代表性的检测方法进行对比实验，并考虑训练集中僵尸节点规模为100、1 000、10 000对检测性能的影响。对比方法是基于CNN和LSTM的深度学习检测方法（CNN_LSTM）[8]、基于SOM的检测方法[13]。

2.4 实验结果与分析

本文使用第2.2节提到的4项评估指标在不同图卷积层层数、不同僵尸网络节点规模下进行对比实验，结果如表1所示。4项指标中，F1值能反映模型的稳定性，ACC值能准确反映预测结果的准确性，因此，根据表1中F1和ACC两项指标绘制折线图，如图3、4所示。从表1和图3、4可以看出：图卷积层层数一致时，在更大规模僵尸网络社区上训练的模型检测效果明显优于小规模僵尸节点训练得到的模型，说明训练样本包含的僵尸网络规模大小对模型训练影响较大。同时，模型图卷积层层数在4层以上时有更好的图卷积效果，说明在深层图卷积模型上稳定性更好。

表 1 不同深度及不同僵尸节点规模条件下模型实验结果

Tab. 1 Experimental results of the model at different depths and different bot node sizes

图卷积层层数	100个僵尸节点				1 000个僵尸节点				10 000个僵尸节点			
	FPR/%	FNR/%	ACC/%	F1/%	FPR/%	FNR/%	ACC/%	F1/%	FPR/%	FNR/%	ACC/%	F1/%
2	10.00	76.00	57.00	35.82	5.30	74.20	60.25	39.36	0.914	73.24	62.925	41.92
4	7.00	62.00	65.50	52.41	6.10	60.10	66.90	54.66	0.513	32.24	82.63	80.54
8	3.00	36.00	80.50	76.65	1.10	31.20	83.85	80.99	0.231	11.90	93.94	93.56
12	2.00	14.00	92.00	91.49	0.30	11.60	94.05	93.69	0.009	1.82	99.09	99.08

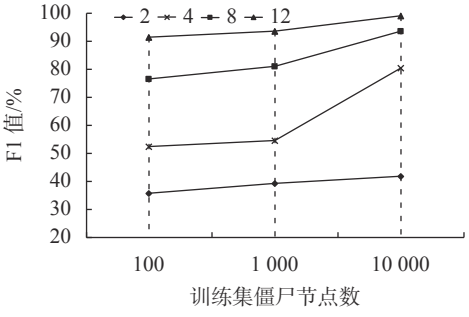

图 3 不同层数图神经网络模型F1值

Fig. 3 F1-score on graph neural network model with varying number of layers

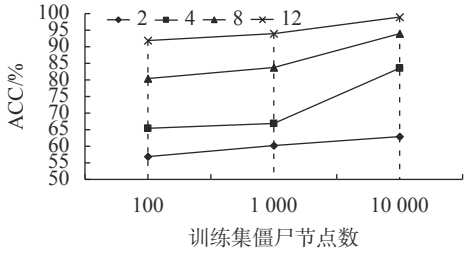

图 4 不同层数图神经网络模型ACC

Fig. 4 ACC on graph neural network model with varying number of layers

本文方法与其他方法的对比结果如表2所示。将能反映模型稳定性和预测结果准确性的F1和ACC指标绘制为折线图，如图5、6所示。从表2和图5、6可以看出，在训练集包含僵尸节点数量较小时，本文方法的F1值和检测准确率ACC能达到90%以上，说明本文方法的稳定性优于其他两类对比方法；在训练集包含僵尸节点数量较大时，3类方法都能达到较高的检测准确率，但是本文方法的误报率和漏报率明显低于其他两类方法，说明增加训练集中僵尸节点数量对本文所提模型训练效果提升更大。

表 2 不同模型检测结果

Tab. 2 Detection results on different models

模型	100个僵尸节点				1 000个僵尸节点				10 000个僵尸节点			
	FPR/%	FNR/%	ACC/%	F1/%	FPR/%	FNR/%	ACC/%	F1/%	FPR/%	FNR/%	ACC/%	F1/%
CNN_LSTM	2.00	35.00	81.33	78.33	0.50	19.10	90.19	89.78	0.060	14.33	92.81	92.25
SOM	2.00	30.00	83.92	81.28	0.20	15.70	92.05	91.38	0.080	5.45	97.24	97.16
本文方法	2.00	14.00	92.00	91.49	0.30	11.60	94.05	93.69	0.009	1.82	99.09	99.08

