基于神经微分方程的区块链地址风险行为识别算法

梁飞[1]，王瑞丽[2]
（1.北京市公安局经济犯罪侦查总队，北京 100061；2.北京中科链源科技有限公司，北京 100123）

摘　要：首先提出了Tgm_ODE模型，实现了波场链上的钱包地址利用USDT进行犯罪行为的识别；然后模型利用神经常微分方程模型（Neural ODE）学习到节点地址随不同的交易时间间隔而带来的特征连续变化的规律，同时引入了门控机制用于筛选出交易邻居节点地址所带给中心节点的影响强度，门控机制设计中加入了节点地址之间的交易关联性强度，最后利用自注意力机制融合不同交易时刻的节点地址特征，输出节点地址的特征表示。实验证明，Tgm_ODE模型能够有效捕捉节点地址随不规则的交易间隔时间动态变化的特征，在测试集中精准率、召回率和F1指标上优于传统的检测模型。

关键词：神经微分方程；时序模型；门控机制；自注意力机制
中图分类号：TP393
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2024211

Blockchain address risk behavior identification algorithm based on neural differential equations

LIANG Fei[1], WANG Ruili[2]
1. Economic Crime Investigation Brigade of Beijing Municipal Public Security Bureau, Beijing 100061, China
2. Beijing Zhongke Chain Source Technology Co., Ltd., Beijing 100123, China

Abstract: First, the Tgm-ODE model was proposed, which realized the identification of criminal behavior using USDT for wallet addresses on the wavefield chain. Then a neural ordinary differential equation model (Neural ODE) was used to learn the continuous changes in the characteristics of node addresses with different transaction time intervals. At the same time, a gate mechanism was introduced to filter out the impact of neighboring node addresses on the central node. The gate mechanism design incorporated the strength of transaction correlation between node addresses. Finally, the self attention mechanism was used to fuse the node address features at different transaction times, outputting the feature representation of node addresses. Experimental results show that the Tgm-ODE model can effectively capture the dynamic changes of node addresses with irregular transaction intervals, and outperforms traditional detection models in terms of precision, recall, and F1 metrics in the test set.

Keywords: neural differential equation, time series model, gating mechanism, self attention mechanism

0　引言

区块链技术作为21世纪最具变革性的创新之一，正在深刻改变全球的金融和科技生态，但任何新型科技的问世都会有正反面，大量的网络犯罪正在利用区块链去中心化和匿名化的属性[1]，尤其是利用泰达币（USDT）进行犯罪的危害最为严重。USDT已经演化为全球的支付手段，因此在链上有效检测交易识别犯罪的节点地址显得迫在眉睫。本文以波场链上的USDT作为切入点，构建出相应的检测方法。

收稿日期：2024–09–18
通信作者：梁飞，475662476@qq.com

1 相关工作

波场币TRX（TRONIX）是一种基于区块链技术的加密货币，采用了高性能的区块链技术，通过使用DPoS共识算法来加快交易速度并提高可扩展性，因此利用波场链进行USDT交易也成为主流。波场链上的交易形态与图结构是契合的，钱包地址类似图中的节点，交易可以看作图中节点之间的连边，因此这种抽象的关系符合了图算法模型的输入形式。图神经网络是一种专门用于处理图形数据的图算法模型，通过强大建模能力能够有效地捕捉图中节点之间的复杂关系，更好地分析区块链交易数据中模式。

图神经网络用于区块链分析的任务分为异常检测、账户分类、交易追溯，基本的方法是通过交易图数据驱使图神经网络学习到节点在稠密空间内的向量表示。Xia等[2]提出了基于归因分析的自适应图嵌入算法，采用节点重新标记策略构建以太坊交易网络结构和属性特征，从而实现恶意账户地址的检测任务；Chen等[3]采用门控循环单元（GRU）神经网络捕获该交易序列内的时间特征，从而实现了以太坊网络钓鱼的识别任务；Choi等[4]提出了深度图遍历和分类DGTSD（DeepWalk-Transformer）模型，利用Transformer模型的多头注意力机制，有效地学习和分析以太坊交易图中的复杂模式和关系，更准确地识别以太坊上的欺诈活动；Liu等[5]提出了基于有偏随机游走的图嵌入算法GTN2vec模型，通过挖掘以太坊交易记录，综合考虑罪犯的行为模式和交易网络的结构信息，能够自动提取风险的节点地址特征；Kim等[6]提出一种账户交易异质图ATGraph（account-transaction graph）模型，模型将区块链交易记录表示为具有多边的异构交易图，实现了针对存在风险行为节点地址的表示学习。尽管现有的方法大多采用了图算法模型强大的特征提取能力，但却忽视了节点地址特征在交易时间上连续变化的因素，同时也未能有效地考虑随时间演化的过程中不同的交易节点地址本身携带的特征对中心节点地址特征的影响力。

