

文章编号: 1006-3080(2025)02-0270-07

DOI: 10.14135/j.cnki.1006-3080.20240507001

基于 GraphSAGE-MGAT 的工控系统入侵检测方法

胡育鸣, 王华忠

(华东理工大学能源化工过程智能制造教育部重点实验室, 上海 200237)

摘要: 提出一种融合了图随机采样与聚合(GraphSAGE)和改进的图注意力网络(GAT)的工控入侵检测图神经网络算法, 以处理工控入侵检测中存在的特征种类多和数量大等复杂性。首先将入侵检测流量数据构建为图结构形式, 利用 GraphSAGE 采样和聚合邻居节点信息得到节点的 embedding 向量, 降低图结构空间复杂度, 提高对大量数据处理的效率。运用改进的多头图注意力机制, 丰富捕获的特征信息, 计算节点之间的相关性和重要性, 为各个节点分配相应权重, 提高分类精度。将该方法在工控数据集上验证, 实验结果表明, 该方法具有更好的时间效率以及更高的检测精度。

关键词: 工控系统; 入侵检测; 图随机采样与聚合; 图注意力网络; 图结构

中图分类号: TP309

文献标志码: A

工业控制系统(简称工控系统, ICS)广泛应用于能源、石化、交通等关键基础设施, 然而由于控制系统本身和运行管理等方面存在的漏洞, 造成工控系统被网络攻击的事件不断出现^[1]。标志性的事件就是 2010 年伊朗布什尔核电站受到恶意蠕虫 Stuxnet 的攻击^[2], 对伊朗的核计划造成重大打击。2017 年中东的一家能源工厂因施耐德 Triconex SIS 的零日漏洞遭到攻击, 标志着除了常规的控制外, 安全控制系统也成为攻击目标, 这种非对称攻击给 ICS 安全带来了更加严峻的挑战, 加强 ICS 安全保护变得十分紧迫。

入侵检测系统可以检测并识别各种类型的恶意攻击, 如病毒、蠕虫、木马、拒绝服务攻击等, 它通过监控网络流量、系统行为和异常模式, 可以识别并报告潜在的攻击活动, 帮助管理员及时采取措施应对威胁^[3]。由于深度学习在处理大量数据方面具有很好的性能, 很多研究者将其应用于入侵检测领域, 并取得了一定的成果^[4]。Li 等^[5]提出了一种基于多卷积神经网络(Multi-CNN)融合的深度学习入侵检测

方法, 根据相关性将特征数据分成 4 部分, 然后将一维特征数据转换成灰度图, 利用流量数据可视化的方法, 将 Multi-CNN 引入入侵检测问题, 得到 4 种结果中最好的一种。赵志达等^[6]提出一种结合了改进麻雀搜索算法(ISSA)和 LightGBM 的工控入侵检测算法, 引入离散数据处理方式, 改进了种群位置更新函数, 提高种群多样性来增强算法全局搜索能力。Alem 等^[7]针对入侵检测中误报率高的问题, 提出了一种通过决策系统(DMS)使用神经网络(NN)将基于规范的入侵检测系统(IDS)和基于 BI-ANomaly 的 IDS 相结合的方法, 该方法在检测中能够区分攻击与故障。沈华等^[8]针对网络攻击中类型多样、分布不均导致基于机器学习的入侵检测方法泛化能力差的问题, 首先提出基于随机子空间的入侵检测模型(BAVE-ELM); 然后以 BAVE-ELM 作为一个子分类器, 提出基于自适应集成的网络入侵检测模型; 最后, 引入对抗训练, 提出了基于对抗机器学习的入侵检测模型, 在节约计算资源的同时提高了检测模型的泛化能力。尽管上述方法在入侵检测精度方面

收稿日期: 2024-05-07

基金项目: 国家自然科学基金(61973119)

作者简介: 胡育鸣(1999—), 男, 浙江丽水人, 硕士生, 主要研究工控信息安全。E-mail: Y30210949@mail.ecust.edu.cn

通信联系人: 王华忠, E-mail: hzwang@ecust.edu.cn

引用本文: 胡育鸣, 王华忠. 基于 GraphSAGE-MGAT 的工控系统入侵检测方法[J]. 华东理工大学学报(自然科学版), 2025, 51(2): 270-276.

