基于交易网络特征增强的比特币异常地址识别

张梦楠,吴礼发
(南京邮电大学 网络空间安全学院,江苏 南京 210023)

摘 要:比特币由于其便捷性、匿名性、全球性、高流动性的特点,为犯罪分子使用其作为价值传递的媒介从事犯罪活动提供了理想的工具,产生大量利用比特币进行勒索、洗钱、非法毒品、武器交易等异常交易问题。传统基于有监督的异常地址识别方法由于交易信息单一,不能全面和准确地反映地址间的关系,异常地址识别率较低。该文提出了一种基于交易网络特征增强的比特币异常地址识别方法。该方法将比特币交易数据转化为复杂网络,并提出一种基于改进的 PageRank 的节点重要性特征构造方法,根据比特币交易特点,引入比特币交易额度和频率相关性得到新的 PageRank 值并加入特征集。通过对不同的机器学习方法进行比较以获得最佳的预测模型,提升检测模型的分类效果。与传统的检测方法相比,结合网络信息的模型具有更好的检测性能,其中极限梯度提升树(XGBoost)分类器效果最好,F1 分数由原来的 0.83 提升至 0.94,AUC 值由原来的 0.88 提升至 0.95。

关键词:比特币;异常地址识别;机器学习;特征提取;网络科学
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2023)09-0008-08
doi:10.3969/j.issn.1673-629X.2023.09.002

Abnormal Address Recognition of Bitcoin Based on Enhanced Transaction Network Features

ZHANG Meng-nan, WU Li-fa
(School of Cyberspace Security, Nanjing University of Posts and Telecommunications, Nanjing 210023, China)

Abstract: Because of its convenience, anonymity, globality and high mobility, Bitcoin provides an ideal tool for criminals to use it as a medium of value transmission to engage in criminal activities, resulting in a large number of abnormal transactions such as extortion, money laundering, illegal drugs and weapons trading. The traditional method of anomaly address recognition based on supervision cannot fully and accurately reflect the relationship between addresses due to the single transaction information, so the recognition rate of anomaly address is low. Therefore, we propose a Bitcoin anomaly address recognition method based on transaction network feature enhancement. This method converts Bitcoin transaction data into a complex network and extracts network features, and proposes a node importance feature construction method based on improved PageRank. According to Bitcoin transaction features, the Bitcoin transaction quota and frequency correlation are introduced to obtain new PR values and add them to the feature collection. By comparing different machine learning methods, we can get the best prediction model and improve the classification effect of the detection model. Compared with the traditional detection methods, the model combined with network information has a better detection performance. Among them, the XGBoost classifier has the best performance. The F1 score increases from 0.83 to 0.94, and the AUC value increases from 0.88 to 0.95.

Key words: Bitcoin; abnormal address recognition; machine learning; feature extraction; network science

0 引 言

比特币交易采用匿名制,用户参与交易的账号不需要与其真实身份进行关联,而是由保证比特币所有权的电子签名中的公钥经过一系列加密运算产生的哈希值(被称为“地址”)来代表。一个账户可以拥有多个比特币地址,用户使用这些地址进行比特币交易。因此即使每笔交易信息都会被公开记录于比特币区块链上,也无法确认每笔交易背后用户的真实身份和这笔交易的真实用途。这种匿名性虽然很好地保障了比特币用户的隐私,但也带来了很多问题,特别是将比特币用于非法活动的支付工具,如恐怖融资、盗窃、诈骗和勒索。

收稿日期:2022-11-18 **修回日期**:2023-03-21
基金项目:国家重点研发计划项目(2019YFB2101704)
作者简介:张梦楠(1999-),女,硕士研究生,研究方向为数据挖掘;通信作者:吴礼发(1968-),男,博士,教授,博导,研究方向为网络安全与软件安全。

比特币异常交易是指勒索诈骗、黑客攻击、混币服务、暗网交易等非法活动中出现的不太正常或不太可能的比特币交易[1],异常地址则是完成这些异常交易的相关地址。近年来,已有不少学者提出了各种比特币异常交易和异常地址识别方法,如基于启发式的地址聚类算法[2-4]、基于无监督学习的聚类算法[5-8]和基于有监督学习的分类算法[9-11]。基于启发式的地址聚类算法,虽然能在一定程度上通过启发条件快速识别哪些地址属于同一用户,但判断该地址是否异常还存在一定限制,且过度依赖人工参与、缺乏灵活性。传统基于无监督的地址聚类方法,由于没有充分利用比特币交易信息,导致较高的误报率与漏报率,且对特征中的噪声较为敏感。基于有监督的异常地址识别方法由于交易信息单一,不能全面和准确地反映地址间的关系,异常地址识别率较低。

针对以上问题,该文提出了一种基于比特币交易网络的特征提取方法,构建了基于交易网络特征的异常地址识别模型 TNF-AARM(Abnormal Address Recognition Model based on Transaction Network Features),该模型将交易数据映射成为网络结构,实现地址与地址之间的关联。在特征构造方面,提出了一种基于改进的 PageRank 节点重要性特征构造方法,然后利用复杂网络相关算法提取其他网络地址特征,最后结合集成学习算法构建分类器,进而对异常地址进行识别。最终模型 F1 分数为 0.94,AUC 值为 0.95。

