区块链网络中关键性节点评估

陈立军[1] 张 屹[1] 陈孝如[1] 杨 微[1] 何 培[2]

[1](广州软件学院软件工程系 广东 广州 510990)

[2](广州大学计算机网络工程学院 广东 广州 510006)

摘 要 区块链系统正在被快速地集成到各种技术中,而底层网络拓扑结构对区块链性能的影响非常有限。该文提出基于符号变化的频谱划分方法,研究每个网络节点对整个区块链性能的重要性,通过根据不同的临界性指标来选择关键性节点评估,并使用模拟实验来调查删除这些节点后产生的性能退化,得出最关键的节点是导致性能下降最大的节点。同时,与现有的中间中心性、紧密中心性和程度中心性等关键指标进行比较发现,在删除这些关键节点时区块链性能下降得更快,因此该方法优于现有的三种方法,维护了区块链的安全和稳定。

关键词 区块链 关键性节点 区块链攻击 区块链安全性 网络分析

中图分类号 TP311.13 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2024.12.049

EVALUATION OF THE CRITICALITY OF NODES IN THE BLOCKCHAIN NETWORK

Chen Lijun[1] Zhang Yi[1] Chen Xiaoru[1] Yang Wei[1] He pei[2]

[1](*Department of Software Engineering, Software Engineering Institute of Guangzhou, Guangzhou 510990, Guangdong, China*)

[2](*School of Computer Network Engineering, Guangzhou University, Guangzhou 510006, Guangdong, China*)

Abstract Blockchain system is rapidly integrated into the various kinds of technology, and the affection from underlying network topology structure the performance of block chain is very limited. This paper presents a spectrum partitioning method based on symbol variation. The importance of each network node to the whole blockchain was studied. We selected the critical evaluation of nodes according to the different criticality index. We used simulation experiment to investigate after remove the node performance degradation and it was concluded that the key of the node was one of the largest nodes, resulting in a decline in performance. At the same time with the existing in the middle of the centricity, degree of tight centricity and centricity key indicators such as comparison, we found that when to remove these key nodes, the block chain performance reduced faster. Therefore, this paper concludes that the proposed method is superior to the existing three methods, thus maintaining the security and stability of the blockchain.

Keywords Blockchain Critical nodes Blockchain attacks Blockchain security Network analysis

0 引 言

随着去中心化数字货币的发明,当今的比特币、技术和网络通信处于十字路口[1],替代传统通信方法的一种可能是支撑比特币的技术,即区块链[2]。区块链具有与 Web 一样大的潜力,已成为可用于形成分布式解决方案的关键技术之一,这激发了研究人员在诸如物联网(IoT)[3-4]、智能电网基础设施[5]和医疗保健系统等领域选择基于区块链的架构。

区块链是经过密码验证的分布式分类账,为网络中的用户维护一组交易记录,这些事务反映了用户之间的信息交换,并借助数据泛洪在整个网络中进行中继,交易一旦生成,就会在整个网络中泛洪,一旦到达

收稿日期:2021 - 03 - 01。2018 年度广东省普通高校重点科研平台和科研项目(2018KQNCX395);广东省质量工程项目(ky20160001)。**陈立军**,讲师,主研领域:区块链。**张屹**,教授。**陈孝如**,副教授。**杨微**,讲师。**何培**,教授。

几个功能强大的节点,便会验证其真实性。这些功能强大的节点在网络中称为矿工,矿工通过将经过验证的交易区块泛洪到网络上来维护数据交换协议,以便每个其他节点都可以更新其分类账,每个网络都是在网络完全连接的基本假设之上,这意味着每个事务在相同的时隙中被每个矿工接收,并且由矿工发起的每个数据泛洪到达网络中所有可能的节点。实际上,区块链可能具有拓扑限制,例如,网络上的僵尸网络攻击[6]或 DDoS 攻击都有可能使目标节点无法用于网络通信,而且,如果这种攻击成功地针对了网络中最关键的节点,从而对其进行了分区或破坏,那么由于合法的用户凭据,矿工可以验证一侧到另一侧产生的任何交易,但不能够到达另一部分,因此使解决方案不可行。