Citation: HU Yuming, WANG Huazhong. Intrusion Detection Method of Industrial Control System Based on GraphSAGE-MGAT[J]. Journal of East China University of Science and Technology, 2025, 51(2): 270-276.

具有很好的效能,但是由于工控入侵检测数据量大,特征种类多,这些算法训练时资源耗费大,时间长。此外,上述方法只考虑了在表格数据格式下节点的属性信息,忽略了数据之间内在的交互信息。在ICS中,许多设备之间存在复杂的相互关系,这可以为入侵检测提供有价值的补充信息。图形结构正好可以表示数据对象之间的这种关系,通过将数据对象构建成图,就能利用其所包涵的结构信息,更好地检测数据中的异常。

图卷积神经网络(GCN)具有强大的建模能力,很多研究者将其应用于大数据分类研究,并取得了一定成果。文献[9]引入一种各向异性图卷积网络(AGCN),通过端到端方式学习有效的表示,对图结构数据进行半监督节点分类,AGCN可以通过共同训练和自训练集成到现有的基于图的卷积网络中进行半监督学习,在多个数据集中平均准确率可达83%。文献[10]利用异构信息网络和外生知识的表征学习,引入外生知识构建文本加权异构信息网络(HINT),提出一种构建了异构信息网络的HINT-GCN新型文本分类方法,分类精准度最高达到98.24%。文献[11]提出了一种多项式图卷积(PGCN)的方法,利用一个单一的PGCN层解决主流卷积算法中多个卷积层堆叠导致信息流动造成偏差的问题。

基于GCN在处理大量数据分类问题方面的强大能力,可以将其用于解决工控入侵检测问题,将网络数据流量看作一个复杂的图结构,通过节点分类进行入侵检测。但是,由于GCN保留了图全局结构信息,在处理真实的工业数据时,因为数据量庞大,导致入侵检测训练花费大量时间,降低了检测的时效性。同时,因为数据被构建为一个图结构,在GCN训练过程中,会采集到测试集或者验证集中的样本,降低了检测的准确性。图随机采样与聚合(GraphSAGE)引入采样机制,对邻居节点进行采样聚合[12],具有以下优势:(1)解决了GCN训练时需要知道全图信息的问题;(2)减少了训练数据量,降低了CPU和GPU的负担,提升了训练速度;(3)模型训练参数与图结构的节点个数无关,使得GraphSAGE能够处理结构变化的图;(4)既能处理有监督任务,也能处理无监督任务。在图结构中,每个节点之间的关系并不是一模一样的,图注意力网络(GAT)引入了注意力机制,将网络中每个节点之间的关系用权重表示,能够更好地泛化和表达节点特征[13],提高分类的准确性。

基于GraphSAGE和GAT各自的优点,本文提

出了一种融合GraphSAGE采样和GAT注意力机制的GraphSAGE-GAT算法,针对GCN算法中处理大量数据时训练时间长的的问题,使用采样方式,降低了训练复杂度,同时引入注意力机制,赋予节点之间相关权重系数,提高分类精准度,并针对实际数据集中特征值种类多,导致捕获特征信息不够准确的问题,改进了注意力评分机制,提出GraphSAGE-MGAT算法。将本方法运用于入侵检测中,并在新加坡科技大学的SWaT工业数据集[14]上进行实验验证。

1 基本理论

1.1 GCN

GCN主要通过对相邻节点信息之间的传播和聚合来实现,图神经网络处理的结构数据在欧式空间中通常是不规则的网络结构[15],可以将图结构定义为 $G=(V, E, A)$,在图 G 中, V 代表所有节点的集合, E 代表所有相连边的集合, A 表示节点之间相互关系的邻接矩阵,一般为一个 $N \times N$ 的矩阵。图结构有两个维度:时间和空间,在空间维度上,不同类型的节点和边组成了不同的空间结构图,比如有向图、权重图、边信息图、节点异构图等;在时间维度上,引入的节点随着时间变化而变化,形成了时空图。本文定义一个无向图,其中有 N 个节点,每个节点都有自己的特征值,节点特征组成 $N \times D$ 维的特征矩阵 H ,节点关系组成1个 $N \times N$ 维的邻接矩阵 A ,则在GCN训练中,每一层的传递公式为:

$$H^{(l+1)} = \text{softmax}(\tilde{D}^{-\frac{1}{2}} \tilde{A} \tilde{D}^{-\frac{1}{2}} H^{(l)} W^{(l)}) \quad (1)$$

