基于 GCN 的 IOTA 寄生链检测

刘韦淇[1]，侯永超[1]，木又青[2]，丁智颖[1]，刘明灏[1]，赵金东[1]

(1. 烟台大学 计算机与控制工程学院　山东 烟台 264600；
2. 联勤保障部队大连康复疗养中心　辽宁 大连 116600)

摘要：随着物联网技术的不断发展,确保物联网环境中的交易安全至关重要。Internet of Things application(IOTA)网络作为一种专为物联网设计的分布式账本技术,在处理海量设备间交易时尤为重要。寄生链攻击作为一种常见的攻击方式,通过在 IOTA 主缠结(Tangle)中认证非法交易,严重威胁了网络的安全性能。为应对这一问题,提出一种基于图卷积神经网络(graph convolutional network, GCN)的方法来检测 IOTA 网络中的寄生链交易。通过分析正常交易与寄生链交易的行为差异,提出四个属性为交易的特征值,以反映两者之间的差异。根据寄生链攻击规则,构建多个包含寄生链的模拟 IOTA 网络并生成数据集,通过训练后的模型对交易节点进行分类,从而识别恶意节点。实验结果表明,模型在检测恶意交易方面的准确率超过 80%,可以有效检测网络中存在的寄生链交易。

关键词：区块链；IOTA；寄生链攻击；图卷积神经网络；物联网

中图分类号：TP393　　**文献标志码**：A　　**文章编号**：1671-6841(2026)03-0041-09

DOI：10.13705/j.issn.1671-6841.2024176

Using GCN to Detect Parasitic Chains Attacks in IOTA

LIU Weiqi[1], HOU Yongchao[1], MU Youqing[2], DING Zhiying[1], LIU Minghao[1], ZHAO Jindong[1]

(1. *School of Computer and Control Engineering*, *Yantai University*, *Yantai* 264600, *China*;
2. *Dalian Rehabilitation and Rehabilitation Center of Joint Logistics Support Force*, *Dalian* 116600, *China*)

Abstract: With the deveopment of the Internet of Things (IoT) technology, transaction security in IoT environments become critical. The IOTA network, a distributed ledger technology designed specifically for IoT, plays a crucial role in managing transactions among numerous devices. Parasitic chain attacks, a common threat, undermine network security and performance by validating illegal transactions in the IOTA main tangle. A method based on graph convolutional networks (GCN) was proposed to detect parasitic chain transactions in the IOTA network. By analyzing the behavioral differences between normal and parasitic chain transactions, four attributes were identified as feature values to capture these differences. Simulated IOTA networks containing parasitic chains were constructed based on the attack rules to generate datasets, and the trained model was used to classify and identify malicious nodes. Experimental results demonstrated that the model achieved over 80% accuracy in detecting malicious transactions, effectively identifying parasitic chain transactions in the network.

Key words: block chain; Internet of Things application(IOTA); parasitic chain attack; graph convolutional network; Internet of Things(IOT)

收稿日期:2024-10-26
基金项目:国家自然科学基金项目(62405262)
第一作者:刘韦淇(1999—　),男,硕士研究生,主要从事 IOTA 寄生链研究,E-mail: 1450846558@qq.com。
通信作者:赵金东(1974—　),男,副教授,主要从事区块链、物联网和大数据处理研究,E-mail: zhjdong@ytu.edu.cn。

0 引言

分布式账本技术在联邦学习、智能交通和供应链管理等领域已广泛应用于信任和数据交换问题[1-3]。传统区块链难以满足大规模物联网环境下的可扩展性与交易费用需求[4]。为此,IOTA 社区提出基于有向无环图(directed acyclic graph, DAG)的拓扑结构以存储区块,但区块概念尚未完全去除[5]。随着 ByteBall 的推出,DAG 分布式账本才逐渐被广泛关注。

IOTA 是基于 Tangle 结构的 DAG 设计,提供高效、无手续费的数据交换[6],每笔交易只需认可两笔前序交易即可加入网络,从而缩短验证时间并提高系统扩展性[7]。然而,Tangle 结构也带来安全方面的挑战,其中寄生链攻击是常见的威胁[8]。攻击者创建私下的次 Tangle,通过双花攻击影响主 Tangle。寄生链具有结构灵活、攻击行为隐蔽、选择性批准、攻击位置自由等特点,极大地增加了检测难度与攻击成功率。现有的保护方法包括更改网络规则、使用中心化的 Coordinator 组件,优化尖端选择算法或马尔可夫链蒙特卡罗(Markov chain Monte Carlo, MCMC)方法等,这些方法虽提升了安全性,但对去中心化和网络发展带来了负面影响[9]。

为解决上述问题,本文提出一种创新的特征值选择方法,并利用 GCN 有效处理图异常节点的能力检测 IOTA 网络中的寄生链攻击。该方法突破了传统预防寄生链攻击方法的局限性,通过四类关键特征和先进的 GCN 模型,有效识别 IOTA 网络中潜在的恶意交易。本文的主要贡献如下。

1) 提出特征值与引入 GCN。首次将 GCN 应用于 IOTA 网络的寄生链检测,设计了有效的特征值表示方法,通过 GCN 提高了复杂网络攻击的识别能力。2) 模拟与分析。研究了随机漫步者的规则并改进惩罚机制,分析改进后随机游走子进入寄生链的概率,为特征选择和模型优化提供支持。3) 模型训练和验证。对 GCN 模型进行了优化,以更好适应 IOTA 寄生链检测,并用实验验证了其显著的检测能力与泛化性。