因此本文基于神经微分方程的理论，在交易时间间隔不同的情况下，动态化地聚合节点地址连续变化的特征，同时应用在波场链上犯罪地址的识别任务。

2 相关知识背景

微分方程广泛应用于描述复杂的连续过程，能够建模变量在某个过程中的变化规律，如式(1)所示。

$$\frac{\mathrm{d}y}{\mathrm{d}t}=f_\theta(y(t),t) \tag{1}$$

其中，$y(t)$是未知函数，t是自变量，f_θ函数描述了t时刻在$y(t)$处的导数变化率。神经常微分方程[7]是一种基于常微分方程的深度学习方法，它结合了传统的基于神经常微分方程（Neural ODE, neural ordinary differential equation）数值求解技术和神经网络模型。通过使用Neural ODE来建模数据的演化过程，能够自动地学习数据的动力学特征，从而进行预测和生成等任务。神经常微分方程积分解的形式如式(2)所示。

$$y(T)=y(0)+\int_0^T f_\theta(y(t),t)\mathrm{d}t \tag{2}$$

其中，$y(0)$表示初值，f_θ表示任意的神经网络模型。在求解方程的过程中，可以利用欧拉法求解任意时刻t的解，同时f_θ能够利用数据进行训练，从而拟合相应任务的数据集。

3 模型结构设计原理

本文提出的Neural ODE模型用于识别波场链中交易存在风险行为的恶意地址，将节点地址的交易变化过程使用神经网络为基础的微分方程进行建模，从而建立起随交易时间变化的动态节点特征，借助图模型聚合节点特征的方法，同时沿交易时间引入了交易节点地址之间关联性强度和门控机制，实现针对邻居节点地址特征融合。模型能够更好地捕捉网络的历史信息和演化机制对节点表示的影响程度，在本文中将模型简记为Tgm_ODE。

Tgm_ODE模型运行流程如图1所示，首先用h_{-1}表示初始时刻的隐层状态，通过神经微分方程模型得到隐层的中间态$\hat{h}_0$，然后与中心节点地址x_0的特征利用门控机制进行特征融合，输出为t=0时刻的隐层状态h_0，接着将h_0作为输入，通过微分方程模型得到隐层的中间态$\hat{h}_1$，同时利用门控机制融合在$t=1$时刻与x_0节点地址产生交易的x_1的特征进行融合，然后得到激活后的隐藏状态h_1，以此类推，最终得到节点地址x_0在T时刻的隐藏状态h_T，最后将不同时刻的隐藏状态h_t利用自注意力机制进行特征融合得到节点地址x_0的特征表示。

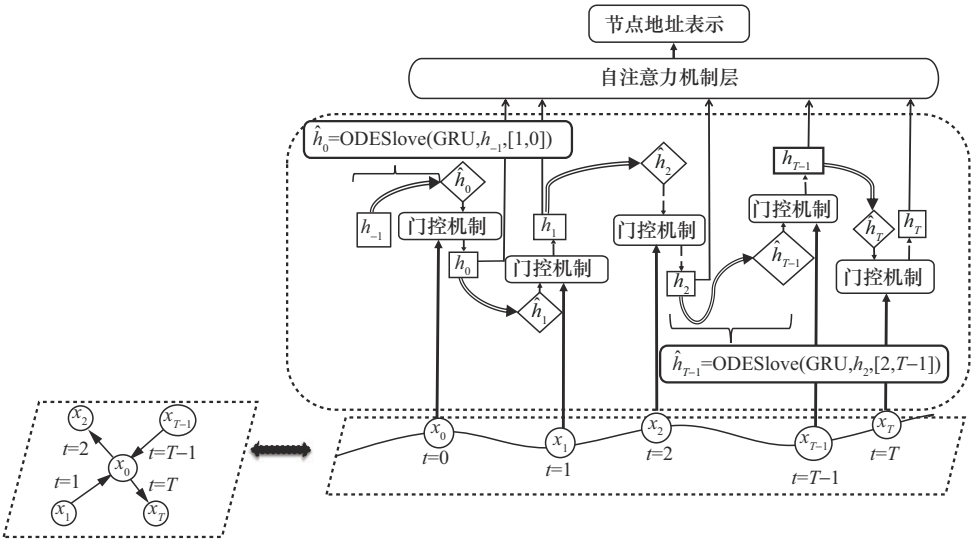

图1　Tgm_ODE模型运行流程

4　Tgm_ODE模型的组成原理

Tgm_ODE模型建立在节点地址随时间变化产生交易的动态时序环境中，核心是挖掘中心节点地址，随交易时间的变化使得节点特征随之变化的特性。模型主要分为3个部分：一是建立起了以神经常微分方程为基础的时序模型；二是利用节点地址之间的交易关系强度构建了门控机制，完成了不同时刻下对邻居节点特征的保留程度；三是利用自注意力机制针对不同时刻的节点状态值进行融合，最终输出中心节点地址的特征表示。