过去,已经进行了大量研究来识别这些关键节点,与其他节点相比,这些关键节点对网络的影响更大,由于网络的拓扑结构,这些节点变得越来越重要,一些众所周知的方法是“中间中心性”,它基于节点所参与的最短路径路由的数量来评估节点的关键性;“紧密中心性”,它考虑了节点与所有其他节点的接近程度;程度中心性[7],它使用节点度来突出节点的关键性。众所周知,所有这些方法在其考虑的场景中都可以很好地工作,但是在基于区块链的设置中,节点的可访问性具有最高优先级,因此它们往往会误判节点的关键性。在这项工作中,本文提出基于符号变化的频谱划分方法,并通过特定于区块链的事物流信息进行增强,以突出节点的关键性,所提出的方法将节点视为关键节点的前提是该节点位于某个割集中并经历最高的流量,割集定义为一组节点,这些节点在其邻居之间观察到向量的符号变化[8],对所提出的方法进行了评估,以了解区块链大小和丢包率的变化,并且观察到,从网络上删除最关键的节点后,该方法表现出更大的区块链大小减小和更大的丢包率,从而胜过了现有方法。

1 背 景

区块链近来受到了广泛的关注,重点关注区块链的内在操作特性,例如信息传播[9]、密钥管理[10]、分类账架构、区块链合同[11]和共识协议[12]。区块链网络具有构成其整体功能的众多功能,下面简要说明其中一些最主要的内容。

(1) 交易:交易是由发送方为网络中的特定接收方生成的消息,它包含发送方的公钥、接收方的公钥、传输的数据和签名,该签名由发件人使用发件人的私钥生成,以提高安全性。

(2) 堵塞:区块链是按区块排列的数据链,一个块的头包含几个组成部分,例如时间戳、上一个块的哈希、默克尔树的根哈希和现时值,块的主体包含所有事务,这些交易由矿工验证,然后附加到链上,每个区块都使用哈希码进行标识,该哈希码是使用区块内的内容生成,这包括节点之间的实际事务、时间戳、随机数和前一个块的哈希,因此使其不受随机两次支出攻击的影响,因为即使单个参数的微小变化也会使该块无效。

(3) 默克尔树:默克尔树是基于哈希的数据结构,其中每个叶节点包含事务性块的哈希,每个非叶节点包含其子节点的哈希,默克尔树通过重复散列数据并产生最终的数字指纹来汇总所有已验证的交易。

(4) 时间戳:每个交易块都有一个相关的时间戳,这增强了网络的安全性,并确保新创建的块与所有现有块都一致,其中新块的时间戳不能早于已添加的时间戳。

(5) 矿业:为了将交易添加到区块链中,一些具有所需计算能力的节点会对传入的交易执行加密操作,称为工作量证明,这有助于验证交易的真实性,一名矿工为此工作获得了少量报酬。

(6) 工作量证明(PoW):工作量证明是一种方法,在这种方法中,矿工相互竞争以增加障碍并获得报酬,PoW 方法的目标是解决数学哈希,随着区块链大小的增加,哈希变得越来越复杂[12]。

在基于区块链的设置中,发件人生成交易,使用其私钥进行签名以进行识别,然后在网络上进行广泛传播。每个矿工等待一个预定义的时间,以获取在该时隙中生成的所有交易,并在接收到它们之后将它们组合成一个块,每个块使用其自己的哈希函数进行验证,该哈希函数也构成前一个块的哈希,然后由矿工开采一个区块,并在完成后使用矿工的私钥进行签名。将一个已签名的块广播到网络中,在该网络中,接收此块的每个节点会将其添加到其现有链中。

尽管交易是真实的,但主要有两种情况可以通过区块链模型退出交易:

(1) 触发事务时,将为其分配时间戳,如上所述,在该交易的验证过程中,该过程将检查时间戳是否符合网络的要求标准,如果接收到的时间戳不大于前 11 个时间戳的中间值,则该事务将被拒绝,因为该事务太旧而无法在当前时间进行验证。

(2) 网络的所有节点的公钥最初都浮动在区块链

网络中,当某个节点可能由于恶意攻击而从网络中删除时,它的公钥仍然保留,在验证过程中,网络将检查发送方或接收方是否为空,即两者是否为空节点,如果是这样,则拒绝该交易并且不对其进行验证。