1 相关工作

为解决 IOTA 中的寄生链问题,文献[10]根据寄生链的随机形状与特征将其分为三类并分析不同类型的攻击效果。随后,Gullen 等[11]提出了 k 阶寄生链结构,对其成功率和结构特性进行分析。Chen 等[12]提出了将大额交易拆分为小额交易的方法来有效防御小规模、低成本的寄生链攻击,但对高算力或高成本攻击效果有限。马红超[13]指出,IOTA 网络初期,MCMC 算法能有效预防寄生链攻击,随着交易速率增加,攻击成本逐渐上升,寄生链攻击的成功几率也会大幅降低。他建议调整游走子参数以增强各阶段的安全性。朱新玲[14]发现,MCMC 算法虽降低了初期寄生链攻击成功率,却导致遗孤交易增多,会对网络发展产生负面影响。此外,文献[9]通过评分函数检测特定类型的寄生链,其效果局限于简单结构,难以应对复杂形态的寄生链攻击。

当前防御措施多为调整算法参数或交易发布方式,虽然减少了寄生链攻击,但影响网络运行稳定性。此外,攻击者可以根据修改后的网络规则设计出新的攻击手段,进一步提高攻击的成功率。一旦攻击成功,现有方法难以及时检测和识别网络中潜入的寄生链交易,从而无法有效保证交易的安全性。

基于上述分析,为了确保网络正常发展的同时有效防止寄生链攻击,本文提出了一种基于 GCN 的寄生链检测方案。通过 GCN 学习 IOTA 网络中主 Tangle 和寄生链结构间的关系,无须手动调整网络规则或参数也可适应不同的攻击场景。本文设计一组反映交易节点行为差异的特征值用于训练 GCN 模型,并有效区分主 Tangle 与寄生链交易,尤其在应对高算力或高成本攻击时表现出色。实验结果表明,该方案无须改变网络规则,即可高效识别复杂寄生链攻击,保障 IOTA 网络的安全性与正常运行。

2 方法概述

本文提出的寄生链检测方法的核心在于结合 GCN 与 IOTA 网络交易的行为特征,通过分析主 Tangle 与寄生链交易的差异提取特征值,并用于训练 GCN 模型,以检测异常节点。

2.1 系统框架

本文通过分析异常交易的行为特征提取特征值,并利用这些特征值训练图卷积神经网络,使用训练后的模型对网络中的所有交易进行分类,得到异常交易的集合。实验中将交易表示为图的节点,将交易之间的认证关系表示为图的边。给定一个含有寄生链的 IOTA 网络图 $G=(V,E)$,$V=\{\{V_{p1},V_{p2},\cdots,V_{p\lambda}\},\{V_{a1},V_{a2},\cdots,V_{a\mu}\}\}$,其中:$V$ 是节点集合;V_{px} 与 V_{ax} 分别为图中常规节点与异常节点;λ 为图 G 中常规节点的数量;μ 为图 G 中异常节点的

数量;E 是边集合。识别出的异常节点集合为 V'。预测结果函数为 G,表示异常节点的集合 $V' \subseteq V$,且 $\forall V_{ax} \in V', G_{V'} = 1$。

实验主要任务为:1) 通过分析 IOTA 网络中正常交易与异常交易的行为差异,找到合适的特征值用于模型训练;2) 利用训练后的模型预测网络中存在的恶意交易,通过不同规模下的准确率、$F1$ 值等指标验证特征值选择的合理性,并通过损失值验证 GCN 模型的有效性。为此,需要选择能够有效表达 IOTA 网络中交易属性的特征值。随后提取节点的特征值作为 GCN 的输入特征,并利用二分类损失函数对所有节点进行分类,并给予标签类型,即

$$Label_{[V_p]} = 0,\ Label_{[V_a]} = 1。$$

将节点之间的关系存储到邻接矩阵,并将标签、节点特征值以及邻接矩阵输入模型中迭代训练。最后,在测试阶段将各节点的特征值输入训练好的模型得到图卷积神经网络预测的准确率、召回率、$F1$ 值等指标,具体算法流程如下。

1) 随机生成 IOTA 网络结构 A,并将其编码为适用于 GCN 的数据集,具体包括生成网络的邻接矩阵、A 中节点的标签 $Label_{[A]}$、各节点的特征矩阵。