其中, $H^{(l)}$ 表示第 l 层的节点特征矩阵; $\tilde{A} = A + I$, I 表示单位矩阵,表明在卷积操作中,需要注意上层节点自身的特征值对下层节点的影响; $\tilde{D}$ 是 $\tilde{A}$ 的度矩阵; $W^{(l)}$ 则是需要训练的参数矩阵。

1.2 GraphSAGE

在大型网络数据集中,使用GCN训练需要已知所有节点状态,这个条件对于真实的网络是不现实的,而且使用GCN训练时,每一层节点的embedding向量将会呈指数型增长,产生庞大的计算量。为了克服这个问题,GraphSAGE使用随机采样的方式,每个节点保留固定数量的邻接节点,工作流程如下:

(1)对每个顶点采样一定数量的邻接节点作为待聚合信息的相关节点,假设采样邻接节点数量为 m ,若节点的邻接节点数量大于 m ,则采取无放回抽样;若节点的邻接节点数量小于 m ,则采取有放回的抽样方式,直到取出 m 个邻接节点;

(2)根据聚合函数聚合邻接节点所蕴含的信息,得到图结构中顶点的向量表示。

在第 k 层时,对于顶点 v ,首先用顶点 v 的邻接节点的 $k-1$ 层的 embedding 来产生其邻接节点的第 k 层聚合(表示为 $h_{N(v)}^k$),之后将 $h_{N(v)}^k$ 和顶点 v 的第 $k-1$ 层聚合(表示为 h_v^{k-1})进行拼接(Concat),经过一个非线性变换产生顶点 v 的第 k 层 embedding 表示,公式可表示为:

$$h_{N(v)}^k = \text{aggregate}(\{h_v^{k-1}, \forall v \in N(v)\}) \quad (2)$$

$$h_v^k = \sigma(W^k \times \text{concat}(h_v^{k-1}, h_{N(v)}^k)) \quad (3)$$

其中, k 为聚合层数, $N(v)$ 表示对顶点 v 的邻接节点进行平均采样, σ 为激活函数, W^k 为权值矩阵, GraphSAGE 的流程图如图 1 所示。

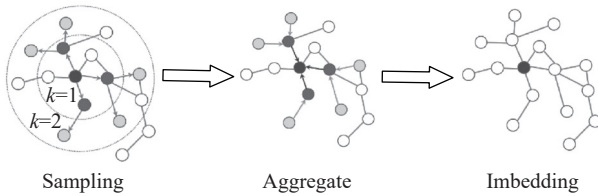


图 1 GraphSAGE 流程图
Fig. 1 Flowchart of GraphSAGE

1.3 GAT

相比于普通的 GNN, GAT 引入了注意力机制和非线性特征转换,能够更好地表达节点之间的特征关系。首先,对于顶点 v ,计算其和邻接节点 c 之间的相似系数 e_{vc} :

$$e_{vc} = \alpha([Wh_v][Wh_c]), c \in N_v \quad (4)$$

式中, W 是可学习权重矩阵, h_v 和 h_c 分别表示顶点 v 和顶点 c 的输入特征,之后,对其进行归一化处理:

$$a_{vc} = \frac{\exp(\text{LeakyReLU}(e_{vc}))}{\sum_{k \in N_v} \exp(\text{LeakyReLU}(e_{vk}))} \quad (5)$$

式中, LeakyReLU 为激活函数, N_v 表示节点 v 的邻居节点的集合,根据计算的注意力系数,将特征值加权求和:

$$h_v' = \sigma\left(\sum_{c \in N_v} a_{vc} Wh_c\right) \quad (6)$$

2 改进的 GraphSAGE-MGAT 算法

GraphSAGE 算法虽然解决了 GCN 算法运算量大、每层节信息呈指数增长的问题,但同时也导致了训练结果相比 GCN 全局训练得到的准确率下降的

问题。针对此问题,本文将图注意力机制引入 GraphSAGE 算法,提出一种融合了 GraphSAGE 和 GAT 的 GraphSAGE-GAT 算法,该算法在提高了检测效率的同时,兼顾了检测的准确性。

但是,传统的注意力函数将会带来以下问题:图注意力系数仅基于单一相似度计算,导致特征向量无法充分表达节点的多特征信息,影响检测的准确性,故提出一种基于多头注意力 (Multi-Head Attention) 机制的多头图注意力机制,将多组计算得到的图注意力系数输出拼接在一起,得到的注意力系数从多方面特征关系描述节点相似度,使得分类更加准确,改进算法记作 GraphSAGE-MGAT 算法。