4.1　神经常微分方程模块

针对波场中节点地址的交易间隔是不规则的属性，传统的时序建模神经网络无法有效建模交易时间间隔不固定的场景，因此Tgm_ODE模型利用神经常微分方程对节点地址随不规则的交易时间间隔进行建模，同时选择了GRU替代了描述隐状态的演化函数f_θ，如式(3)所示，用训练数据学习到GRU的参数，从而建立符合波场交易的节点特征动态变化的微分方程。

$$\frac{\mathrm{d}y}{\mathrm{d}t}=\mathrm{GRU}(y(t),t) \tag{3}$$

4.1.1　GRU模型原理

GRU是时序化模型，由2个门控机制组成，如式(4)~式(7)所示。

$$z_t=\sigma\left(W_z h_{t-1}+b_z\right) \tag{4}$$

$$r_t=\sigma\left(W_r h_{t-1}+b_r\right) \tag{5}$$

$$\tilde{h}_t=\tanh\left(W_h(r_t\odot h_{t-1})+b_h\right) \tag{6}$$

$$h_t=z_t\odot\tilde{h}_t+(1-z_t)\odot h_{t-1} \tag{7}$$

其中，z_t对应输出更新门的向量，r_t对应重置门的向量，更新门负责控制上一时刻状态h_{t-1}对当前时刻状态的影响程度，更新门的值越大说明上一时刻h_{t-1}的信息被保留得就越多。重置门负责控制丢弃前一时刻的状态信息h_{t-1}的程度，重置门的值越小说明h_{t-1}所携带的信息被丢弃得越多。更新记忆阶段为保留和丢弃信息2个步骤，使用同一个门控z_t对$\tilde{h}_t$和h_{t-1}进行特征的筛选，最终输出h_t。

4.1.2　神经常微分方程模型的运行原理

在Tgm_ODE模型中，将利用神经常微分方程模块生成节点地址随交易时间而变化的隐状态$\hat{h}_t$，微分方程函数设定为含可训练参变量的GRU[8]，利用微分方程的数值近似求解方法欧拉法得到从$t-1$的输入隐含状态h_{t-1}到t时刻的输出中间态隐藏状态$\hat{h}_t$，如式(8)所示，h_{t-1}作为输入的初始值，利用欧拉法的多轮迭代得到t时刻的中间隐藏状态$\hat{h}_t$，完成了交易时间间隔中的状态的连续演变过程。

$$\hat{h}_t=\mathrm{ODESolve}(\mathrm{GRU},h_{t-1},[t,t-1]) \tag{8}$$

这里需要说明的是，$\hat{h}_t$并不是迭代t时刻神经常微分方程模型的初始值，因为模型假设了在不同时间间隔都会对应不同初值的积分曲线，所以针对$\hat{h}_t$需要利用接下来的门控机制进行激活，从而更加精细地刻画交易时间动态视角下的特征变化。

4.2　节点地址账户关联性强度的门控机制模块

为了实现时序神经常微分方程在不同交易时刻邻居节点地址携带信息量的影响程度，Tgm_ODE

模型采用门控机制动态地实现针对历史信息的保留和新信息加入的多少，引入了节点地址账户关联性强度和邻居节点地址的影响力共同完成门控机制的建立方法 。

Tgm_ODE 模型适用的场景为时间序列化的节点地址交易模式，模型设法在时序节点地址交易的过程中融合邻居节点地址对中心节点地址特征变化的影响强度，这种变化需要在不同交易时刻提取节点特征，因此提出了衡量节点地址之间的关联性强度计算方式。关联性强度涉及两方面的因素，一方面是邻居节点地址本身的交易关联性和影响力，另一方面是中心节点地址和邻居节点地址之间的相关程度。基于上述两方面因素构建起节点地址之间的关联强度，旨在实现不同时刻邻居节点地址对中心节点地址特征的动态表达。

4.2.1 邻居节点地址的影响力

邻居节点地址影响力计算式为

$$\tau_{ij}=\frac{N_{ij}}{\Delta t}+\frac{\lg(\mathrm{sum}(V_{ij}))}{N_{ij}}+\lg V_{ij} \tag{9}$$

其中，N_{ij}表示节点地址i和j的历史交易次数，Δt为节点i和j在交易历史中首次交易时间距t时刻的交易时间间隔，$\frac{\lg(\mathrm{sum}(V_{ij}))}{N_{ij}}$表示节点地址$i$和$j$之间在$t$时刻之前的平均交易金额，$\mathrm{sum}(V_{ij})$表示节点地址$i$和$j$在$t$时刻之前的历史交易总额，$V_{ij}$表示$t$时刻的交易额度。因此$\tau_{ij}$衡量了节点地址$j$对于节点地址$i$的影响力。