1　相关工作

近几年来,很多研究人员对比特币异常交易地址识别方法进行了研究。

在无监督学习方面,毛洪亮等人[2]提出一种基于启发式条件的聚类方法,能够对匿名比特币地址进行相关性聚类,从而发现被同一用户团体控制的地址群。Bartoletti 等人[3]利用多输入启发式方法进行聚类,设计出一套描述庞氏骗局的包含标签地址的公开数据集,通过分类方法比对,最后验证随机森林是检测异常地址的最佳分类器。来自浙江大学的吴磊等人[3]收集并分析了四种有代表性的比特币混合服务商的大量交易数据,提出了一个识别混币服务地址的通用抽象模型,利用一种启发式方法在实验数据集中找到了 92% 以上的混币服务交易地址。Patil[5]和 Zambre[6]基于数据挖掘的方法,使用无监督技术 K-means 来检测比特币中的欺诈行为。2014 年,Spagnuolo 等人[7]提出了一个模块化框架 BitIodine,以半自动方式标记用户的身份和行为信息,并应用于调查 CryptoLocker 勒索软件,准确量化了支付的赎金数量以及有关受害者的地址信息。Hirshman 等人[8]试图探索比特币交易系统中的洗钱和混币服务,并且追溯出混币服务的输入端。论文首先把比特币地址中属于同一用户的地址聚合起来,然后使用 K-means 方法将用户聚集到具有相似特性的组中,最终发现各聚类中心中存在一定的异常交易行为。

在有监督学习方面,Lee 等人[9]根据交易特征检测比特币交易中的非法交易地址,以暗网丝绸之路地址为比特币的交易标准进行手动分类,然后用随机森林和人工神经网络算法对 90 多万条交易数据进行模型训练,其中随机森林模型的 F1 指标高达 0.98。Toyoda[10]通过交易模式提出了一种新的提取高收益投资计划(High Yield Investment Program,HYIP)检测特征的方案,分析了 1 500 个相关比特币地址,根据交易频率和比特币位数及其流量等交易特征,利用有监督的机器学习分类器方法进行识别,同时对比了是否使用地址聚类方法验证了模型分类的有效性。Lin 等人[11]将 Toyoda 提到的特征作为基线特征,加入生命周期、交易时间等额外统计特征,将地址或实体的交易发生时间表征为离散随机变量,用这些特征或特征组合使用逻辑回归、支持向量机、XGBoost 等方法训练了 8 个分类器,其中 LightGBM 获得 87% 的准确率,显著提高了比特币地址分类的性能。2021 年,国内学者俞莎莎等人[12]提出交易非法性程度概念——交易不可信度,并提出算法对其进行量化并融合到现有模型,提高了检测精度和召回率。郑子彬等人[13]使用手动检查样本和 XGBoost 基于从智能合约的用户账户提取的账户特征和代码特征建立回归树模型,最后预测出了以太坊上运行的超过 400 个庞氏骗局的智能合约地址。周健等人[14]提出了基于机器学习的欺诈账户地址的检测及特征分析模型,同时引入解释机器学习模型输出(SHapley Additive exPlanations,SHAP)值对数据特征进行分析。

2　文中方法

文中方法的主要思想是将比特币地址的交易关系抽象为一张庞大的网络,利用研究复杂网络的方法提取交易网络特征构造融合交易特征,再结合机器学习技术训练模型进行异常地址识别。这些网络信息的加入实现了地址的从单点到网络、从微观到宏观的信息扩充,提升了对比特币地址认知的全面性。

该文首先对比特币交易数据集和标签数据集进行预处理,提取原生地址特征,再提取节点和边的信息建立比特币交易网络;接着提取研究复杂网络的常用指标作为新的网络特征,将地址的原生特征和网络特征作为新的融合交易特征,结合集成算法建立 TNF-AARM 模型。整体识别技术路线如图 1 所示。