2　方法设计

在区块链环境中,基础网络拓扑在定义节点特征方面起着至关重要的作用。在理想情况下,成功的矿工将是能够以最小的延迟因子在特定时间窗口内接收所有可能交易的矿工。这意味着,如果两个矿工在同一网络上,则最早接收所有交易的一个矿工将比另一个矿工有优势,由于网络丢失,第二个矿工可能不会收到所有交易,或者在定义的时间窗口期满后,第二个矿工可能会收到一个交易。时间窗口是指矿工期望接收所有交易的时间段,一旦收到,它们就会被挖去一块,这些网络丢失可能是由于网络中的节点受损或故障而引起,而数据包接收的延迟可能是由于网络中的瓶颈而引起。为了消除这些问题,及时识别这些关键节点至关重要,这可能会对区块链网络的性能产生重大影响。

考虑到区块链设置的体系结构,这项工作利用了我们先前工作[13]中提出的频谱划分方法,并为其补充了与区块链设置相关的新功能。本文借助标志更改方法来帮助识别网络中的关键节点,提出的方法通过计算网络中所有节点的特征向量,然后根据观察到的符号变化形成割集[14]。特征向量值同时具有正号和负号,这些符号有助于识别网络的两个部分,所提出的方法识别出这些节点,这些节点的相邻节点具有不同的特征向量符号,并将它们标记为割集的一部分,这些节点代表了网络的瓶颈,所有这些节点的删除将导致网络分区[13],属于该割集的节点基于它们正在观察的业务流模式而彼此优先,在区块链设置中,网络流量往返于矿工,因此属于割集的节点(也经历最大流量)被视为网络中最关键的节点。本文正式定义频谱划分方法如下:

让一个简单的无向图 $G=(V,E)$,由顶点集 V 和边集 E 组成,其中 $|V|=n$ 和 $|E|=m$。邻接矩阵 $\boldsymbol{A}$ 是 m 行、n 列的矩阵,其中每一行和每一列对应于 G 的顶点,此矩阵的任何元素 a_{ij} 表示顶点 i 和顶点 j 之间的边数。对于图 G,矩阵 $\boldsymbol{A}$ 将关于主对角线对称,而 a_{ij} 的值将为 1 或 0。矩阵 $\boldsymbol{D}=(d_1,d_2,\cdots,d_n)$,其元素是 G 的所有顶点的度,对于矩阵 $\boldsymbol{D}$ 的任何元素 d_{ii},i 表示图中的顶点,而 d_{ii} 的绝对值是该特定顶点的度,对于矩阵 $\boldsymbol{D}$,d_{ij} 的任何其他元素的值为 0,对于上述图 G,拉普拉斯矩阵 $\boldsymbol{L}$ 定义为:

$$\boldsymbol{L}=\boldsymbol{D}-\boldsymbol{A} \tag{1}$$

因此,$\boldsymbol{L}$ 的对角元素 L_{ij} 等于顶点 v_i 的度,如果顶点 v_i 与 v_j 相邻,则非对角元素 L_{ij} 为 1,否则为 0。特征值和特征向量提供了对图连接性的深入了解,如果存在向量 $\boldsymbol{X}$,则让任何矩阵 $\boldsymbol{A}$ 都使得 $\boldsymbol{AX}=\lambda\boldsymbol{X}$,对于某个标量 λ,则将 λ 称为特征值 $\boldsymbol{X}$ 的 $\boldsymbol{A}$ 的特征值。因此,拉普拉斯矩阵 $\boldsymbol{L}$ 的特征值以升序排列使得 $0=\lambda_1\leqslant\lambda_2\leqslant\cdots\leqslant\lambda_n$,本特征值中的零的多重性代表网络的断开连接的组件数,第二最小特征值 $\mu(G)=\lambda_2$,表示网络的代数连通性,代数连接性越小,网络越容易断开连接。在获得第二最小特征值 λ_2 之后,相应的特征向量 $\boldsymbol{v}=(v_1,v_2,\cdots,v_n)$ 是矩阵 $\boldsymbol{L}$ 的特征向量,特征向量具有正负两个实体,具有不同符号的元素表示相互连接不良的连接的子图。因此,特征值有助于识别图形的那些部分(将其删除)可能会将网络分成两个部分,也称为割集,在网络中,此割集 S 的节点对于整个功能至关重要,对于任何顶点 v,如果其至少一个邻居的特征值的符号不同于其自己的符号,则将其包含在割集 S 中。基于业务流 $T(x)$ 评估割集 S 中的节点的临界性,此产生的优化问题可以定义为:

$$\begin{aligned} &P=\arg(\max T(x)) \quad x\in S\\ &s=\arg(\min u(G(V-\alpha))) \quad \alpha\in V \end{aligned} \tag{2}$$