4.2.2 节点地址之间的相关性

节点地址之间的相关性利用了地址之间交易共同对手数量进行了衡量，如式(10)所示。

$$s_{ij}=\frac{\Gamma(i)\cap\Gamma(j)}{\Gamma(i)\cup\Gamma(j)} \tag{10}$$

其中，$\Gamma(i)$表示t时刻之前与节点i产生交易的邻居地址的集合，$\Gamma(j)$表示t时刻之前与节点j产生交易的邻居地址的集合。针对$\Gamma(i)$和$\Gamma(j)$的2个集合求交并比，可以得到节点地址i和j之间的相关性s_{ij}，s_{ij}的取值是0到1之间的实数，基于交易邻居的重合数量进而计算出节点地址之间的相关程度。最终利用邻居节点地址的影响力和地址之间的相关性共同计算出中心节点地址与邻居节点地址之间的交易关联性强度，如式(11)所示。

$$u=\frac{1}{1+\exp(-W[\tau_{ij},s_{ij}])} \tag{11}$$

其中，τ_{ij}和s_{ij}是上述的2个因素，同时转化为二维向量，再利用可学习的参数W进行特征变换，最后得到了归一化的输出向量u。本文模型在实现节点地址交易强的影响力中引入了门控机制，设定节点i为中心交易节点地址，j为在不同时刻t与i存在交易行为的节点地址，这里需要强调的是在初始时刻，输入为中心节点地址，设定τ_{ij}和s_{ij}的值为0，此时u的向量值为1，从而保证了中心节点地址特征完全被保留。

4.2.3 门控机制实现方法

针对中心节点地址i，沿着交易时间方向进行展开，存在多个节点地址j与i存在交易的行为，为了刻画节点j对于i的影响力能够在特征选择上发挥作用，因此本文模型中设计了门控机制[9]，如式(12)所示。

$$h_t=u\odot W_{in}x+(1-u)\odot\hat{h}_t \tag{12}$$

其中，u为门控参数，如式(11)计算得到的归一化关联性强度所示。将u视为保留节点j所携带的特征信息量的比例，最终得到不同节点地址j对于i的沿交易时间的特征融合。

4.3 时序节点地址特征融合 Attention 层模块

Tgm_ODE 模型中的每个时间步t都会得到隐层输出h_t，通过特征变换进而得到m_t，为了增强节点地址特征的表达能力，采用了自注意力机制[10]对于不同时间步上 m_t进行特征的融合，将隐层 m_t按时刻0到T组成输入矩阵$\boldsymbol{M}$，同时用参数矩阵$\boldsymbol{W_Q}$、$\boldsymbol{W_K}$、$\boldsymbol{W_V}$作用于$\boldsymbol{M}$，得到$\boldsymbol{Q}$、$\boldsymbol{K}$、$\boldsymbol{V}$矩阵，如式(13)所示。计算自注意力系数矩阵，同时用 Softmax 的方式对自注意力系数矩阵进行归一化，之后作用于矩阵$\boldsymbol{V}$，实现$\boldsymbol{M}$矩阵在不同时刻列向量的融合，最终对矩阵进行平均化的操作，如式(14)所示，输出的o为中心节点地址特征向量表示。

$$\boldsymbol{Q}=\boldsymbol{W_Q}\boldsymbol{M},\boldsymbol{K}=\boldsymbol{W_K}\boldsymbol{M},\boldsymbol{V}=\boldsymbol{W_V}\boldsymbol{M} \tag{13}$$

$$o=\mathrm{mean}\left(\mathrm{Softmax}\left(\frac{\boldsymbol{Q}\boldsymbol{K}^{\mathrm{T}}}{\sqrt{d}}\right)\boldsymbol{V}\right) \tag{14}$$

4.4 损失层的构建方式

Tgm_ODE 模型损失计算层如式(15)所示，对节点地址的特征表示o进行变换得到$\hat{y}_i$，$\hat{y}_i$是正例输出概率值。损失函数通过计算分类交叉熵得到损失值，如式(16)所示，其中y_i表示第i个样本的标签，通过优化Loss值实现对Tgm_ODE模型中参数

的训练。

$$\hat{y}_i = \mathrm{Sigmod}(W_{\mathrm{out}} o_i + b_{\mathrm{out}}) \tag{15}$$

$$\mathrm{Loss} = -\frac{1}{N}\sum_{i \in N}\left(y_i \log\left(\hat{y}_i\right) + (1 - y_i)\log\left(1 - \hat{y}_i\right)\right) \tag{16}$$

综上所述，给出Tgm_ODE模型各组成部分的原理说明和实现过程，具体的算法伪代码如算法1所示。

算法 1　融合神经微分方程的动态时序节点表示

输入　$G = \{(x_0, x_{1\cdots T})\}$，$x_0$表示中心节点地址的初始特征，$x_{1\cdots T}$表示沿时间线与中心节点地址存在交易的邻居节点地址的特征