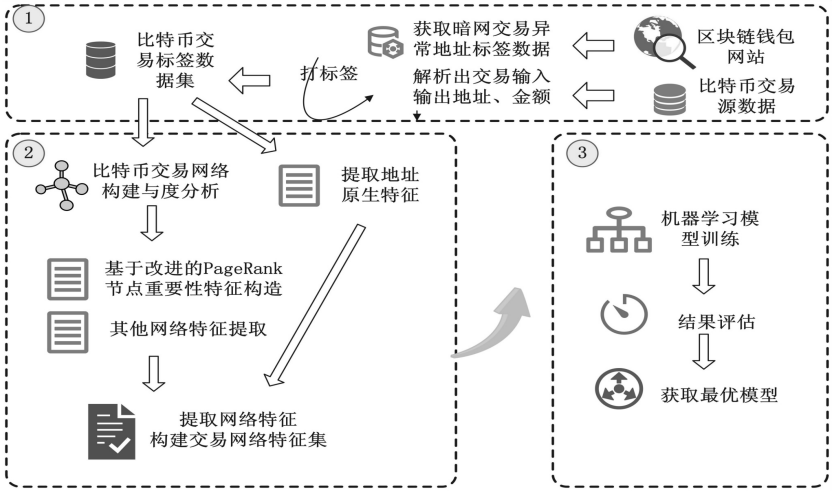

图 1 比特币异常地址识别技术路线

2.1 网络构建与度分析

比特币交易是指资金从某些比特币地址转移至另一些比特币地址的过程[15],每笔交易都由交易输入和交易输出组成,交易输入指明了比特币资金的来源和交易签名,交易输出指明了比特币交易的金额和资金的去向地址,并被比特币资金新拥有者的密钥锁定。比特币区块链上每个区块的第一笔交易由挖矿产生,这笔交易称为币基交易(Coin-Base Transaction),也成为“创币交易”,其挖矿脚本无对应地址即无输入地址,只有输出脚本对应一个交易地址,这个地址就是矿工用来收取奖励的地址。从每个区块的第二笔交易开始,输入脚本和输出脚本分别对应了一个独立的地址,这类既有输入地址又有输出地址的交易被称为普通交易。每笔交易按其双方比特币地址的数量可以分为一对一、一对多、多对一、多对多等交易形式图。

一个典型的网络是由许多节点与连接两个节点之间的一些边组成的,其中节点用来代表真实系统中不同的个体,而边则用来表示个体之间的关系[16]。一个具体的网络可抽象为一个由点集 V 和边集 E 组成的图 $G=(V,E)$。将比特币交易中的每个比特币地址作为节点,交易金额的流向作为边,就可以建立比特币交易网络[17]。

比特币区块链中有若干交易单,交易网络中的节点是交易双方的地址,边代表了比特币在不同地址之间的流动方向,因此分析交易网络就可以分析参与交易的用户之间的地址使用情况[18]。根据交易单中表示的地址关系建立比特币交易网络,输入地址集中每个地址与输出地址集中每个地址均建立一条边,可以组成有向网络。

对于度分布,该文计算了比特币地址交易额度分布和交易频率度分布。如图 2 和图 3 所示,比特币网络中各节点之间存在不均匀分布,整体呈现幂律分布,更类似无标度模型,而非小世界网络或者随机图。网络中少数节点拥有极其多的链接,而大多数节点只有很少量的连接。

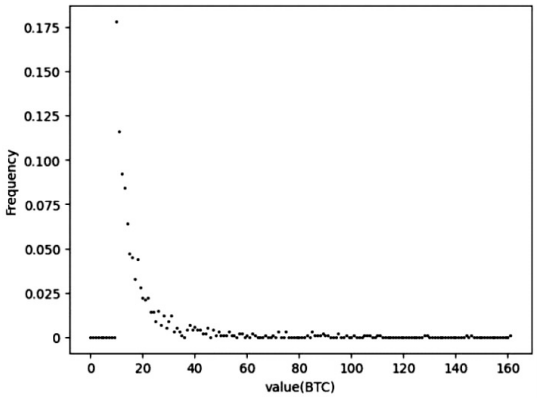

图 2 交易额度分布

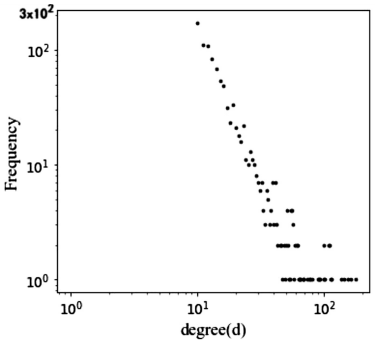

图 3 交易频率分布

由此可以看出在区块链网络中,大多数节点只有极少数量和极小金额的交易。根据以上分析,交易金额数量大的但交易数量小的节点是关注的重点,这是因为暗网交易往往会涉及大金额交易;同时,交易数量大且交易金额等额的节点也是关注的重点,因为很多暗网交易有时不是一笔完成,而是通过大量等额的小交易来分批进行。所以异常交易地址会呈现两个特点:一是该地址输入或输出金额很大;二是该地址的输入输出交易数量多且金额相等,这为后续检测算法提供了依据。

2.2　特征提取

比特币交易完整信息包含每笔交易的 txid、hash、vin、vout 等字段信息,首先根据这些信息解析出输入、输出地址以及每笔交易的金额再结合映射表,去除多余数据;接着提取交易地址的特征,包括该地址分别作为输入、输出地址的交易数量、交易金额等用于训练机器学习模型的关键特征。因为异常地址可能表现出一些共同特征,例如高输入频率、一笔交易中有多个相同的输出等,故从交易数据中提取出了 12 个特征,详细特征集名称及其描述如表 1 所示。