2) 将步骤 1) 生成的数据集输入 GCN 模型中进行训练,得到训练好的 GCN 模型。

3) 随机生成另一个 IOTA 网络结构 B,并提取相应的数据集,包括节点特征矩阵,邻接矩阵,各节点的标签 $Label_{[B]}$。

4) 将步骤 3) 中提取的节点特征矩阵与邻接矩阵输入训练好的 GCN 中,得到节点标签的预测结果 $Label_{[T]}$。

5) 将预测结果 $Label_{[T]}$ 与真实标签 $Label_{[B]}$ 进行对比和评估,计算评估指标,以衡量模型性能。

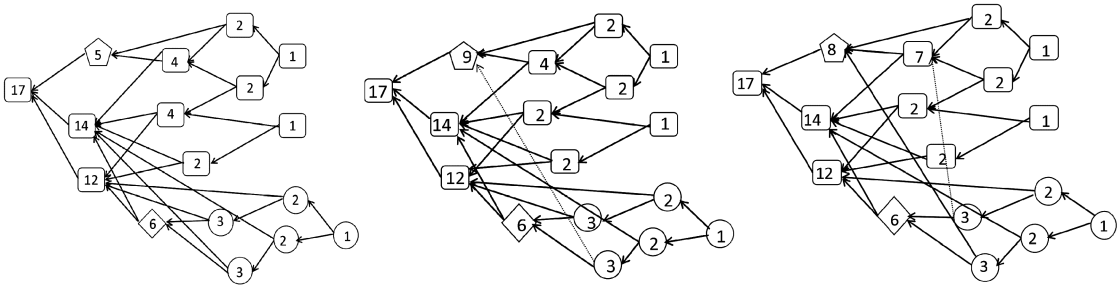
2.2　节点特征值的提取

由于本文是通过对 IOTA 网络中的各个交易及其之间的联系对网络中的寄生链进行检测,所以省去了交易时间和交易内容等属性。

在分析主 Tangle 与寄生链的结构时发现,寄生链中交易的行为与常规 IOTA 网络交易的行为存在差异,主要有以下两种。

1) 各交易的累计权重和入度。游走子更倾向于选择累计权重较高的交易进行认证,攻击者为了增加被选中的概率,常通过认证高权重交易集中构建寄生链,导致其入度和累计权重迅速提升,与相邻节点差距加大。在 GCN 模型中,节点属性的传播会逐渐影响相邻节点,训练中这种效应进一步强化特征区分。He 等[15] 的研究指出,入度和累计权重是区分常规交易和恶意活动的关键指标。因此本实验选取入度和累计权重作为特征值,以提升模型在检测恶意活动方面的性能。

2) 各交易中未认证交易的 ID 及其个数。在复杂的寄生链结构中,仅依靠入度和累计权重作为特征值进行模型训练不足以应对更隐蔽的攻击模式。通过深入分析寄生链的行为特征,发现寄生链不集中认证单一的交易时,可以使寄生链更具隐蔽性。此外,考虑到攻击者的算力有限,为了提高攻击效率,寄生链交易不会认证与被攻击交易相关的交易。图 1 展示了 IOTA 中恶意节点的攻击方式,节点上的数字表示各个交易的累计权重。五边形节点表示被攻击的交易;菱形节点表示攻击者创建的用于双花攻击的交易;正方形节点为正常交易;圆形节点为攻击者在寄生链中创建的正常交易,其目的是增加菱形交易的累计权重以获得更高被游走子选中的概率。



(a) 不认证被攻击的交易　　(b) 认证被攻击的交易　　(c) 间接认证被攻击的交易

图 1　恶意节点攻击方式

Figure 1　Malicious node attack methods

在图 1(a)中,攻击者发布的交易并未对受攻击交易进行认证,而是选择认证与受攻击交易无关的其他交易,从而提高了这些无关交易的权重。这种策略有两个主要优势:一方面,减少了游走子选择受攻击交易的概率;另一方面,增加了游走子选择恶意交易的概率。在图 1(b)和图 1(c)中,寄生链中权

重为3的交易直接或间接认证了受攻击的交易,这导致图1(b)和图1(c)中的五边形节点的累计权重远大于图1(a)中的五边形节点。这种方式既降低了攻击成功的概率,也增加了攻击的成本,不符合攻击者的预期目标。因此,攻击者不会牺牲原本较低的攻击效率去认证与受攻击交易相关的交易,从而导致寄生链交易与常规交易在选择认证对象时表现出不同的偏好。因此,引入每笔交易的未认证交易ID及其数量作为特征值属性,可以有助于区分寄生链节点与常规节点。

基于上述分析,提取的特征包括:累计权重、入度、未认证交易的ID及数量。鉴于攻击者资源有限且追求更高成功率与低成本,这些特征不仅适用于简易和k阶寄生链,还能有效检测更复杂的寄生链结构。

2.3 GCN公式分析与改进

IOTA网络的交易结构适合作为图结构进行分析,将每笔交易视为节点,认证关系构成边。这种图结构为使用GCN检测IOTA网络异常行为提供了有效的建模基础。首先,IOTA交易节点的局部平滑性使得相邻节点通常具有关联性,GCN通过聚合节点及其邻居特征,有助于识别异常模式。其次,GCN的特征传播性使其能捕捉寄生链攻击中局部特征的异常聚集。因此,本文利用GCN检测IOTA网络中的异常交易可有效识别隐蔽的寄生链攻击模式,提升检测精度。

图卷积操作可以表示为[16]

$$\boldsymbol{H}^{l+1}=\sigma(\tilde{\boldsymbol{D}}^{-\frac{1}{2}}\tilde{\boldsymbol{A}}\tilde{\boldsymbol{D}}^{-\frac{1}{2}}\boldsymbol{H}^{(l)}\boldsymbol{W}^{(l)}),\tag{1}$$

其中:$\boldsymbol{H}^{(l)}$为第l层节点矩阵,维度为$n\times d_l$,n是节点的数量,d_l为第l层的特征维度;$\tilde{\boldsymbol{A}}=\boldsymbol{A}+\boldsymbol{I}$为加入了节点到自身环路的邻接矩阵;$\tilde{\boldsymbol{D}}=\sum_{i=1}^{N}\tilde{\boldsymbol{A}}_{ii}$为$\tilde{\boldsymbol{A}}$的度数矩阵;$\boldsymbol{W}^{(l)}$为第$l$层节点的权重矩阵;$\sigma(\cdot)$为激活函数。节点的输入特征为

$$\boldsymbol{X}=\begin{pmatrix} cw_{(v_1)} & deg_{(v_1)} & \mu_{(v_1)} \\ \vdots & \vdots & \vdots \\ cw_{(v_n)} & deg_{(v_n)} & \mu_{(v_n)} \end{pmatrix},\tag{2}$$