输出　$x_0 \to o$，输出x_0经过转换后的表示特征

1) 初始化 $h_{-1} = 0$

2) for t in 0,1,2,⋯,T do

3)　$\hat{h}_t = \mathrm{ODESolve}(\mathrm{GRU}, h_{t-1}, [t, t-1])$

4)　$u = \dfrac{1}{1 + \exp(-W[\tau_{ij}, s_{ij}])}$

5)　$h_t = u \odot W_{in} x_t + (1 - u) \odot \hat{h}_t$

6)　$m_t = W_O h_T + b_O$

7) end for

8) $o = \mathrm{Attention}(m_{1\cdots T})$//$o$是最终的中心节点地址$x_0$的特征。

9) return o//返回特征值。

5　数据集的准备与特征处理

5.1　数据集的收集

数据集的收集是在各类涉虚拟币案件办理过程中，积累波场链中1 566个与风险行为相关联的恶意地址，这些地址主要为上游的电信诈骗、网络赌博、非法换汇为基础的沉淀数据。将1 566作为标签化数据，同时设定成中心节点地址。为了能够提取到犯罪的交易特征，采样过程中按照节点地址相应的作案时间进行一阶邻居采样。采样的规则是沿时间增加的方向，在TRC-20协议中涉及USDT交易的邻居进行采样，经过筛重后共有146 782个地址在相应发案时间范围内与中心节点地址存在USDT交易。之后随机采样1 566个地址作为正常的标签，继续按上面的方式进行采样，得到137 670个节点地址，因此整个训练数据集中，风险标签地址数量为1 566个，时序一阶邻居地址为146 782个，正常交易地址标签同样为1 566个，时序一阶邻居地址为137 670个。

5.2　数据集的特征处理

节点地址初始特征直接决定模型训练的有效性和预测的准确性，需要科学地建立起一套能够反映节点地址交易的本质属性的初始特征，为了精细刻画节点地址的交易行为，在特征构建过程中综合运用了图网络和统计学的指标，同时考虑了波场链中波场币承担维持波场链正常运行的影响因素，因此在特征构建过程中综合考虑波场币和泰达币交易的关联性，因此每个节点地址构建了26个维度特征作为初始特征。其中前20个维度特征分别利用波场的中的原生币波场币和泰达币以相同的计算方式进行创建，为了简化只描述泰达币的特征建立方法，波场币用括号进行注明，具体构建方法如下。

节点地址泰达币（波场币）出度：节点地址转出方向交易的次数，记作USDT（TRX）_Out_Dgree。

节点地址泰达币（波场币）入度：节点地址转入方向交易的次数，记作USDT(TRX)_In_Dgree。

输出泰达币（波场币）总量：节点地址转出泰达币的总量：记作USDT(TRX)_Out_Value。

输入泰达币（波场币）总量：节点地址转入泰达币的总量，记作USDT(TRX)_In_Value。

平均输出泰达币（波场币）总量：节点地址转出泰达币总量的平均值，计算式为USDT（TRX）_Out_Value/USDT(TRX)_Out_Dgree，记作USDT_AvgOutValue。

平均输入泰达币（波场币）总量：节点地址转入泰达币总量的平均值，计算式为USDT（TRX）_InValue/ USDT（TRX）_In_Dgree，记作AvgInValue。

输出最小值：节点地址转出泰达币（波场币）在历史交易中的最小值，记作USDT（TRX）MinOutValue。

输出最大值：节点地址转出泰达币（波场币）在历史交易中的最大，记作USDT（TRX）MaxOutValue。

输入最小值：节点地址转入泰达币（波场币）在历史交易中的最小值，记作USDT（TRX）MinInValue。

输入最大值：节点地址转入泰达币（波场币）在历史交易中的最大值，记作USDT（TRX）MaxInValue。

泰达币出度与波场币出度的比值，计算式为USDT_Out_Dgree/TRX_ Out_Dgree。

泰达币入度与波场币入度的比值，计算式为USDT_In_Dgree/TRX_ In_Dgree。

输出泰达币总量与输出波场币总量的比值，计算式为USDT_Out_Value/TRX_Out_Value。

输入泰达币总量与输入波场币总量的比值，计算式为USDT_In_Value/TRX_In_Value。

平均输出泰达币总量与平均输出波场币总量的比值，计算式为USDT_AvgOutValue/ TRX_AvgOutValue。

平均输入泰达币总量与平均输入波场币总量的比值，计算式为USDT_AvgInValue/ TRX_AvgInValue。

6 实验结果和分析

6.1 实验环境

实验选择Windows11 64位操作系统，CPU i9-9900K，GPU GeForce 3080Ti，Tgm_ODE模型代码使用Python语言，同时使用DGL图神经网络库进行的编写，编辑软件为JetBrains PyCharm。