表 1　原生地址特征集

名称	描述
balance	该地址的比特币余额
in_value	该地址的输入总金额
out_value	该地址的输出总金额
indgree	该地址作为输入地址时接收的交易数
outdgree	该地址作为接收地址时接收的交易数
tx_total	与该地址有关的总交易数
txin_rate	输入频率
txout_rate	输出频率
in_value_ave	输入金额均值
out_value_ave	输出金额均值
rate	$\text{rate} = \frac{\text{outdgree} - \text{indgree}}{\text{outdgree} + \text{indgree}}$
rate_tran	$\text{rate\_tran} = \frac{\text{indgree}}{\text{outgree}}$
days	地址存活天数

在网络科学研究中,最受关注的研究指标一般是节点的度、平均路径长度、聚类系数和度分布[19]。对于区块链网络,由于匿名性的限制,难以将大量未标注的具体账户地址与现实相关联。但同样的,由于交易的公开透明,复杂网络的多种指标分析并没有受到干扰[20]。

比特币网络中交易特征是指区块链交易网络中各种统计和聚类分析等指标,如节点数、边数、度、度分布、聚类系数等[21]。此外,该文在此基础上还增加了改进的 PageRank 值、节点的接近中心性、紧密中心性、核心度、约束值等新指标。

2.2.1　基于改进 PageRank 的节点重要性特征构造

PageRank 算法是用于搜索引擎中网页排序的经典算法[20],用来衡量一个页面的重要程度。该算法认为如果一个页面 P 的前置页面越多,代表 P 重要程度越高,且 P 的前置页面的重要程度越高,该算法的模型可以表示为:

$$\mathrm{PR}(x) = \frac{1-\alpha}{N} + \alpha \sum_{i=1}^{n} \frac{\mathrm{PR}(Y_i)}{C_{\mathrm{out}}(Y_i)} \tag{1}$$

式中:$\mathrm{PR}(x)$ 为网页 x 的 PR 值;$\mathrm{PR}(Y_i)$ 为链接到网页 x 的网页的值;$C_{\mathrm{out}}(Y_i)$ 为网页 Y_i 的出链数量;α 为阻尼系数,表示在任意时刻,用户到达某页面后并继续向后浏览的概率。

该文借鉴 PageRank 算法将网页链接价值概念作为重要性排名因素的思想,将其引入复杂网络节点的重要性评估并将其作为新的交易网络特征。

根据 2.1 小节的分析,比特币交易网络中异常地址的交易额度和频率存在一定规律,故在 PageRank 基础上引入交易额度和频率相关性,重新计算节点的 PR 值作为新的交易网络特征加入训练。设地址 i 的节点度为 F_i,交易额度为 T_i,则二者的皮尔逊相关系数 R_{FT} 为:

$$R_{\mathrm{FT}} = \frac{n\sum F_i T_i - \sum F_i \sum T_i}{\sqrt{n\sum F_i^2 - \left(\sum F_i\right)^2} \cdot \sqrt{n\sum T_i^{\,2} - \left(\sum T_i\right)^2}} \tag{2}$$

设节点度的权值为 W_F,则交易额度的权值为 $W_T = W_F \cdot R_{\mathrm{FT}}$,研究地址 i 对其他地址的影响程度时,设地址 m 的全部交易数为 F_m,与地址 i 有交易往来的交易数为 F_{mi},则地址 i 与其它地址的皮尔逊相关系数 R_{mit} 为:

$$R_{mit} = \frac{n\sum F_m F_{mi} - \sum F_m \sum F_{mi}}{\sqrt{n\sum F_m^2 - \left(\sum F_m\right)^2} \cdot \sqrt{n\sum F_{mi}^2 - \left(\sum F_{mi}\right)^2}} \tag{3}$$

地址 m 与地址 i 有交易往来是的权值为 $W_{mit} = W_T \cdot R_{mit}$,地址 i 对地址 m 的影响程度即 $\mathrm{INF}_{im} = W_{mit} + W_F$,故地址 i 的总影响程度即为 $\mathrm{INF}_i = \mathrm{INF}_{im_1} + \mathrm{INF}_{im_2} + \cdots + \mathrm{INF}_{im_n}$,将 INF_{im} 类比到不同地址之间即可得到初步的转移矩阵 $\boldsymbol{m}_{ij}$。在此基础上,该文将比特币交易地址在一个交易网络中的综合影响程度做如下定义:

$$W(i) = \mathrm{Indgree}(i) \cdot \alpha + \mathrm{Outdgree}(i) \cdot \beta + \mathrm{Active}(i) \cdot \gamma \tag{4}$$

其中,$\alpha + \beta + \gamma = 1$,$\alpha$、$\beta$、$\gamma$ 为权值;$\mathrm{Active}(i)$ 表示该地址的活跃度,即:

$$\mathrm{Active}(i) = \frac{n_i}{N} \tag{5}$$

其中,i 表示相关的交易数,N 表示该地址的存活时间。则得到最终的加权概率转移矩阵为:

$$\boldsymbol{M}_{ij} = W(i) \cdot m_{ij} \tag{6}$$

通过公式进行马尔可夫迭代收敛得到最终的 PR 值:

$$\mathrm{PR}_{(u_i)} = d \cdot \sum \mathrm{PR}_u(u_j) \cdot M_{ij} + \frac{1-d}{n} \tag{7}$$