其中:$\boldsymbol{X}$表示初始输入特征矩阵;$cw_{(v_i)}$表示节点v_i的累计权重;$deg_{(v_i)}$表示节点v_i的入度;$\mu_{(v_i)}$表示节点v_i未认证交易的个数。然而,IOTA网络中的未认证的节点数量和未认证状态各不相同,难以直接作为GCN的输入。为此,本文采用单独的特征向量存储各节点的未认证状态,即

$$\boldsymbol{u}(v_i)=[u_{i_1},u_{i_2},\cdots,u_{i_m}],\tag{3}$$

其中:$\boldsymbol{u}_i$为各个节点的单独特征向量。通过这种方式,初始特征矩阵$\boldsymbol{X}$能够捕捉到IOTA网络中交易节点的重要属性,确保GCN能够更精确地处理节点特征。在GCN中,通过节点之间的连接关系进行信息传递,使每个节点能够获取其邻居节点的信息,从而提升异常节点检测的准确性。每个节点的图信号传递公式为

$$\boldsymbol{H}_v^{(l+1)}=\sigma\Big(\sum_{z\in N(v)}\frac{1}{deg(v)}\boldsymbol{H}_z^{(l)}\boldsymbol{W}^{(l)}\Big),\tag{4}$$

其中:$\boldsymbol{H}_v^{(l)}$表示节点v在第l层的表示;$N(v)$表示节点v的邻居节点的集合;$\boldsymbol{H}_z^{(l)}$表示邻居节点z在第l层的表示。这使得每个节点能够利用其邻居节点的信息来更新自身的表示,从而实现图信号传递。与传统的图结构信息不同的是,在IOTA网络中,除去创世交易,每个交易都需要认证两个交易以加入网络,每个交易的出度才是IOTA网络中各交易的有用度数。对公式(4)中度的运算规则需要做一些改变,即

$$\boldsymbol{H}_v^{(l+1)}=\sigma\Big(\sum_{z\in N(v)}\frac{1}{deg(v)-2}\boldsymbol{H}_z^{(l)}\boldsymbol{W}^{(l)}\Big)。\tag{5}$$

但这个规则并不适用于尖端交易,由于尖端交易刚加入IOTA网络,减去出度后,尖端交易的度数之和变为0,会出现无穷大的情况。所以针对尖端交易,改变图信号传递公式为

$$\boldsymbol{H}_v^{(l+1)}=\begin{cases}\sigma\Big(\sum_{z\in N(v)}\frac{1}{deg(v)-2}\boldsymbol{H}_z^{(l)}\boldsymbol{W}^{(l)}\Big), N(v)>2,\\ \sigma\Big(\sum_{z\in N(v)}\frac{1}{deg(v)-1}\boldsymbol{H}_z^{(l)}\boldsymbol{W}^{(l)}\Big), N(v)=2,\end{cases}\tag{6}$$

其中:$deg(v)=2$代表刚加入网络的尖端交易,此时它们的邻居节点只有两个。在信息传递后,应用一个非线性激活函数σ,具体使用ReLU,以增加网络的非线性,整个信息传播过程可以表示为

$$\boldsymbol{H}^{(l+1)}=\sigma(\tilde{\boldsymbol{A}}\boldsymbol{H}^{(l)}\boldsymbol{W}^{(l)})。\tag{7}$$

在GCN中,需要引入归一化项,以处理不同节点的邻居数量的情况,其中每个节点的归一化通常涉及邻居节点的特征的平均或加权平均。每个节点的归一化可以表示为

$$\boldsymbol{H}_v^{(l+1)}=\sigma\Big(\sum_{z\in N(v)}\frac{1}{\sqrt{deg(z)deg(v)}}\boldsymbol{H}_z^{(l)}\boldsymbol{W}^{(l)}\Big)。\tag{8}$$

此时,$\boldsymbol{H}_v^{(l+1)}$表示节点v经过归一化后的特征,这种形式的归一化有助于将节点的特征更新为与其邻接节点的平均特征相关的值,从而在卷积操作中考虑了节点的局部邻居信息。

本文使用了两个卷积层,激活函数分别采用 ReLU 和 softmax,整体的正向传播的公式为

$$\boldsymbol{Z} = f(\boldsymbol{X},\boldsymbol{A}) = \mathrm{softmax}(\tilde{\boldsymbol{A}}\mathrm{ReLU}(\tilde{\boldsymbol{A}}\boldsymbol{X}\boldsymbol{W}^{(0)})\boldsymbol{W}^{(1)})。\tag{9}$$

最后,计算二分类交叉损失函数,即

$$\mathcal{L} = -\frac{1}{N}\sum_{i=1}^{N}[y_i\log(y\_hat) + (1-y_i)\log(1-y\_hat)],\tag{10}$$

其中:y 是样本标签,如果样本属于正例,取值为 1,否则取值为 0;y_hat 是模型预测样本是正例的概率。得到的损失函数一方面说明了训练的 GCN 模型性能的好坏;另一方面也说明了模型的预测值与真实标签是否接近。

2.4　MCMC-I 算法

MCMC 尖端选择算法又称有偏随机漫步算法,是 IOTA 网络中常用的尖端交易选择算法。MCMC 算法的目标是选择两个尖端交易以创建一个新的交易,并将其添加到 Tangle 中。该算法的步骤如下。