图 1 说明了该方法的工作原理,每个节点计算其对应的特征向量值,并与相邻节点共享,这些节点评估这些值,并在相邻节点之间看到符号变化时将自己标识为关键节点,这些值在图 1 中表示为节点标签,然后,割集中的节点将观察通过它们的流量,以识别网络中最关键的节点,删除这些节点将对网络产生严重影响,它们将导致由于节点删除而导致的数据包丢失和由于时间戳到期而导致的数据包丢失,让我们考虑在所考虑的场景中删除节点 B,在前一种情况下,如果节点 A 为节点 B 生成交易,则到达矿工 X,该矿工 X 会评估交易的有效性,并由于节点 B 不存在而将其丢弃,在后一种情况下,删除节点 B 将重定向所有流量通过节点 C 会产生瓶颈,从而导致时间戳过期,交易将以延迟的方式到达各个矿区的矿工,因此报告的时间早于可接受的时间窗口,由于时间戳过期,这将导致数据包丢失。此外,从割集中删除所有节点将使网络划分为群集,从而增加数据包丢弃率,这将对区块链的规模产生不利影响,使矿工无法看到在网络另一端进行的任何交易。

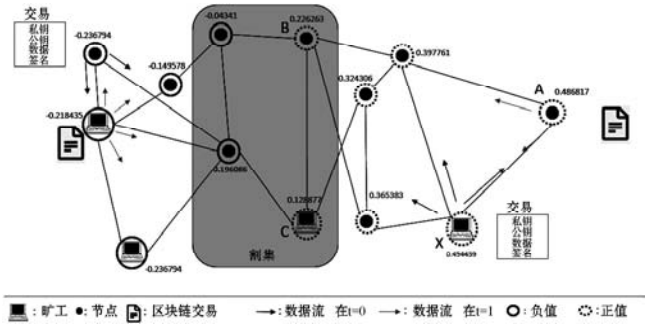


图 1 区块链模型的表示

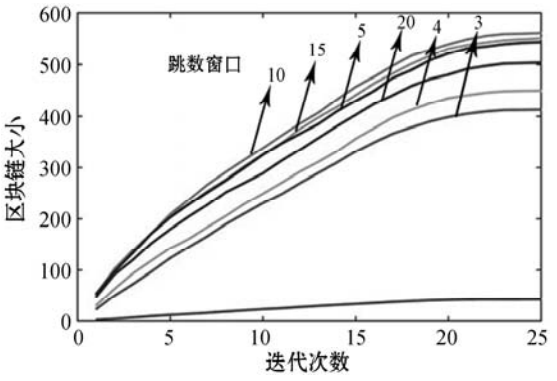
3 仿真与结果

本节将在基于区块链的环境中针对现有方法(介于中间性、紧密性、程度中心性和随机节点去除)方面评估所提出方法的性能。本文报告了区块链大小的变化,由于节点删除导致的数据包丢失增加以及由于跳数限制导致的数据包丢失增加,由于仿真环境的限制,此仿真设置使用了跳数而不是时间戳,其中可接受的时间窗口的上限表示为跳数限制,还对所提出的方法进行了可变网络密度、可变跳数限制和不同矿工数量的评估。

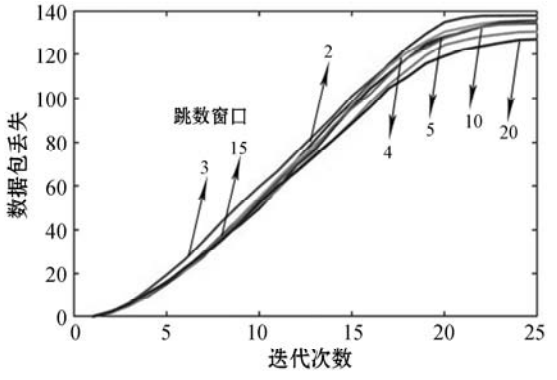
本文考虑使用均匀随机分布将 1 000 个节点互连在一起的网络,该网络在随机选择的发送者和接收者之间生成 1 000 个事务,在每次迭代后进行评估,其中一次迭代覆盖一组随机事务,每次迭代的上限为 100 个事务,本节中报告的结果是平均 50 个随机网络拓扑。