2.2.2　其他网络特征提取

度中心性(Degree Centrality)是网络分析中刻画节点中心性的最直接度量指标。在比特币交易网络

中,一个地址的节点度中心性越高就意味着与其产生交易关联的地址越多,该节点在网络中就越重要。计算公式如下:

$$DC_i = \frac{k_i}{N-1} \tag{8}$$

其中, k_i 表示现有的与节点相连的边的数量, $N-1$ 表示节点 i 与其他节点都相连的边的数量。

介数中心性(Betweenness Centrality)是通过经过某个节点的最短路径的数目来刻画节点重要性的指标,在比特币网络中,介数中心性越高的节点地址在资金流转中所起的作用越大。

$$BC_i = \sum_{v_s \neq v_i \neq v_t, s<t} \frac{\sigma_{st}(v_i)}{\sigma_{st}} \cdot C \tag{9}$$

其中, $\sigma_{st}(v_i)$ 表示从节点 s 到节点 t 的最短路径的总数量, σ_{st} 表示这些最短路径中经过的路径的数量。

紧密度中心性(Closeness Centrality)表示一个节点到网络内其他所有节点的平均距离,一个具有较高紧密度中心性的比特币地址比其他地址更重要。

$$D_c(v_i) = \left[\frac{1}{N-1}\sum_{j\neq i}^{n} g(v_i, v_j)\right]^{-1} \tag{10}$$

其中, N 表示节点所属网络中的节点总数量, $\sum_{j\neq i}^{n} g(v_i, v_j)$ 表示节点和的最短距离。

根据上述对比特币网络的分析,将分析复杂网络的常用指标作为新的特征并加入特征集,如表 2 所示。

表 2 交易网络特征集

名称	描述
degree centrality	度中心性
pagerank	交易网络中节点的重要性
closeness	交易网络的紧密中心性
betweenness	介数中心性
……	……

3 实验与分析

3.1 数据收集与预处理

3.1.1 数据来源

该文使用比特币公开交易数据进行实验研究。该数据集(http://xblock.pro/#/search?types=datasets)由伊诺瓦大学公布,从比特币客户端 bitcore 进行节点同步并获取,记录了截至 2020 年 2 月的比特币交易数据。为了方便使用,该文已经将比特币地址映射为地址 ID。数据集分为以下 6 张表。

(1)表 bitcoin_blockhash,记录了区块链中约 20 万区块的枚举,以 blockID 为索引,记录了区块哈希、创建时间和交易数量等信息,数据维度为(277 443,4);

(2)表 bitcoin_txhash,记录了此数据集中使用的交易 ID 和区块链中使用的交易哈希,数据维度为(30 048 983,2);

(3)表 bitcoin_addresses,记录了字符串表示的比特币地址和此数据集中使用的地址 ID,数据维度为(24 618 959,2);

(4)表 bitcoin_tx,记录了所有交易的枚举,以交易 ID 为索引记录了每笔交易的输出、输出交易数等信息,数据维度为(30 048 983,2);

(5)表 bitcoin_txin,记录了所有类型为输入交易的交易信息,以交易 ID 为索引,记录了发送地址和金额信息,数据维度为(65 714 232,3);

(6)表 bitcoin_txout,记录了所有类型为输出交易的交易信息,以交易 ID 为索引,记录了接收地址和金额信息,数据维度为(73 738 345,3)。

标签数据地址来自论坛网站 Wallet Explorer(https://www.walletexplorer.com/),该网站对比特币地址做了分类,例如交易所、矿池、赌博和暗网。使用 Python3 的 Beautiful Soup 库开发了一个网络爬虫获取该网站下暗网 SilkRoad 截至 2020 年的交易哈希值列表。该列表包含约 5 万条非法交易的地址哈希值。该文根据收集到的标签地址数据,借鉴文献[9]的方式对数据集进行手动标注,其中属于暗网类别下的比特币地址标记为非法(1),其他标记为合法(0)。

3.1.2 数据及配置

尽管收集到的非法交易地址非常有限,仅有 5 万条,相比于 200 万的数据总量呈现数据不平衡现象,但这也符合现实场景中合法交易多于非法交易的情况。在样本不平衡的建模任务中,其实更关注的是少数类别的分类正确情况,这就导致了实际的建模目标和模型本身的优化目标不一致,因此若直接将不平衡的数据应用在样本不平衡较为敏感的模型上,例如逻辑回归模型就会侧重于识别合法交易而未能更好地识别非法交易节点。在实验中,为避免数据不平衡现象造成的影响,考虑对样本量偏大的数据进行随机下采样,仅随机选取数据集的一部分,最终以 10∶1 比例选取合法交易和非法交易数据组成实验所用数据集。具体数据分割见图 4。