多头注意力机制是将独立学习得到的多组不同的线性投影变换查询范围 (Query)、键 (Key) 和值 (Value),然后,将变换后的查询范围、键和值进行注意力汇聚,再输出拼接在一起,并通过一个可学习的线性投影进行变换,得到最终输出。多头注意力机制的流程如图 2 所示。

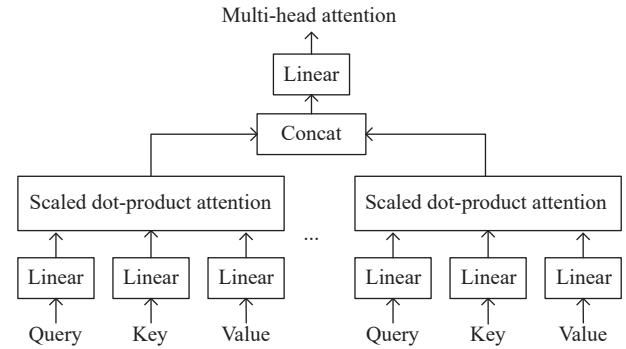


图 2 多头注意力机制流程图
Fig. 2 Flowchart of the multi-head attention mechanism

图 2 中,查询范围、键、值的初始值由输出向量 X 与对应的权重矩阵 W^q 、 W^k 、 W^v 分别乘积得到:

$$\text{Query} = W^q X \quad (7)$$

$$\text{Key} = W^k X \quad (8)$$

$$\text{Value} = W^v X \quad (9)$$

将多头注意力机制引入 GAT 中,则对于顶点 v ,计算多个其和邻接节点 c 之间的相似系数:

$$e_{vc}^{h-p} = \alpha([W^{h-p} h_v][W^{h-p} h_c]), c \in N_v \quad (10)$$

其中, $h-p$ 表示第几头图注意力机制, W^{h-p} 为线性变换权重矩阵。

进行归一化处理:

$$a_{vc}^{h-p} = \frac{\exp(\text{LeakyReLU}(e_{vc}^{h-p}))}{\sum_{k \in N_v} \exp(\text{LeakyReLU}(e_{vk}^{h-p}))} \quad (11)$$

每头注意力机制下的嵌入式表示为:

$$h_v^{h-p} = \sigma \left(\sum_{c \in N_v} a_{vc}^{h-p} \mathbf{W}^{h-p} h_c \right) \quad (12)$$

将每头注意力机制得到的嵌入式表示进行拼接, 即可得到多头图注意力机制下, 经过聚合之后的嵌入表示:

$$h'_v = \rho \left[\text{ELU} \left(h_v^{h-p} \right) \right] \quad (13)$$

其中, ρ 表示进行拼接计算, ELU 为激活函数。GraphSAGE-MGAT 算法的伪代码如表 1 所示, GraphSAGE-MGAT 算法的模型结构如图 3 所示。

表 1 改进的 GraphSAGE-MGAT 算法

Table 1 Improved GraphSAGE-MGAT algorithm

Input: Graph(V, E); Input feature $\{x_v, \forall v \in N(v)\}$; Number of floors K ;
 Weight matrix: $\mathbf{W}^k$; Nonlinear activation function: σ ; Differentiable
 aggregate function: Aggregate; Adjacent function N ; $v \rightarrow 2^v$

Output: z_v

$h_v^0 \leftarrow x_v, \forall v \in V$

for $k = 1 \dots K$ do

for $v \in V$ do

$h_{N(v)}^k \leftarrow \text{aggregate}(\{h_v^{k-1}, \forall v \in N(v)\})$

$e_{vc}^{h-p} = \alpha([\mathbf{W}^{h-p} h_v][\mathbf{W}^{h-p} h_c]), c \in N_v$

$a_{vc}^{h-p} = \frac{\exp(\text{LeakyReLU}(e_{vc}^{h-p}))}{\sum_{k \in N_v} \exp(\text{LeakyReLU}(e_{vk}^{h-p}))}$

$h_v^{h-p} = \sigma \left(\sum_{c \in N_v} a_{vc}^{h-p} \mathbf{W}^{h-p} h_c \right)$