1) 选择所有累积权重在 $[S,2S]$ 之间的交易(S 是个足够大的数)[17]。

2) 独立地将 N 个粒子(particle)放置到 1)中选定的交易上。

3) 上述 N 个粒子分别独立运行离散时间随机行走,该行走指向缠结中的尖端交易,即从交易 x 到交易 y 的转移是可能的,当且仅当 y 证明 x。

4) 若 y 证明 x,U_x,U_y 分别为交易 x 和交易 y 的累积权重,则粒子从 x 转移到 y 的概率 $\exp(-\alpha(U_x-U_Y))$ 成正比,计算公式为

$$P_{xy} = \exp(-\alpha(U_x-U_Y))\Big(\sum_{z;z\rightsquigarrow x}\exp(-\alpha(U_x-U_z))\Big)^{-1},\tag{11}$$

其中:z 代表与节点 x 相连的其他节点;α 是用于调整转移概率分布控制参数,且 $\alpha > 0$。

5) 删除很快到达尖端交易的游走子,因为这些尖端交易是“懒惰尖端交易”。找出最先到达尖端交易的两个粒子。若两个尖端交易没有冲突,则输出这两个尖端交易;否则,另选两个没有冲突的尖端交易。

在传统的概率选择机制中,寄生链会倾向于集中认证一个大权重交易以增加游走子选中自己的概率,同时增加该交易的入度,导致潜在的局部偏差和不均匀性,使该节点往往被过度选择。为了减少这种偏差,本文提出了 MCMC-I 算法,该算法在传统 MCMC 算法基础上引入了针对大入度节点的惩罚机制(incorporation of a penalty mechanism, IPM),这一算法对选择概率进行了重新调整,旨在减少对大入度节点的选择概率,并同时增加对被遗漏节点的选择概率,对于那些较少被访问的节点赋予更高的概率。具体采用了一个基于节点入度 I_Y 的修正因子对其进行修正,并加入概率计算中。这个修正因子导致大入度节点的选择概率相对降低,公式为

$$Q_{xy} = P_{xy} + 1/(I_Y+1),\tag{12}$$

其中:Q_{xy} 为加入修正因子后粒子从 x 转移到 y 的概率。之后对该算法进行归一化,即

$$NP_{xy} = Q_{xy}/\sum Q_{xy},\tag{13}$$

其中:NP_{xy} 为归一化后粒子从 x 转移到 y 的概率。通过这一调整达到了两个目标:一方面,减少了对大入度节点的选择概率,提高了算法的平衡性和稳健性;另一方面,增加了对被遗漏节点的选择概率,促进了对网络全局性质的探索,使网络更加稳定。

3　实验验证

本章通过损失函数、预测准确率、召回率和 $F1$ 值等指标评估所提方案的可靠性。由于 IOTA 网络的随机性,目前尚无通用的开源数据集可用于训练和测试,本文采用自生成数据集进行实验。训练集基于随机生成的 IOTA 网络结构图中的交易属性构建,而测试集则来源于规模相同的随机生成 IOTA 网络结构中的交易。通过从交易属性中提取特征值用于模型训练,并对测试集进行预测,将预测标签与实际标签对比计算模型的损失值及各项评估指标,从而验证模型的有效性和特征值的适用性。

3.1　实验设置

实验在配备 Windows 11 操作系统的机器上进行,使用 R7 6800H 处理器和 16 GB 内存,未使用 GPU,而是利用 16 个逻辑 CPU 核心,编程语言为 Python。

由于缺乏专用的 IOTA 仿真平台,且无法获取 IOTA 的真实结构,本实验采用仿真方式生成带有寄生链的 IOTA 网络。该过程分为生成随机 IOTA 网络和在其上加入寄生链两部分。实验使用阿尔伯特(barabási-albert, BA)模型生成 IOTA 网络的拓扑结构[18],其具有以下特点:1) 度分布呈幂律,少数节点连接较多;2) 节点重要性,新节点倾向于连接高累计权重的节点;3) 网络鲁棒性,对随机故障鲁棒,但对有针对性攻击脆弱,这与 IOTA 在寄生链攻击下的表现一致。

随后,在生成的常规网络中加入寄生链交易,创建寄生链的步骤为:1) 提取网络中与被攻击交易无

关的交易组成集合 $attached = \{a1, a2, \cdots, an\}$，用于寄生链交易的认证；2）预设寄生链交易数 *parasite_nodes* 所占比例为网络交易总数的 25% ~ 30%[9]；3）使寄生链交易中的前 k 个交易依次认证前一个交易和集合 *attached* 中的交易；4）余下的寄生链交易按标准 DAG 规则认证寄生链中的交易。

算法 1 寄生链的创建

输入：只有常规交易的 DAG 图，网络交易总个数 *all_nodes*，寄生链交易依附在常规交易上的交易集合 *attached*。

输出：带有寄生链的 DAG 图。

1） *parasite_nodes*←25% to 30% of *all_nodes*

2） k←*parasite_nodes*/2

3） *parasite_chain*←初始化空的寄生链列表

4） for i=1 to k do

5） 创建寄生链交易 *parasite_i*，认证 *parasite_i*−1 与 *attached* 中的某项交易

6） 将 *parasite_i* 加入 *parasite_chain*

7） end for

8） for i=k+1 to *parasite_nodes* do

9） 创建 *parasite_i*，认证 *parasite_chain* 中的两个随机交易

10） 将 *parasite_i* 加入 *parasite_chain*

11） end for

按照此规则，先生成带有寄生链的 DAG，提取其节点特征值作为训练集。然后，生成另一个 DAG，提取其节点属性作为测试集。为确保检测的针对性，训练集和测试集中的总交易数量与寄生链交易数量保持一致。