3.1.3 模型评价指标

在分类任务中,最常用的评价指标是准确率(Accuracy)、精确率(Precision)、召回率(Recall)、F1 分数(F1-score)和 AUC 值,其详细定义如下:

$$Accuracy = \frac{TP + TN}{TP + FN + FP + TN} \tag{11}$$

$$Precison = \frac{TP}{TP + FP} \tag{12}$$

$$Recall = \frac{TP}{TP + FN} \tag{13}$$

$$F1-score=\frac{2\cdot P\cdot R}{P+R}=\frac{2\cdot TP}{M+TP-TN} \tag{14}$$

$$AUC=\frac{1}{2}\sum_{i=1}^{m-1}(x_{i+1}-x_i)(y_i-y_{i+1}) \tag{15}$$

其中,m、TP(true positive)、FP(false positive)、TN(true negative)和 FN(false negative)分别表示样本总数、真正例数、假正例数、真反例数和假反例数。ROC 曲线是以 FP 为横坐标,TP 为纵坐标绘制出来的曲线,AUC 值表示 ROC 曲线下面积和,x_i、y_i 分别表示 ROC 曲线上的横纵坐标值。

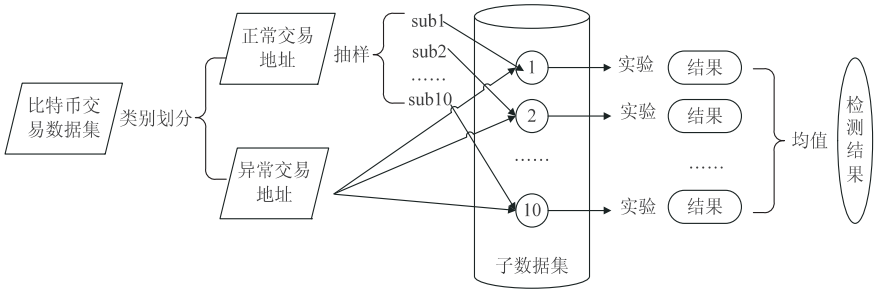

图 4　数据集分割示意图

3.2　建立模型

3.2.1　数据准备

为验证文中方法的优越性,将根据文献[9]使用的特征提取方法建立基模型,旨在排除表现不佳的分类器对实验结果的影响,为后续模型算法选择做准备以及作为文中改进方法的对照组。数据准备包括以下几个部分:

(1)划分训练集和测试集。由于使用随机下采样的方法在数据层面排除了样本不平衡对分类的影响,故直接采用随机划分训练集和测试集的方法,利用 Python3 中 sklearn 包中的 train_test_split 函数得到比例 7∶3 的训练集和测试集数据,通过设置参数 random_state 增加参与训练的数据的随机性,对数据集共进行 10 轮训练。

(2)特征标准化。为避免某一个取值范围特别大的特征对距离或梯度计算造成影响,需要对数据进行标准化,将数据按均值中心化再按标准差缩放,从而加快求解速度和提升模型精度。调用 sklearn 中的 preprocessing. StandardScaler 模块标准化特征矩阵。

3.2.2　训练模型

对上述处理好的数据,分别使用单分类器算法 LR、SVM 和集成分类器算法 RFC、GBDT、XGBoost(简称 XGB)建立分类模型,模型用于测试集数据,得到非法地址的分类精确率、召回率、F1 分数等 10 轮训练后的平均值结果。

依据第 2 节所述,首先提取节点和边的信息。在所研究的数据集中,首先连接表 bitcoin_txin 和表 bitcoin_txout,找出所有交易对应地址的输入和输出关系,然后生成一张记录源节点地址哈希值和目标节点地址哈希值的边表,存储为 CSV 格式,该表记录了每笔交易的输入和输出地址 ID,表的维度为(1 048 575, 2)。根据此地址关系数据集,调用 python3 中的 igraph 包建立有向图,根据图节点的属性提取各网络指标作为新的特征集。将数据集随机分成 10 组建立模型并应用到测试集,10 组数据集的训练结果均值见表 3。

表 3　训练结果

方法	模型	指标				
		Accuracy	F1-score	Recall	Precision	AUC
文献[9]	LR	0.712 6	0.768 8	0.969 6	0.636 9	0.716 2
	SVM	0.771 8	0.728 5	0.621 2	0.880 8	0.769 7
	RFC	0.862 0	0.834 2	0.973 1	0.793 6	0.863 6
	GBDT	0.814 3	0.838 4	0.977 3	0.734 0	0.816 6
	XGB	0.883 3	0.891 2	0.970 3	0.824 1	0.884 5
TNF-AARM	LR	0.831 8	0.579 1	0.460 3	0.780 7	0.708 4
	SVM	0.924 1	0.842 6	0.807 2	0.881 1	0.885 3
	RFC	0.942 9	0.891 3	0.929 7	0.855 9	0.938 5
	GBDT	0.950 3	0.901 9	0.907 0	0.896 8	0.935 9
	XGB	0.974 3	0.947 2	0.916 1	0.980 5	0.955 0