$h'_v = \rho[\text{ELU}(h_v^{h-p})]$

$h_v^k \leftarrow \sigma(\mathbf{W}^k * h'_v * \text{concat}(h_v^{k-1}, h_{N(v)}^k))$

end

$h_v^k \leftarrow \frac{h_v^k}{\|h_v^k\|_2}, \forall v \in V$

3 基于 GraphSAGE-MGAT 算法的入侵检测模型

本文构建了基于 GraphSAGE-MGAT 算法的 ICS 入侵检测模型。具体步骤如下:

(1) 构建图结构。基于工控数据集构建图神经网络, 数据集中每条数据都包含了所有设备的状态信息和流量信息, 将数据集中的每条数据看作一个节点, 数据的每个值看作节点的一个特征, 依据数据间的关系构建边和邻接矩阵; 将数据集划分为训练集、验证集、测试集, 比例为 7 : 1 : 2;

(2) 参数初始化。初始化训练的参数, 确定迭代次数, 规定待优化的超参数的范围;

(3) 邻接节点采样。对每个节点的邻接节点进行固定数量的随机采样;

(4) 计算注意力机制权重。依据当前节点和所采样节点的相似系数, 计算两个节点间的多头注意力函数, 并进行归一化, 拼接得到新的注意力系数;

(5) 信息聚合。对节点信息进行聚合更新, 得到该节点新的 embedding 向量, 依据向量进行分类检测, 计算交叉熵函数, 更新权重系数;

(6) 判断, 交叉熵函数是否符合预期, 若符合, 停止迭代; 否则, 从步骤(2)再次开始迭代;

(7) 保存得到最优结果的超参数, 建立基于 GraphSAGE-MGAT 的入侵检测模型, 并在测试集上进行验证。入侵检测模型流程如图 4 所示。

其中, 交叉熵损失函数 $L(x, y)$ 表达如下:

$$L(x, y) = - \sum_{i=1}^C x_i \log y_i \quad (14)$$

式中, x_i 表示真实标签的第 i 个元素, y_i 表示模型预测 x 属于第 i 个类别的概率。然后通过反向传播算法, 计算模型参数对于损失的贡献, 得到损失函数的梯度:

$$\frac{\partial L}{\partial w} = \frac{2}{N} \sum_{i=1}^N x_i (y_i - y'_i) \quad (15)$$

$$\frac{\partial L}{\partial b} = \frac{2}{N} \sum_{i=1}^N (y'_i y_i) \quad (16)$$

式中, w 为特征权重, 表示模型特征的重要性; b 为偏置值, 表示模型的基准输出。使用梯度下降法更新参数 w 、 b :

$$w' = w - \eta \frac{\partial L}{\partial w} \quad (17)$$

$$b' = b - \eta \frac{\partial L}{\partial b} \quad (18)$$

式中, η 为学习率。

4 实验结果与分析

4.1 实验环境和数据集

本文实验在 Intel(R) Core(TM) i5-8300H CPU @ 2.30GHz 和 Windows10 64 位操作系统的设备上运行, 运行环境为 python 3.9。为验证本文所提方法的检测效果, 使用新加坡科技大学的 SWaT 数据集, 该数据集用于研究水处理系统中存在的网络攻击。SWaT 数据集包括 7 d 正常运行的实验数据和 4 d 受到攻击的实验数据, 数据集记录了实验期间 51 个传