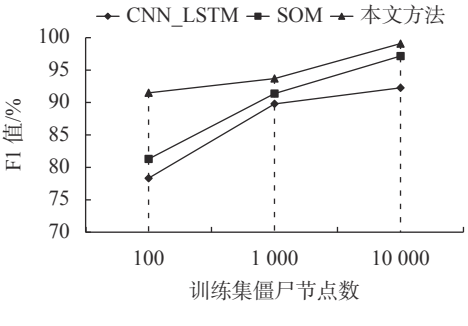

图 5 不同模型的F1值

Fig. 5 F1-score of contrastive experiments on different models

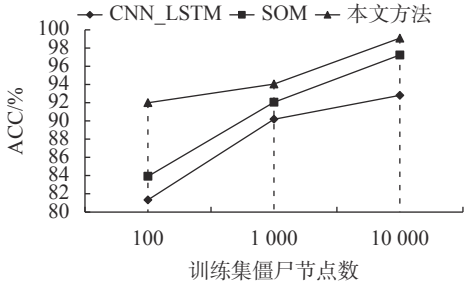

图 6 不同模型的ACC

Fig. 6 ACC of contrastive experiments on different models

3　总结与展望

本文提出一种基于图神经网络的P2P僵尸网络检测模型，采用图融合方法将生成多个特征图融合后作为GNN模型的输入，引入注意力机制作为节点状态更新函数，结合多个图卷积层的堆叠实现对交互特征的降维抽取和对高阶结构信息的挖掘。相比基于CNN_LSTM和SOM等算法的僵尸网络检测方法，本文方法的特征学习只针对节点交互特征以及网络拓扑结构的信息，不需要对流量协议特征进行提取，因此，可对加密、采用混淆技术的僵尸网络进行检测。实验结果表明，对P2P僵尸网络节点的检测有效且准确率在一定程度上优于其他算法，训练集中包含合适的僵尸节点数量能更有利于模型学习节点间的交互特征，同时，深层模型具有更好的检测准确率和更低的误报率。现阶段的本文方法基于空间层次进行检测，在未来的研究工作中，将重点研究基于时序和空间两个层次的检测方法，更有效地对节点特征进行挖掘学习。

参考文献：

[1] 国家计算机网络应急技术处理协调中心(CNCERT/CC).2020年中国互联网网络安全报告[EB/OL].[2021–08–01].https://www.cert.org.cn/publish/main/8/2021/20210721130944504525772/20210721130944504525772_.html.

[2] Wu Di,Cui Xiang,Liu Qixu,et al.Research on ubiquitous botnet[J].Netinfo Security,2018(7):16–28.[吴迪,崔翔,刘奇旭,等.泛在僵尸网络发展研究[J].信息网络安全,2018(7):16–28.]

[3] Chen Xingshu,Zeng Xuemei,Wang Wenxian,et al.Big data analytics for network security and intelligence[J].Advanced Engineering Sciences,2017,49(3):1–12.[陈兴蜀,曾雪梅,王文贤,等.基于大数据的网络安全与情报分析[J].工程科学与技术,2017,49(3):1–12.]

[4] Algelal Z M,Ghani Aldhaher E A,Abdul–Wadood D N,et al.Botnet detection using ensemble classifiers of network flow[J].International Journal of Electrical and Computer Engineering (IJECE),2020,10(3):2543.

[5] Wu Di,Fang Binxing,Cui Xiang,et al.BotCatcher:Botnet detection system based on deep learning[J].Journal on Communications,2018,39(8):18–28.[吴迪,方滨兴,崔翔,等.BotCatcher:基于深度学习的僵尸网络检测系统[J].通信学报,2018,39(8):18–28.]

[6] Niu Weina,Zhang Xiaosong,Sun Enbo,et al.Two stage P2P botnet detection method based on flow similarity[J].Journal of University of Electronic Science and Technology of China,2017,46(6):902–906.[牛伟纳,张小松,孙恩博,等.基于流相似性的两阶段P2P僵尸网络检测方法[J].电子科技大学学报,2017,46(6):902–906.]

[7] Wang Wei,Zhu Ming,Zeng Xuewen,et al.Malware traffic classification using convolutional neural network for representation learning[C]//Proceedings of the 2017 International Conference on Information Networking (ICOIN).Da Nang:IEEE,2017:712–717.

[8] Luo Fuhua,Zhang Aixin.Botnet detection technology based on deep learning[J].Communications Technology,2020,53(1):174–179.[罗扶华,张爱新.基于深度学习的僵尸网络检测技术研究[J].通信技术,2020,53(1):174–179.]