3.2 参数设定

在 IOTA 网络中，随着交易速率的提升，单位时间内发布的交易量增加，导致攻击成本上升、攻击效率下降。本文采用 MCMC-I 作为游走子选择尖端交易的算法，记录了在不同规模的 IOTA 网络中，攻击者算力不变时，游走子漫步到寄生链节点的概率，如图 2 所示。

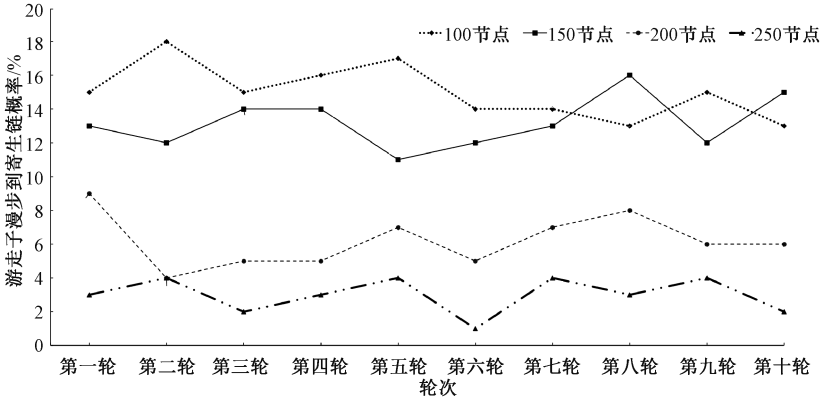


图 2 游走子在不同网络规模漫步到寄生链交易概率

Figure 2 On different network scales, the probability of a random walker selecting a parasitic chain transaction

图 2 中，横轴为实验轮次，纵轴为游走子漫步到寄生链的概率。随着 IOTA 网络节点规模增大，且攻击者算力不变，游走子到达寄生链的概率逐步下降；在 200 节点时降至 10%以下，250 节点时进一步降至 5%以下。这表明随着网络规模增大，攻击成功率显著降低，攻击成本增加。而在网络初期，攻击成功率较高（平均超过 15%），所需算力也更低，因此更易被攻击。文献[8]指出，寄生链在网络初期威胁更大，交易速率上升将使攻击难度增加。文献[19]分析了攻击成功的成本函数，并指出小规模网络中的攻击成本更低。鉴于此，本文实验重点在于评估模型在 IOTA 网络初期中的预测效果，交易规模选择 100、150、200 节点。

3.3 模型损失值评估

在本实验中，超参数设置如下：训练的迭代次数 *num_epochs* 为 100，Adam 优化器的初始学习率 *lr* 为 0.001，第一个图卷积层包含 8 个隐藏单元，第二个图卷积层的隐藏单元数为 2。由于整个图的节点都被同时用作训练集，因此未进行批处理训练。

该实验采用交叉验证的方式验证 GCN 模型的稳定性和可使用性。在使用交叉验证的方法对模型进行评测时，平均测试集损失值是一项很重要的评估标准。取 10 次损失值的平均数为一轮，得到的每轮平均损失值如图 3 所示。

图 3 中，平均损失值的最大值范围在[0.530, 0.560]，最小值范围在[0.520, 0.545]，平均损失值收敛在 0.54 左右。当节点个数不同时，同一轮次表现出的损失值极差范围在[0.025, 0.16]，这意味着模型在不同节点下均表现出鲁棒性，具有较强的泛化能力。