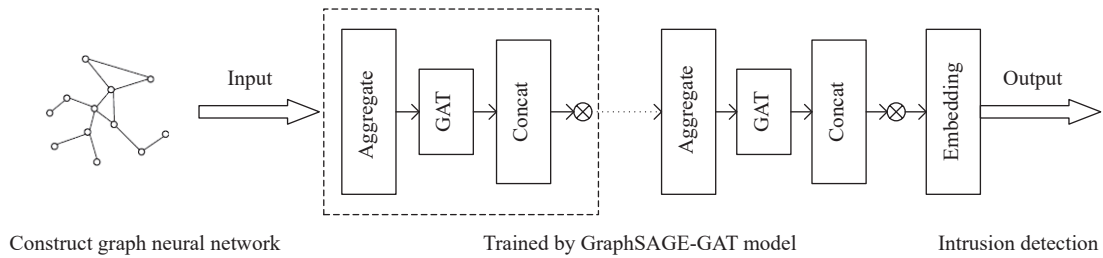


图 3 GraphSAGE-MGAT 算法的模型结构图

Fig. 3 Model structure diagram of GraphSAGE-MGAT algorithm

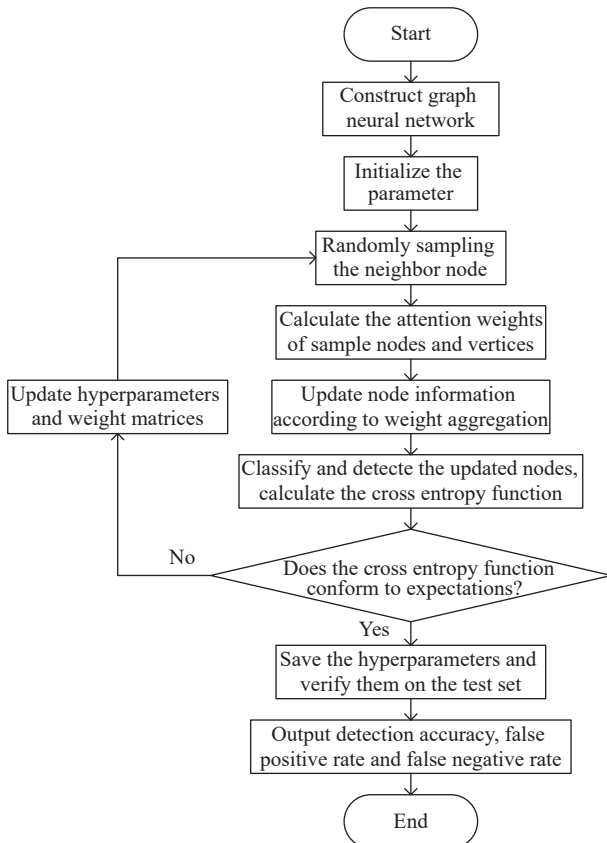


图 4 GraphSAGE-MGAT 入侵检测模型流程图

Fig. 4 Intrusion detection model flow chart of GraphSAGE-MGAT

传感器和执行器的参数。数据集共有 449918 条可用于分析的数据,其中正常样本数据 395297 条,受攻击样本数据 54620 条,受攻击类型如表 2 所示。

本文采用全部 449918 条数据作为实验数据,将数据集划分为训练集、测试集和验证集,其中训练集占 70%,为 314943 条;测试集占 20%,为 89984 条;验证集占 10%,为 44991 条。数据集的每个样本含有 51 个特征值和 1 个类别标签。

4.2 评价指标

本文运用 3 个评价指标来判断模型的性能。查准率(P)是指预测为正常数据中真实正常数据的比例,查全率(R)是指所有正常数据中检测出来的比例,调和平均值($F1$)是将两者看作同等重要, $F1$ 值越

表 2 SWaT 攻击类型

Table 2 Types of SWaT attack

Type of attack	Attack times
Single Stage Single Point(SSSP)	26
Single Stage Multi Point(SSMP)	4
Multi Stage Single Point(MSSP)	2
Multi Stage Multi Point(MSMP)	4

高,表示性能越好,相应的计算公式如下:

$$P = \frac{TP}{TP + FP} \quad (19)$$

$$R = \frac{TP}{TP + FN} \quad (20)$$

$$F1 = \frac{2 \times P \times R}{P + R} \quad (21)$$

其中, TP 表示实际正例,预测也是正例; FP 表示实际反例,预测是正例; FN 表示实际正例,预测是反例。

4.3 实验结果与分析

4.3.1 GraphSAGE-MGAT算法性能评估 为验证本文改进算法的性能,将使用原始注意力机制的 GraphSAGE-GAT 算法和使用多头注意力机制的 GraphSAGE-MGAT 算法与 SVM 算法、MLP 算法、GCN 算法、GraphSAGE 算法进行训练时间和准确率对比。在训练中,迭代次数为 200 次,批次设置为 32,学习率设为 0.001,激活函数采用 softmax,随机采样数不宜过大。经过实验得知,当随机采样量为 5 时,能够在检测效率和准确性上同时得到较优的结果,故本次实验采样数量固定为 5,优化器使用 Adam,梯度下降时采用 dropout 技术防止过拟合,损失函数用交叉熵函数,各个算法的训练时间和检测评估指标值如表 3 所示。