在第一组模拟中,本文以固定的边缘概率 p 评估变化跳数窗口的区块链结果,本文指定 $p=10\%$,并评估跳跃窗口 h 为 2、3、4、5、10、15 和 20。为了更好地说明跳跃窗口的效果,本文假设在此模拟中使用一个矿工,将在以后的仿真设置中删除此假设,以说明该方法的可伸缩性。本文在每次迭代时都会删除属于割集的 10% 节点,并评估结果,重复此操作,直到去除了整个割集为止。

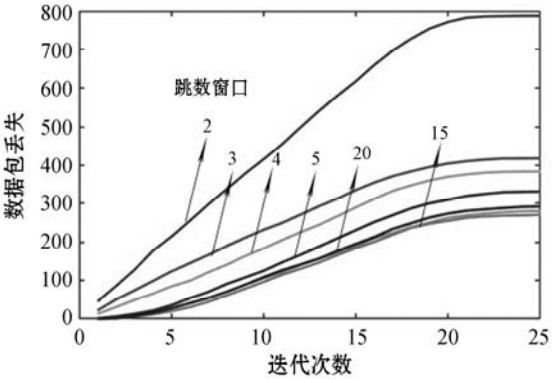
图 2 报告说明,随着跳数窗口从 2 增加到 20,由于跳数而导致的数据包丢弃会减少,如图 2(c)所示,这仅仅是由于可接受的跃点计数窗口增加所致,在该窗口中,即使在覆盖更长的路径后,事务仍然有效,从而使大多数事务都有效。结果还表明线性增加直到大约 20 次迭代,此后数据包丢弃报告无明显变化,这主要是由于交易总数限制为 1 000,跳数导致数据包丢失增加,如图 2(a)所示,减小了区块链的大小,由于删除的节点数量相似,空事务导致的数据包丢弃对所有跃点窗口显示相似的结果。



(a) 区块链大小



(b) 由于空事务包下降



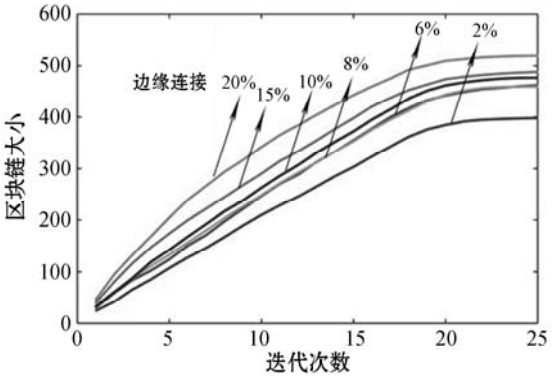
(c) 由于跳数到期包下降

图 2 跳数窗口的变化

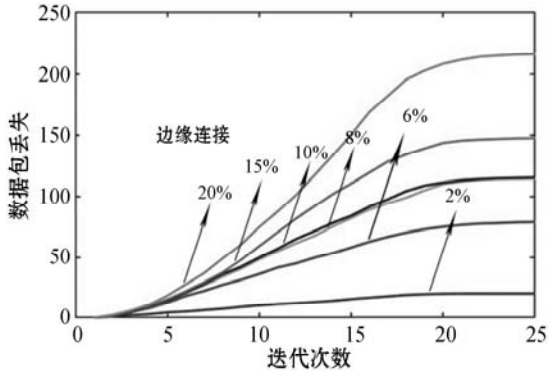
在第二组模拟中,本文用固定的跳数窗口评估了不同边沿概率 p 的结果,指定 $h=4$ 并评估边缘概率,p 为 2%、6%、10%、15% 和 20%,这些模拟是在单个矿工框架上进行的,目的是更好地说明网络密度的影响,在每次迭代时都会删除属于割集的 10% 节点,并评估结果,重复此操作,直到去除了整个割集为止。

图 3 报告说明,随着网络的边缘概率从 2% 增加到 20%,如图 3(c)所示,由于跳数引起的数据包丢失会减少,这是由于网络密度的增加,导致节点之间的连接数量增加,节点间连接性的增加减少了从发送者到接收者所需的跳数。图 3(b)突出显示了由于无效交易增加而导致的数据包丢弃,这可以通过考虑裁切大小来解决,在每个模拟中,都将删除节点,直到割集完