根据文献[9]方法的实验结果来看,类似于 RFC、GBDT、XGB 这样的集成算法相比 LR、SVM 这样的单分类器在各个指标上表现较好,特别是 XGB 表现最佳。因为强分类器本身就是由若干个弱分类器通过一定的组合策略产生,故强分类器在评价结果上通常是要优于弱分类器的。同时还可以观察到,即使是 XGB 这样的强分类器在准确率、F1 分数和 AUC 值都没有达到 0.9,说明现有特征无法提供更多的信息,模型精度有待提升,需要进一步对输入特征进行处理和优化。

从文中方法的实验结果可以看出,除去 LR 模型,其他各分类器精度都得到了一定提升,强分类器的相关评价分数都达到了 0.9 左右,其中 XGB 分类器表现最佳,在准确率、精确率和 AUC 值上都达到了 0.95。LR 模型精度下降的原因可能是新数据集非线性可分,同时这里两者准确率上升而召回率下降,表示模型倾向于将节点分为非法类,产生了过拟合现象,说明对于线性模型来说,网络信息的加入不仅不能提高分类效果,反而容易被当成噪声进行学习。XGB 这样的 Boosting 算法将分类器通过数据的训练不断迭代优化,有序地逐渐提升分类效果,而像 RFC 是通过交叉验证独立、平行的提升其效果。实验中 XGB 对该文所用数据集的效果最好。

3.3 模型评价与比较

将基于文献[9]方法建立的集成算法模型与基于文中方法建立的集成算法模型按照不同的评价标准进行对比,如图 5 至图 8 所示。

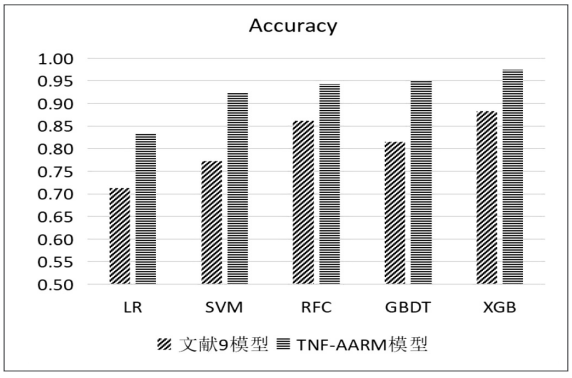

图 5 准确率对比

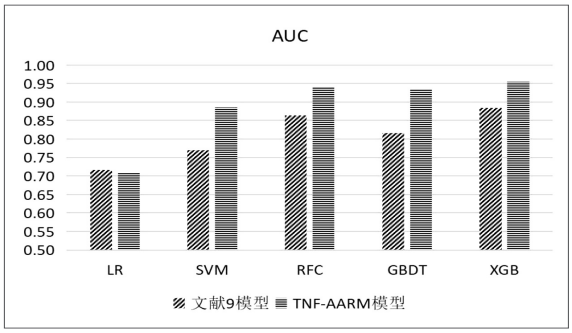

图 6 AUC 值对比

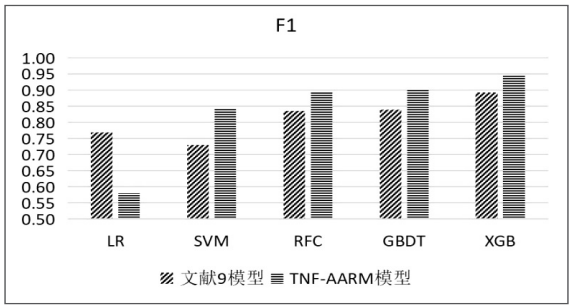

图 7 F1 分数对比

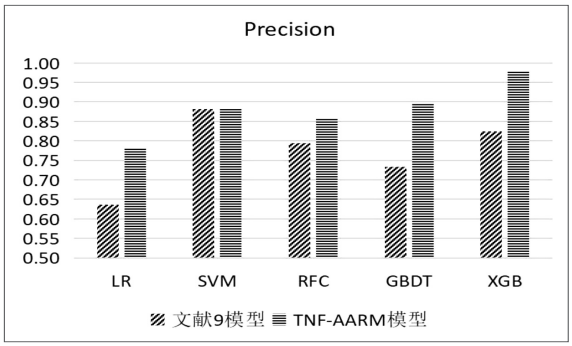

图 8 精确率对比

可以很明显地看到:一方面,对比文献[9]中的地址特征提取方法,该文所使用的方法对大多数不同的分类器在各个指标上都有所提升。在召回率指标上有下降趋势,由 3.1.3 小节准确率和召回率的计算公式可知,二者存在负相关关系,但从作为调和二者的 F1 分数的对比来看,整体结果上文中方法还是优于文献[9]的方法。另一方面,从实验结果可以看到,在这几个强分类器中,XGB 算法表现最佳,得到了最高的 F1 分数和 AUC 值。