由表 3 可知,虽然 GCN 算法具有最高的查准率(98.81%),比 SVM 算法高了 3.43%,比 MLP 算法高出 2.34%,但其模型训练所花时间相比 SVM 算法多 2432 s,耗时增加了 85.12%;比 MLP 算法所花时间多 3525 s,耗时增加 199.8%。GraphSAGE 算法在训练

表 3 各个算法的训练时间和检测结果
Table 3 Training time and detection results of each algorithm

Algorithm	Training time/s	P/%	R/%	F1/%
SVM	2857	95.38	90.58	92.92
MLP	1764	96.47	93.03	94.72
GCN	5289	98.81	97.26	98.03
GraphSAGE	246	89.85	91.32	90.58
GraphSAGE-GAT	285	97.89	95.28	96.57
GraphSAGE-MGAT	296	98.13	96.85	97.49

效率上得到了很大的提升,相比 GCN 算法,时间缩短了 5043 s,所耗时间减少了 95.35%,但其查准率只有 89.85%,降低了 8.96%,损失了较多的准确率。GraphSAGE-GAT 算法在训练效率上同样得到提升,只比 GraphSAGE 算法多耗费 39 s,对比 GCN 算法,在准确度上只损失了 0.92%,而使用了多头图注意力机制的 GraphSAGE-MAGT 算法,在 GraphSAGE-GAT 算法基础上,查准率提升了 0.24%,F1 值提升了 0.92%。实验表明,本文算法很好地兼顾了入侵检测系统所需的效率性和准确性,更加适合进行在线的入侵检测模型更新。

4.3.2 GraphSAGE-MGAT算法与不同算法比较 为了更全面地评估本文算法的检测性能,将 GraphSAGE-MGAT 算法与文献 [16] 中的 CrossFuN 算法、文献 [17] 中的 Time2Event 算法、文献 [18] 中的 TPAD 算法、文献 [19] 中的 Kohonen-IDS 算法进行比对,以上算法都在工控数据集 SWaT 上进行了实验验证,对比结果如表 4 所示。

表 4 不同算法在工控数据集 SWaT 上的检测结果评分对比
Table 4 Comparison of detection results of different algorithms on industrial control data set SWaT

Algorithm	P/%	R/%	F1/%
CrossFuN	96.49	94.22	95.34
Time2Event	92.41	71.20	80.43
TPAD	92.52	92.00	92.26
Kohonen-IDS	96.26	98.82	96.18
GraphSAGE-GAT	97.89	95.28	96.57
GraphSAGE-MGAT	98.13	96.85	97.49

由表 4 可知,本文 GraphSAGE-MGAT 算法的 F1 值相比其他算法得到了显著提高,具体来说,相比 CrossFuN 算法提高了 2.15%,相比 Time2Event 算法提高了 17.06%,比 TPAD 算法提高了 5.23%,比

Kohonen-IDS 算法提高了 1.31%,表明该算法在入侵检测方面具有更好的性能。

5 结束语

本文针对工业入侵检测中数据量大,耗费时间长,数据集特征种类多,影响检测准确度的问题,提出了一种基于 GraphSAGE 和 GAT 结合的算法。利用随机节点采样的方式,降低训练负担,提升训练效率。引入了图注意力机制,通过学习节点之间的权重,使每个节点能更好地捕捉周围节点的特征信息。通过改进注意力评估函数,增强对节点特征信息的特征表达能力,提高了分类准确性。最后将本文算法在工控数据集 SWaT 上进行实验验证,表明该算法在大幅度提升检测效率的同时,同样具有较好的检测准确率。

参考文献:

[1] CONTI M, DONADEL D, TURRIN F. A survey on industrial control system testbeds and datasets for security research[J]. IEEE Communications Surveys & Tutorials, 2021, 23(4): 2248-2294.

[2] RAJA M A Z, NAZ H, SHOAIB M, et al. Design of back-propagated neurocomputing paradigm for Stuxnet virus dynamics in control infrastructure[J]. Neural Computing and Applications, 2022, 34(7): 5771-5790.

[3] DREWEK-OSSOWICKA A, PIETROŁAJ M, RUMIŃSKI J. A survey of neural networks usage for intrusion detection systems[J]. Journal of Ambient Intelligence and Humanized Computing, 2021, 12(1): 497-514.

[4] 刘奇旭, 陈艳辉, 尼杰硕, 等. 基于机器学习的工业互联网入侵检测综述 [J]. 计算机研究与发展, 2022, 59(5): 994-1014.