6.2 评价标准

在实验中，本文通过3个广泛使用的指标，即使用精准率（Precision）、召回率（Recall）和F1这3个指标来衡量模型的准确性，如(17)～式(19)所示。

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \tag{17}$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \tag{18}$$

$$\text{F1} = \frac{2\text{PrecisionRecall}}{\text{Precision} + \text{Recall}} \tag{19}$$

其中，TP表示模型将正例样本预测为正例样本的数量，FP表示模型将负例样本预测为负例样本的数量，FN表示模型将正例样本预测为负例样本的数量。

6.3 实验过程参数设定

在实验过程中，为了适配实验所属环境，取定样本数量为8作为一个批次（batch）训练数据量，迭代训练轮数设置为500，选择Adam优化算法作为训练模型的梯度优化器，迭代步数中的学习率设定为0.001。

6.4 实验训练过程与效果评估

图2展示了Tgm_ODE模型训练过程中随着迭代步数增加，训练集上的损失值和测试集上的精准率的变化曲线。通过曲线可以看出，训练迭代步数与设定的500一致，在0至50步的迭代过程中损失值和精准率分别迅速地下降和提升，迭代步数达到200之后曲线趋于收敛，直至500步时已没有明显变化。

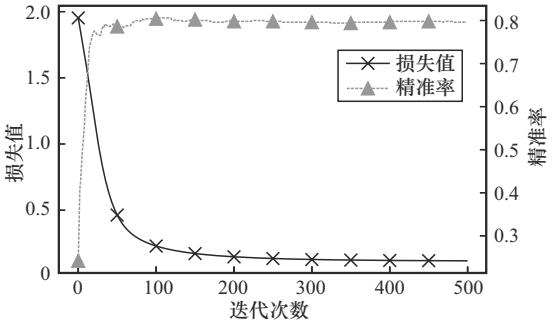

图2 训练集上的损失值和测试集上的精准率的变化

表1展示了Tgm-ODE模型在波场节点地址存在风险的恶意行为的识别效果。为了说明模型的识别能力，测试中加入传统的图神经网络模型GCN和GAT作为对比基线模型。使用精准率、召回率、和F1这3个指标作为模型在测试集上的表现能力的基准指标。从指标中进行分析可以发现，模型在3个基准指标的表现能力均高于GCN和GAT模型。这进一步证明了Tgm-ODE采用的神经微分方程模块建立起方法在捕捉节点特征的动态变化的和提取节点地址之间的相互作用对于模型检测指标的提升有着显著的效果。

表1 模型对比实验结果

使用模型	Precision	Recall	F1
GCN	75.32%	68.38%	71.21%
GAT	78.56%	75.15%	76.81%
Tgm-ODE	82.76%	77.65%	80.12%

6.5 消融实验分析

采用消融实验分析模型中每个部分对识别能力的影响程度，因此拆解Tgm-ODE模型中的组件，

从而分析每个组件对于识别波场存在风险恶意行为结果的关联性。一是使用传统的GRU模型，GRU是时序化模型替代神经常微分方程模块，可以类比传统的图时序化模型，记作Tgm-GRU；二是取消门控机制，直接使用 $W_{in}x_t+\hat{h}_t$ 替代门控机制，记作Tm-ODE；三是针对门控机制内的2个模块进行单一因素的融合，单独使用节点地址之间的相关性，记作Tgs-ODE；四是单独使用邻居节点地址的影响力，记作Tgn-ODE。

分析表2的消融实验结果，可以清楚地看到各模块组件对最终实验结果的影响，神经微分模块对非规则交易时间的建模优势是明显的，Tm-ODE比Tgm-GRU在F1指标提升6.33%，证明了神经微分方程能够有效提取节点地址特征随交易时间间隔演化的特性，同时门控机制的引入也给模型提取节点特征赋予了能力，Tgs-ODE和Tgn-ODE比不引入门控机制的Tm-ODE在F1指标上提升了2.96%和2.86%，进一步验证了门控机制对新加入的邻居节点地址特征信息量的保留和丢弃的操作能够提升模型的识别效果。

表2　　消融对比实验结果

使用模型	Precision	Recall	F1
Tgm-GRU	71.47%	64.78%	67.96%
Tm-ODE	76.25%	72.43%	74.29%
Tgs-ODE	79.15%	75.43%	77.25%
Tgn-ODE	78.32%	76.02%	77.15%
Tgm-ODE	82.76%	77.65%	80.12%