综上所述,文献[9]中使用的特征提取方法,在集成算法模型上表现不错,但文中使用的基于交易网络特征的分类方法,在弱分类器和强分类器上都有较好的表现。而文中基于建立比特币网络,借鉴研究复杂网络的方法提取出一些例如介数中心性、pagerank 等作为输入特征,对于模型来说可以明显增加地址与地址之间关系的信息,在此基础上应用集成算法可以有效地提高分类效果。

4 结束语

基于比特币区块链上交易数据,结合复杂网络的拓扑性质和比特币交易的特点,建立比特币交易网络,提取网络特征加入地址特征集,构建了 TNF-AARM 异常地址识别模型。通过与相关文献进行对比表明,该方法获得了更好的分类效果,对于不同的算法模型在精确度、F1 分数和 AUC 值上均有所提升。事实上,虽然构建交易网络增强了比特币地址特征,但没有考虑比特币实时的交易数据和其他公链和币种的交易数据,加入更多数据是否可以获得更为精准的检测模型,

仍然需要继续探究。同时,所采用的有监督学习方法依赖于有标签数据,识别范围较为局限。对跨链、跨币种异常交易检测、细粒度的异常交易行为检测将是下一步的研究重点。

参考文献:

[1] PHAM T, LEE S. Anomaly detection in bitcoin network using unsupervised learning methods[J]. arXiv1611. 03941, 2016.

[2] 毛洪亮,吴　震,贺　敏,等. 基于启发式的比特币地址聚类方法[J]. 北京邮电大学学报,2018,41(2):27-31.

[3] MASSIMO B, BARBARA P, SERUSI S. Data mining for detecting bitcoin ponzi schemes[C]//2018 crypto valley conference on blockchain technology (CVCBT). Switzerland: IEEE,2018:75-84.

[4] WU L, HU Y, ZHOU Y, et al. Towards under-standing and demystifying bitcoin mixing services[C]//Proceedings of the 30th the web conference. Ljubljana:[s. n.],2021:33-44.

[5] PATIL V R, NIKAM A, PAWAR J, et al. Bitcoin fraud detection using data mining approach[J]. Journal of Information Technology and Sciences,2018,4(2):102-106.

[6] ZAMBRE D, SHAH A. Analysis of bitcoin network dataset for fraud[J]. Unpublished Report,2013,27:66-72.

[7] SPAGNUOLO M, MIAGGI F, ZANERO S. Bitiodine: extracting intelligence from the bitcoin network[C]//International conference on financial cryptography and data security. Christchurch:[s. n.],2014:457-468.

[8] HIRSHMAN J, HUANG Y, MACKE S. Unsupervised approaches to detecting anomalous behavior in the bitcoin transaction network[J]. Stanford: Stanford University,2013:34-42.

[9] LEE C, MAHARJAN S, KO K, et al. Toward detecting illegal transactions on bitcoin using machine learning methods[M]//Blockchain and trustworthy systems. Beijing: Springer,2020:520-533.

[10] TOYODA K, OHTSUKI T, MATHIOPOUL P T. Identification of high yielding investment programs in bitcoin via transactions pattern analysis[C]//IEEE global communications conference. (GLOBE-COM). [s. l.]: IEEE:2017:1-6.

[11] LIN Y J, WU P W, HSU C H, et al. An evaluation of address classification based on transaction history summarization[C]//IEEE international conference on blockchain and cryptocurrency (ICBC). [s. l.]: IEEE:2019:302-310.

[12] 俞莎莎,牛保宁. 基于交易不可信度的比特币非法交易检测[J]. 计算机工程,2022,48(8):166-172.

[13] CHEN W, ZHENG Z, CUI J, et al. Detecting ponzi schemes on ethereum: towards healthier blockchain technology[C]//World wide web confernce. Lyon: International World Wide Web Conferences Steering Committee,2018:1409-1418.

[14] 周　健,张　杰,闫　石. 基于链上数据的区块链欺诈账户检测研究[J]. 计算机应用研究,2022,39(4):992-997.

[15] 张明德,储志强. 基于区块链技术的比特币体系原理研究[J]. 信息网络安全,2020(S2):151-154.

[16] 周　涛,柏文洁,汪秉宏,等. 复杂网络研究概述[J]. 物理,2005,34(1):31-36.

[17] 邢　尧. 比币交易网络的去匿名化技术研究[D]. 南京:东南大学,2017.

[18] 孟　婷. 比特币网络中交易数据特征研究[D]. 北京:北京邮电大学,2021.

[19] 汪小帆,李　翔,陈关荣. 网络科学导论[M]. 北京:高等教育出版社,2012:248-250.

[20] 李南铮. 比特币的网络交易特征分析及实体识别算法研究与设计[D]. 成都:电子科技大学,2021:22-24.

[21] PAGE L, BRIN S, MOTWANI R, et al. The PageRank citation ranking: bringing order to the Web[EB/OL]. (2012-05-13). http://ilpubs. standford. edu:8090/422/.