[5] LI Y, XU Y, LIU Z, et al. Robust detection for network intrusion of industrial IoT based on multi-CNN fusion[J]. Measurement, 2020, 154(2): 107450.

[6] 赵志达, 王华忠. 基于 ISSA-LightGBM 的工控入侵检测研究 [J]. 华东理工大学学报 (自然科学版), 2023, 49(5): 735-743.

[7] ALEM S, ESPES D, NANA L, et al. A novel bi-anomaly-based intrusion detection system approach for industry 4.0[J]. Future Generation Computer Systems, 2023, 145: 267-283.

[8] 沈华, 田晨, 郭森森, 等. 基于对抗性机器学习的网络入侵检测方法研究 [J]. 信息安全, 2023, 23(8): 66-75.

[9] MESGARAN M, HAMZA A B. Anisotropic graph convolutional network for semi-supervised learning[J]. IEEE

- Transactions on Multimedia, 2020, 23: 3931-3942.
- [10] LI H, YAN Y, WANG S, *et al.* Text classification on heterogeneous information network via enhanced GCN and knowledge[J]. *Neural Computing and Applications*, 2023, 35(20): 14911-14927.
- [11] PASA L, NAVARIN N, SPERDUTI A. Polynomial-based graph convolutional neural networks for graph classification[J]. *Machine Learning*, 2022, 111(4): 1205-1237.
- [12] ZHANG T, SHAN H R, LITTLE M A. Causal GraphSAGE: A robust graph method for classification based on causal sampling[J]. *Pattern Recognition*, 2022, 128: 108696.
- [13] 沈传鑫, 王永杰, 熊鑫立. 基于图注意力网络的 DNS 隐蔽信道检测 [J]. *信息安全学报*, 2023, 23(1): 73-83.
- [14] GOH J, ADEPU S, JUNEJO K N, *et al.* A Dataset to Support Research in the Design of Secure Water Treatment Systems[M]. [s.l.]: Springer International Publishing, 2017: 88-99.
- [15] WANG X, WANG Q. An abnormal traffic detection method using GCN-BiLSTM-Attention in the internet of vehicles environment[J]. *EURASIP Journal on Wireless Communications and Networking*, 2023, 2023(1): 1-20.
- [16] BAI Y, WANG J, ZHANG X, *et al.* CrossFuN: Multi-view joint cross fusion network for time series anomaly detection[J]. *IEEE Transactions on Instrumentation and Measurement*, 2023, 72: 1-9.
- [17] LIU P, HAN Q, WU T, *et al.* Anomaly detection in industrial multivariate time series data with neutrosophic theory[J]. *IEEE Internet of Things Journal*, 2023, 10(15): 13458-13473.
- [18] MA S, GUAN S, HE Z, *et al.* TPAD: Temporal pattern based neural network model for anomaly detection in multivariate time series[J]. *IEEE Sensors Journal*, 2023, 23(24): 30668-30682.
- [19] JAGTAP S S, VS S S, SUBRAMANIASWAMY V. A hypergraph based Kohonen map for detecting intrusions over cyber-physical systems traffic[J]. *Future Generation Computer Systems*, 2021, 119: 84-109.

Intrusion Detection Method of Industrial Control System Based on GraphSAGE-MGAT

HU Yuming, WANG Huazhong

(Key Laboratory of Smart Manufacturing in Energy Chemical Process, Ministry of Education, East China University of Science and Technology, Shanghai 200237, China)

Abstract: By integrating Graph Sample and Aggregate(GraphSAGE) and improved Graph Attention Network (GAT), a neural-network-based industrial control intrusion detection is proposed to deal with the complex characteristics of data features in industrial control intrusion detection. Firstly, the intrusion detection traffic data is constructed as a graph structure, and GraphSAGE is used to sample and aggregate neighbor node information to obtain the embedding vectors of nodes, reducing the spatial complexity of the graph structure and improving the efficiency of processing large amounts of data. The improved multi-head attention mechanism is used to enrich the captured feature information, calculate the correlation and importance between nodes, assign corresponding weights to each node, and improve the classification accuracy. This method is verified on an industrial control data set, and the experimental results show that it has better time efficiency and higher detection accuracy.

Key words: industrial control system; intrusion detection; GraphSAGE; GAT; graph structure

(责任编辑: 张欣)