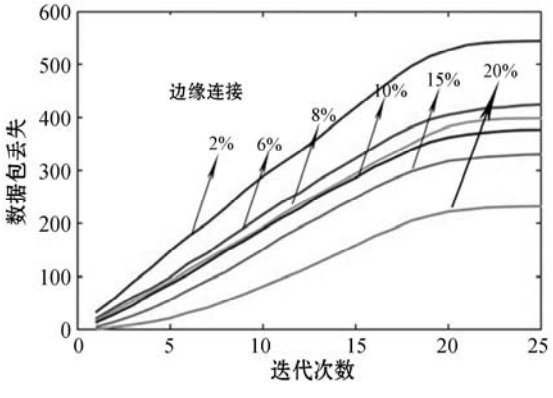
全为空,对于更密集的网络,考虑到节点之间的连接性增加,割据大小会更大。因此,为了更密集的网络,将删除更多节点,这导致网络中的空节点增加,从而由于空事务而增加了分组丢弃,这些下降共同影响了区块链的大小,但是由于跳数限制引起的下降超过了由于无效交易引起的下降,导致了如图 3(a)所示的结果。



(a) 区块链大小



(b) 由于无效交易导致的数据包丢弃

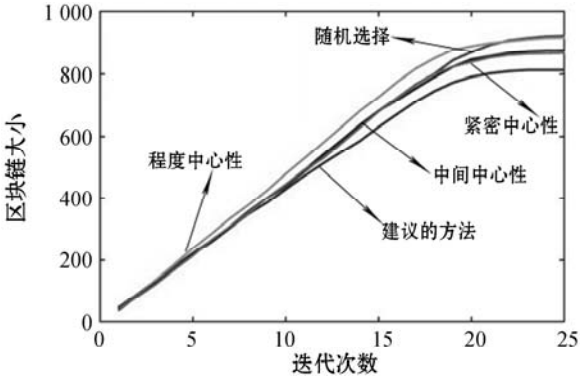


(c) 由于跃点到期的数据包丢弃

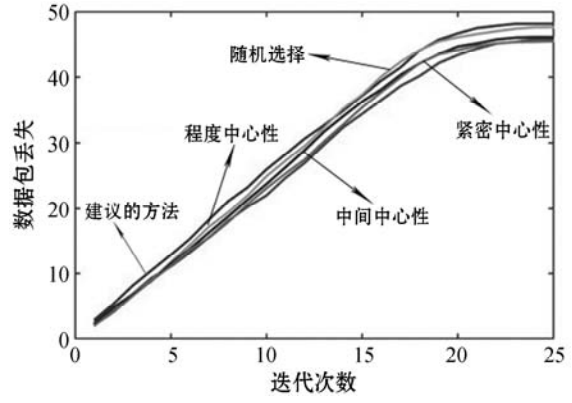
图 3　图表密度的变化

在第三组仿真中,本文将提出的方法与常用的网络分析方法(即随机节点选择、程度中心性、紧密中心性和中间中心性)进行了比较,本文分配 $h=5$ 和 $p=10\%$,这些模拟在单个矿工框架上进行,以更好地说明网络密度和跳数窗口的影响。

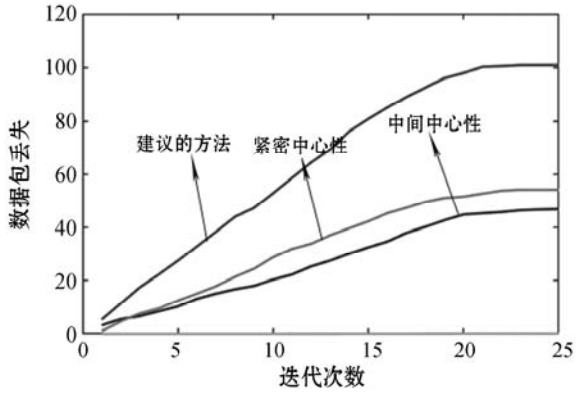
如图 4(c)、图 5(c)和图 5(b)所示,在每次迭代中,本文删除了网络中 10% 的最关键节点,其中删除的节点数是整个网络的 2.5% 、5% 和 10% 的上限。从图 6(c)可以看到,对于本文提出的方法,由于跳跃窗口导致的数据包丢弃量最大,其次分别是介于中间性、紧密性、程度中心性和随机节点选择,如图 4(c)所示。