6.6　模型预测节点编码可视化分析

Tgm-ODE模型针对节点地址预测节点特征编码的表示进行可视化分析，方法是通过TSNE将节点地址的编码映射到二维空间，从而进行可视化分析，随机从测试集中抽取400个样本，其中正例样本和负例样本的比例为1:1。图3为节点地址的原始特征编码，图4为GCN模型输出的特征编码，图5为GAT模型输出的特征编码，图6为Tgm-ODE模型特征编码。通过比较可以发现，Tgm-ODE模型在波场中同一类节点地址特征距离更加紧密，存在风险行为的节点地址和正常节点地址之间的分割边界更加明显。

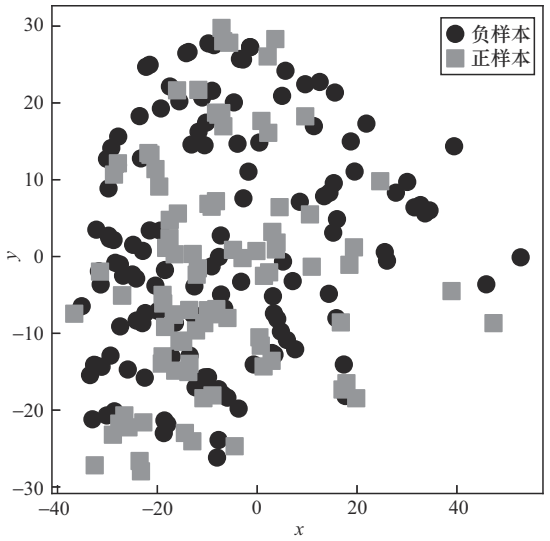

图3　原始特征编码

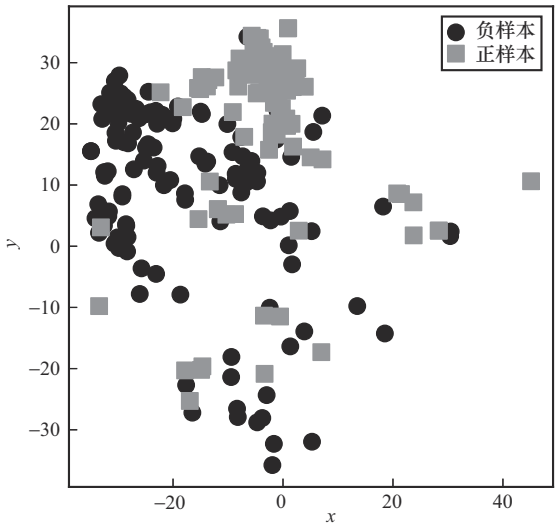

图4　GCN模型特征编码

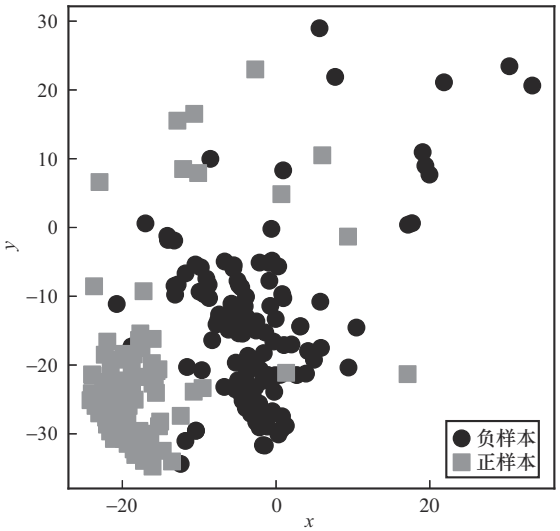

图5　GAT模型特征编码

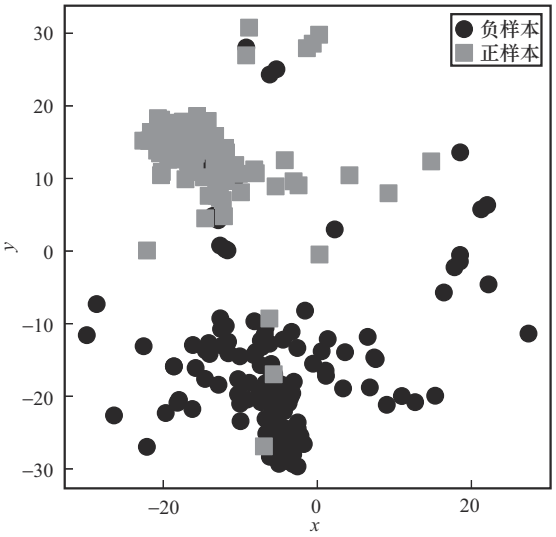

图6　Tgm-ODE模型特征编码

6.7　风险模式行为分析

为了进一步探究Tgm-ODE模型在实际侦查中的价值，具体分析测试集中的样本节点地址被识别为具有风险行为时，发现了4种风险的行为模式，具体如下。

1) 循环贷模式。风险节点地址的会随着交易时间的演化过程与固定的节点交替进行交易，转入的方向有35.2%来自交易所内用户的提币操作，转出的地址存在42.7%的交易所用户，是一种在不同交易所内对泰达币的拆借归集行为，这种行为通常是犯罪团队的囤币行为，这一类模式占据测试集中约12.65%的样本数。