3.4　模型预测评估

对不同节点规模的网络进行 10 轮预测,得到的模型预测的准确率结果如图 4 所示。

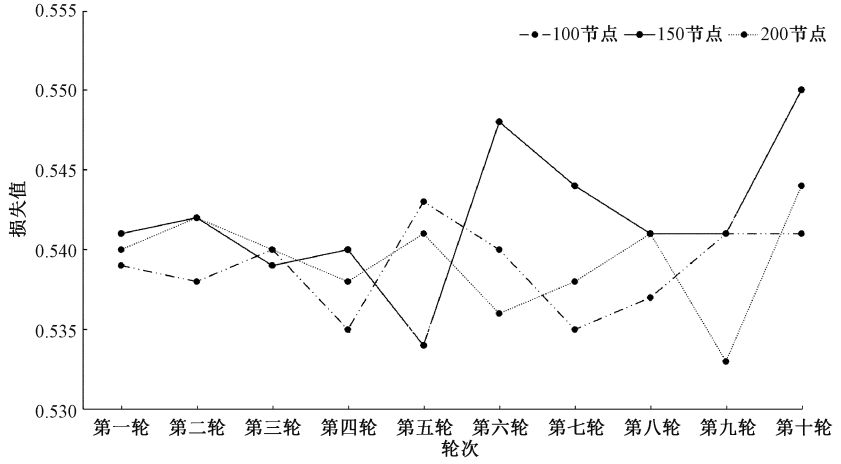


图 3　每轮平均损失值

Figure 3　Average loss value per round

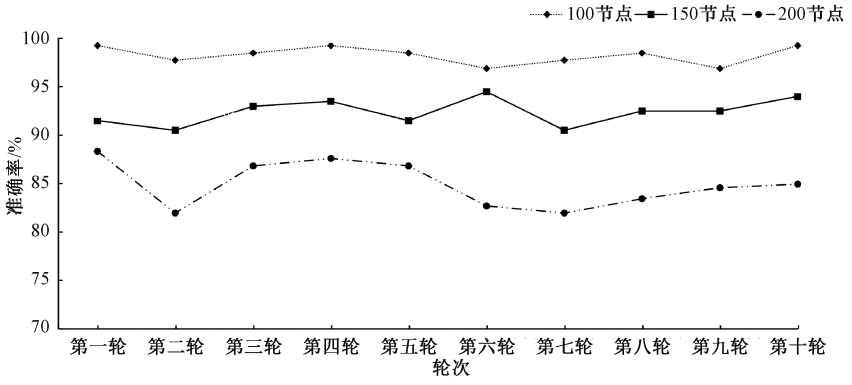


图 4　每轮预测准确率

Figure 4　The accuracy of predictions per round

图 4 数据显示,随着节点规模增加,预测准确率有所下降。这是因为随着 IOTA 网络节点增多,其结构复杂性和噪声因素逐渐增多,影响了模型的预测效果。然而,即便在复杂的 200 节点网络中,模型仍保持了 80%以上的预测准确率。在 100 节点时,模型准确率达到 95%以上。150 节点时也能达到 90%以上。这表明所提特征值在区分正常与异常节点上有效,模型具有良好的扩展性和鲁棒性,适应不同规模的 IOTA 网络并在恶意节点检测中表现稳定。

此外,准确率、召回率、误报率、漏报率、精确率和 $F1$ 值同样用于评估算法效果,各项指标在不同网络规模下的情况如表 1 所示。

表 1　不同网络规模的各项指标

Table 1　The indicators networks of different sizes

节点数量	准确率/%	召回率/%	误报率/%	漏报率/%	精确率/%	$F1$ 值/%
100	98	94	6	6	97	97
150	93	72	28	28	95	83
200	88	65	35	35	91	76

在 IOTA 网络中,随着节点数量的增加,网络结构的随机性使得预测难度增大,从而导致准确率、召回率、精确率和 $F1$ 值逐渐下降。从表 1 可以看出,尽管面临这些挑战,利用本文提出的特征值与 GCN 方法进行检测,模型仍然表现出色。

这些特征值在区分正例和负例方面展现了优异的性能。尤其是在处理更大规模的节点时,尽管模型的精确率和召回率有所下降,但 $F1$ 值的变化表明本

方法在正例预测的准确性和捕获率之间保持了良好的平衡。这证明了该方法的创新性和优质性,并展示了其在处理复杂网络结构时的稳定性和鲁棒性。

3.5 模型泛化性评估

实验在不同规模的数据集和网络结构下也进行了广泛验证,确保特征选择能够泛化至多样化的场景。实验包括对不同交易规模、带有不同数据结构类型寄生链的 IOTA 网络进行测试。具体为:将创建带有其他数据结构类型的寄生链的 DAG 图,并提取图中各节点的特征值作为新测试集,其中创建新寄生链节点的过程如算法 2 所示。

算法 2 新寄生链的创建

输入:只有常规交易的 DAG 图,网络交易总个数 *all_nodes*,寄生链交易依附的常规交易上 *attached*。

输出:带有寄生链的 DAG 图。

1) *parasite_nodes*←25% to 30% of *all_nodes*

2) n←在 1 到 *parasite_nodes* 之间取随机整数

3) *parasite_chain*←初始化空的寄生链列表

4) for $i=1$ to n do

5) 创建寄生链交易 *parasite_i*,认证 *parasite_i*−1 与 *attached*

6) 将 *parasite_i* 加入 *parasite_chain*

7) end for

8) for $i=n+1$ to *parasite_nodes* do

9) 创建 *parasite_i*,认证 *parasite_chain* 中的某个交易和网络中的某个交易

10) 将 *parasite_i* 加入 *parasite_chain*

11) end for

通过这种方式,随机生成带有新类型寄生链结构的 DAG 图,并提取各个节点的累计权重、入度、未认证的节点的个数,以及未认证的节点的 ID 作为测试集。规定生成的测试集与训练集中的总交易数相同。模型的预测评估如表 2 所示。

表 2 预测新类型寄生链不同网络规模的各项指标

Table 2 Indicators for predicting different network scales of new parasitic chains

节点个数	准确率/%	召回率/%	误报率/%	漏报率/%	精确率/%	$F1$ 值/%
100	98	97	3	3	97	97
150	95	98	2	2	85	90
200	85	58	42	42	78	67

从表 2 可以看出,当处理带有新寄生链结构的 IOTA 网络时,训练的模型在不同规模下的预测准确率和 $F1$ 值等各项指标均表现优异。在 100 节点和 150 节点规模时,模型的准确率、$F1$ 值等指标与表 1 中的结果相差不大。在 200 节点规模时,模型的准确率、召回率和 $F1$ 值比表 1 中的结果有所下降,但准确率仍在 80%以上。这表明在较小规模的 IOTA 网络中,网络的随机性较低,模型具有更高的准确率;而随着网络规模的增加,随机性增强,虽然模型的预测性能有所下降,但仍具有不错的预测效果。