(a) 区块链大小

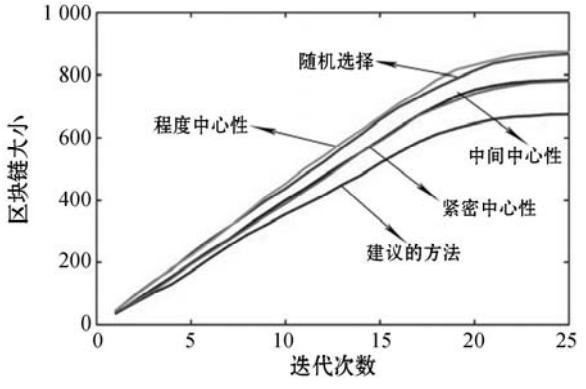


(b) 由于无效交易导致的数据包丢弃

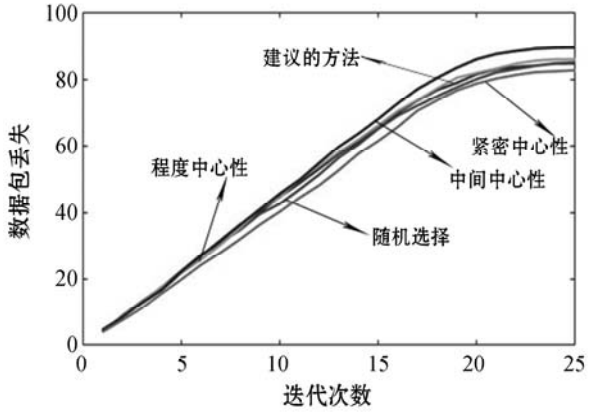


(c) 由于跃点到期的数据包丢弃

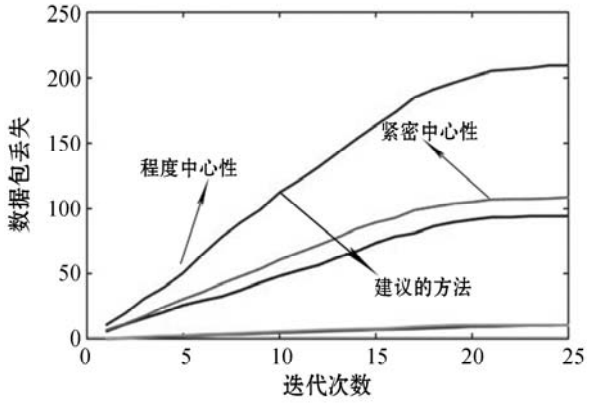
图 4　受攻击的网络的 2.5%



(a) 区块链大小

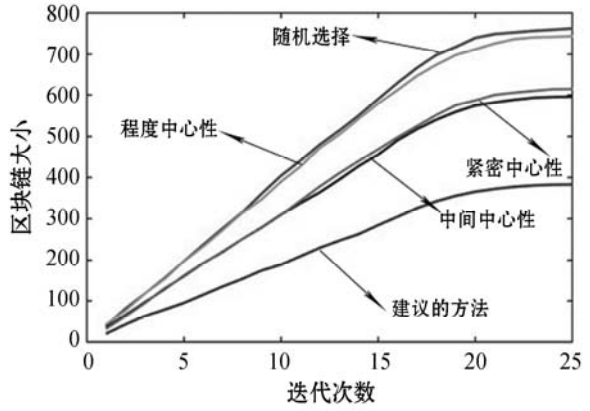


(b) 由于无效交易导致的数据包丢弃

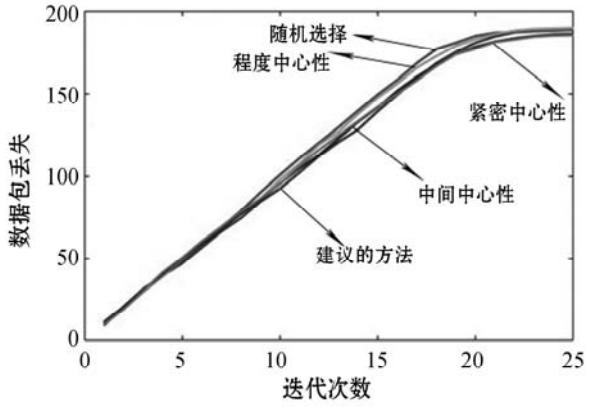


(c) 由于跃点到期的数据包丢弃

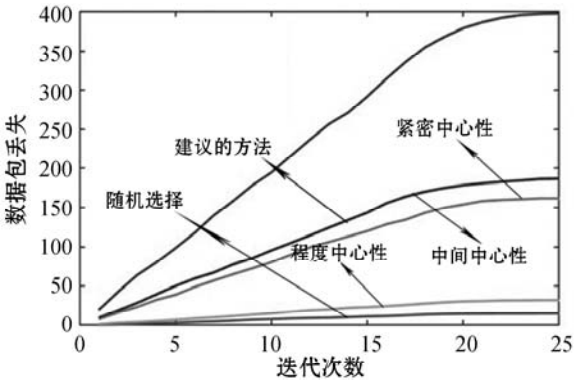
图 5 受到攻击的网络的 5%



(a) 区块链大小



(b) 由于无效交易导致的数据包丢弃



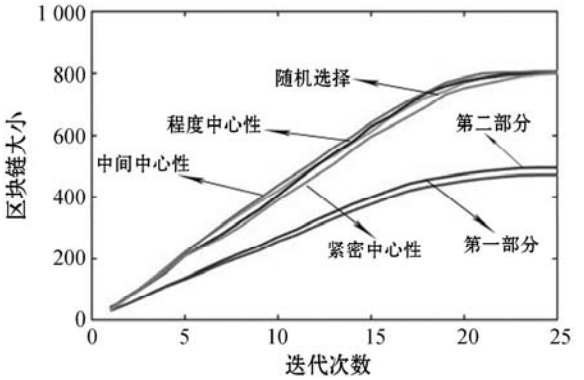
(c) 由于跃点到期的数据包丢弃

图 6 受攻击的网络的 10%

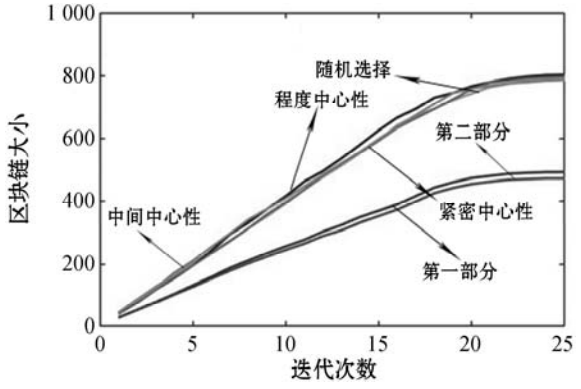
由图 5(c)和图 6(c)可知,由于无效交易导致的数据包丢弃对于所有方法都保持相似,因为删除的节点数与图 4(b)、图 5(b)和图 6(b)中报告的相同。随后,这两个因素影响了区块链的大小,本文方法区块链的大小最小,其次分别是中间中心性、紧密中心性、程度中心性和随机节点选择,如图 4(a)、图 5(a)和图 5(b)所示,图 6(a)由于更好地选择更好的节点,因此提出的方法优于现有方法,这反过来又在网络中造成了瓶颈,从而导致数据包丢失和延迟,当删除的网络百分比从 2.5% 增加到 10% 时,观察到类似的趋势。