2) 流浪者模式。风险节点地址的交易在时间演化过程中某个间隔时间段内有多个地址进行高频转入交易且主要以小额交易为主，然后该节点以相对固定的周期向一个地址统一转出，然后再重复这个过程，这个模式识别出的一般为赌博网站的入金地址，这一类模式占据测试集中约8.21%的样本数。

3) 投机者模式。风险节点地址在交易的时间线上几乎不存在重复的交易对手地址，但交易对手的转入侧和转出侧节点地址之间的相关性的s_{ij}几乎都是大于0.65，节点地址之间存在社团聚集的状态，抽样该种模式的节点地址发现多为境外通联工具中为黑灰产提供担保的担保地址，这一类模式占据测试集中约6.25%的样本数。

4) 清零模式。风险节点地址几乎是单进单出、不留余额的方式进行交易，交易时间间隔几乎在小时级内完成，这种地址抽样发现大部分为风险通道的过渡地址，能够为多个上游犯罪提供服务，这一类模式占据测试集中约5.79%的样本数。

尽管在本节中存在因测试样本数量的不足而带来的缺乏统计学意义的缺陷，但从侧面验证了Tgm-ODE模型挖掘风险行为模式的能力。

7　结束语

本文基于Tgm-ODE模型的架构，核心是搭建可训练的神经微分方程模块用来拟合波场的节点地址随不规则交易时间间隔变化而变化的节点特征表示，同时构建了以交易账户关联性强度为影响的门控机制，最终使得模型能够更好地融合沿时间线而发生交易的邻居节点地址特征。实验证明了模型Tgm-ODE具备捕获节点地址特征随时间变化的演化性质，模型提升了识别波场链上地址通过USDT进行风险行为的能力。

参考文献：

[1] 李大猛, 孙杰, 蒋照生, 等. 虚拟货币犯罪态势及安全治理研究综述[J]. 警察技术, 2023(2): 33-41.
LI D M, SUN J, JIANG Z S, et al. Summary of research on virtual currency crime situation and security governance[J]. Police Technology, 2023(2): 33-41.

[2] XIA Y J, LIU J L, WU J J. Phishing detection on ethereum *via* attributed ego-graph embedding[J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2022, 69(5): 2538-2542.

[3] CHEN Z, HUANG J, LIU S Z, et al. Multiscale feature fusion and graph convolutional network for detecting ethereum phishing scams[J]. Electronics, 2024, 13(6): 1012.

[4] CHOI S H, BUU S J. Learning to traverse cryptocurrency transaction graphs based on transformer network for phishing scam detection[J]. Electronics, 2024, 13(7): 1298.

[5] LIU J Y, YIN C C, WANG H, et al. Graph embedding-based money laundering detection for ethereum[J]. Electronics, 2023, 12(14): 3180.

[6] KIM J, LEE S, KIM Y, et al. Graph learning-based blockchain phishing account detection with a heterogeneous transaction graph[J]. Sensors, 2023, 23(1): 463.

[7] CHEN R T Q, RUBANOVA Y, BETTENCOURT J, et al. Neural ordinary differential equations[C]//Proceedings of the 32nd International Conference on Neural Information Processing Systems. Massachusetts: MIT Press, 2018: 6572-6583.

[8] BROUWER E D, SIMM J, ARANY A, et al. GRU-ODE-Bayes: continuous modeling of sporadically-observed time series[C]//Proceedings of the 33rd International Conference on Neural Information Processing Systems. Massachusetts: MIT Press, 2019: 7379-7390.

[9] 崔文岳, 谷远利, 赵胜利, 等. 基于有向图卷积与门控循环单元的短时交通流预测方法[J]. 交通信息与安全, 2023, 41(2): 121-128.
CUI W Y, GU Y L, ZHAO S L, et al. A method of predicting short-term traffic flows based on a DGC-GRU model[J]. Journal of Transport Information and Safety, 2023, 41(2): 121-128.

[10] 周俊, 曹月恬, 胡斌斌, 等. 基于实时动态图联合学习框架的金融交易风控技术[J]. 电子学报, 2023, 51(10): 2801-2811.
ZHOU J, CAO Y T, HU B B, et al. Real-time dynamic graph unified learning framework for financial transaction risk management[J]. Acta Electronica Sinica, 2023, 51(10): 2801-2811.

[作者简介]

梁飞（1989– ），男，北京人，北京市公安局经济犯罪侦查总队副高级工程师，主要研究方向为深度学习算法、区块链安全等。

王瑞丽（1988– ），女，山西吕梁人，北京中科链源科技有限公司工程师，主要研究方向为区块链数据分析等。