[9] Zheng Li,Li Zhenpeng,Li Jian,et al.AddGraph:Anomaly detection in dynamic graph using attention-based temporal GCN[C]//Proceedings of the Twenty-Eighth International Joint Conference on Artificial Intelligence.Macao:International Joint Conferences on Artificial Intelligence Organization,2019:4419–4425.

[10] Xie Kun,Li Xiaocan,Wang Xin,et al.Graph based tensor recovery for accurate Internet anomaly detection[C]//Proceedings of the IEEE Conference on Computer Communications (IEEE INFOCOM 2018).Honolulu:IEEE,2018:1502–1510.

[11] Deng Ailin,Hooi B.Graph neural network-based anomaly detection in multivariate time series[EB/OL].[2021–08–01].https://arxiv.org/abs/2106.06947

[12] Eswaran D,Faloutsos C,Guha S,et al.SpotLight:Detecting anomalies in streaming graphs[C]//KDD'18:Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining.New York,ACM:2018:1378–1386.

[13] Chowdhury S,Khanzadeh M,Akula R,et al.Botnet detection using graph-based feature clustering[J].Journal of Big Data,2017,4:14.

[14] Lagraa S,François J,Lahmadi A,et al.BotGM:Unsupervised graph mining to detect botnets in traffic flows[C]//Proceedings of the 2017 1st Cyber Security in Networking Conference (CSNet).Rio de Janeiro:IEEE,2017:1–8.

[15] Wang Wei,Wang Yang,Tan Xinlu,et al.Botcapturer:Detecting botnets based on two-layered analysis with graph anomaly detection and network traffic clustering[J].International Journal of Performability Engineering,2018,14(5):1050–1059.

[16] Wang Wei,Shang Yaoyao,He Yongzhong,et al.BotMark:Automated botnet detection with hybrid analysis of flow-based and graph-based traffic behaviors[J].Information Sciences,2020,511:284–296.

[17] Bronstein M M,Bruna J,LeCun Y,et al.Geometric deep learning:Going beyond euclidean data[J].IEEE Signal Processing Magazine,2017,34(4):18–42.

[18] Monti F,Boscaini D,Masci J,et al.Geometric deep learning on graphs and manifolds using mixture model CNNs[C]// Proceedings of the 2017 IEEE Conference on Computer Vision and Pattern Recognition.Honolulu:IEEE,2017:5425–5434.

[19] Zhou Jie,Cui Ganqu,Hu Shengding,et al.Graph neural networks:A review of methods and applications[J].AI Open,2020,1:57–81.

[20] Liu Jie,Li Xiwang.Anomaly detection algorithm in industrial control network based on graph neural network[J].Computer Systems & Applications,2020,29(12):234–238.[刘杰,李喜旺.基于图神经网络的工控网络异常检测算法[J].计算机系统应用,2020,29(12):234–238.]

[21] Qu Qiang,Yu Hongtao,Huang Ruiyang.Spammer detection technology of social network based on graph convolution network[J].Chinese Journal of Network and Information Security,2018,4(5):39–46.[曲强,于洪涛,黄瑞阳.基于图卷积网络的社交网络Spammer检测技术[J].网络与信息安全学报,2018,4(5):39–46.]

[22] Guo Jiayan,Li Ronghua,Zhang Yan,et al.Graph neural network based anomaly detection in dynamic networks[J].Journal of Software,2020,31(3):748–762.[郭嘉琰,李荣华,张岩,等.基于图神经网络的动态网络异常检测算法[J].软件学报,2020,31(3):748–762.]

[23] Kipf T N,Welling M.Semi-supervised classification with graph convolutional networks[EB/OL].[2021–08–01].https://arxiv.org/abs/1609.02907.

[24] He Xiangnan,Liao Lizi,Zhang Hanwang,et al.Neural collaborative filtering[C]//WWW'17:Proceedings of the 26th International Conference on World Wide Web.Perth Australia.Perth:International World Wide Web Conferences Steering Committee,2017:173–182.

[25] Shannon C E.A mathematical theory of communication[J].The Bell System Technical Journal,1948,27(3):379–423.

[26] Kingma D P,Ba J.Adam:A method for stochastic optimization[EB/OL].[2021–08–01].https://arxiv.org/abs/1412.6980.

（编辑　赵　婧）

引用格式: Lin Honggang,Zhang Yunli,Guo Nanxin,et al.P2P botnet detection method based on graph neural network[J].Advanced Engineering Sciences,2022,54(2):65–72.[林宏刚,张运理,郭楠馨,等.基于图神经网络的P2P僵尸网络检测方法[J].工程科学与技术,2022,54(2):65–72.]