4 结语

本文提出了一种基于 GCN 的 IOTA 网络寄生链检测方法,通过分析寄生链与正常交易的行为差异,提取四个关键特征用于模型训练。实验表明,该方法的预测准确率超过 80%,能够有效识别寄生链交易,展现出创新性和有效性。然而,本研究在特征值的选择上一定程度依赖于直观分析,缺乏足够的理论支持,这可能影响特征的泛化能力。未来的研究将进一步探讨特征值选择的理论依据,确保其更具科学性和合理性。此外,实验基于模拟数据集,未来需要使用真实 IOTA 网络数据进一步验证其实际应用性。未来的工作还应继续研究不同特征选择对 GCN 模型训练的影响,并评估该方法在真实网络环境中的安全性和性能。本研究为区块链安全技术的进一步发展提供了有益参考,旨在推动区块链安全技术的创新与进步。

参考文献:

[1] 刘炜, 马杰, 夏玉洁, 等. 一种基于区块链和梯度压缩的去中心化联邦学习模型[J]. 郑州大学学报(理学版), 2024, 56(5): 47-54.
LIU W, MA J, XIA Y J, et al. A decentralized federated learning model based on blockchain and gradient compression[J]. Journal of Zhengzhou university (natural science edition), 2024, 56(5): 47-54.

[2] 田钊, 金鹏祥, 牛亚杰, 等. 区块链在城市道路智能交通中的应用综述[J]. 郑州大学学报(理学版), 2024, 56(6): 9-16.
TIAN Z, JIN P X, NIU Y J, et al. Review of blockchain application in urban road intelligent transportation[J]. Journal of Zhengzhou university (natural science edition), 2024, 56(6): 9-16.

[3] 刘炜, 彭宇飞, 田钊, 等. 基于区块链的医疗信息隐私保护研究综述[J]. 郑州大学学报(理学版), 2021, 53(2): 1-18.
LIU W, PENG Y F, TIAN Z, et al. A survey on medical information privacy protection based on blockchain[J]. Journal of Zhengzhou university (natural science edition), 2021, 53(2): 1-18.

[4] TANWAR S, GUPTA N, IWENDI C, et al. Next generation IoT and blockchain integration[J]. Journal of sensors, 2022, 2022: 9077348.

[5] 高政风, 郑继来, 汤舒扬, 等. 基于 DAG 的分布式账本共识机制研究[J]. 软件学报, 2020, 31(4): 1124-1142.
GAO Z F, ZHENG J L, TANG S Y, et al. State-of-the-art survey of consensus mechanisms on DAG-based distributed ledger[J]. Journal of software, 2020, 31(4): 1124-1142.

[6] SILVANO W F, MARCELINO R. Iota Tangle: a cryptocurrency to communicate Internet-of-Things data[J]. Future generation computer systems, 2020, 112: 307-319.

[7] 王劲松, 杨唯正, 赵泽宁, 等. 基于有向无环图的区块链技术综述[J]. 计算机工程, 2022, 48(6): 11-23.
WANG J S, YANG W Z, ZHAO Z N, et al. Survey of directed acyclic graph based blockchain technology[J]. Computer engineering, 2022, 48(6): 11-23.

[8] CULLEN A, FERRARO P, KING C, et al. Distributed ledger technology for IoT: parasite chain attacks[EB/OL]. (2019-03-21)[2024-08-21]. https://arxiv.org/pdf/1904.00996v2.

[9] GHAFFARIPOUR S, MIRI A. Parasite chain attack detection in the IOTA network[C]//2022 International Wireless Communications and Mobile Computing. Piscataway:IEEE Press, 2022: 985-990.

[10] PENZKOFER A, KUSMIERZ B, CAPOSSELE A, et al. Parasite chain detection in the IOTA protocol[EB/OL]. (2020-04-28)[2024-08-21]. https://arxiv.org/pdf/2004.13409v1.

[11] CULLEN A, FERRARO P, KING C, et al. On the resilience of DAG-based distributed ledgers in IoT applications[J]. IEEE Internet of Things journal, 2020, 7(8): 7112-7122.

[12] CHEN Y F, GUO Y, WANG Y F, et al. Toward prevention of parasite chain attack in IOTA blockchain networks by using evolutionary game model[J]. Mathematics, 2022, 10(7): 1108.

[13] 马红超. 基于 IOTA 分布式账本数据加密存储与检索技术的研究[D]. 北京: 北京邮电大学, 2021.
MA H C. Research on encrypted storage and retrieval technology of distributed ledger data based on IOTA[D]. Beijing: Beijing University of Posts and Telecommunications, 2021.

[14] 朱新玲. 马尔科夫链蒙特卡罗方法研究综述[J]. 统计与决策, 2009, 25(21): 151-153.
ZHU X L. Review on Markov chain Monte Carlo method[J]. Statistics & decision, 2009, 25(21): 151-153.

[15] HE P, YAN T, HUANG C, et al. Welcome to the tangle: an empirical analysis of iota ledger in the chrysalis stage[C]//International Congress on Blockchain and Applications. Berlin:Springer Press, 2023: 419-431.

[16] KIPF T N, WELLING M. Semi-supervised classification with graph convolutional networks[EB/OL]. (2020-04-28)[2024-08-21]. https://arxiv.org/pdf/1609.02907.

[17] BU G, HANA W, POTOP-BUTUCARU M. E-IOTA: an efficient and fast metamorphism for IOTA[C]//Proceedings of the 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services. Piscataway:IEEE Press, 2020: 9-16.

[18] BARABASI A L, ALBERT R. Emergence of scaling in random networks[J]. Science, 1999, 286(5439): 509-512.

[19] CHEN Y F, TANG X D, YAO R, et al. Security analysis of a parasite chain attack in IOTA based on repeated game[J]. Procedia computer science, 2022, 202: 83-88.