在最后一组模拟中,本文证明了所建议的方法与多个矿工之间的可扩展性,并将其与各种网络分析方法进行比较,我们分配 $h=4$ 和 $p=10\%$ 并平均 25 种随机网络拓扑的结果,对于每种网络分析方法,本文都会在迭代开始时删除整个割集。

图 7(a)和图 7(b)分别以相似的模式突出显示了 3 个矿工和 5 个矿工的结果,本文提出的方法明显优于其他方法。如图 7 所示,在本文的方法中,删除割集后,整个网络被分为两部分。这导致每个部分分别维护其自己的区块链副本,彼此之间不一致。由于网络的划分,两个区块链在本文建议的方法中同时运行,但其他方法则不会发生这种划分。本文的方法与现有三种方法的比较见表 1。



(a) 3 个矿工



(b) 5 个矿工

图 7　多种挖掘方案

表 1　本文方法与现有方法比较

影响	方法	
	现有的三种方法	本文方法
跳跃窗口导致的数据包丢弃量	提议的方法 > 中间性 > 紧密性 > 程度中心性 > 随机节点选择	最大
删除节点数引起区块链的大小	中间中心性 > 紧密中心性 > 程度中心性 > 随机节点选择 > 提议的方法	最小
删除割集后网络分成几个部分	不会发生网络划分	两个部分

4　仿真实验的局限性或风险

区块链中运行的全节点越多,面对灾难性的恢复能力就越强。当区块链的数据分布在如此多的设备中时,恶意实体很难一次擦除所有这些数据。即使由于全球危机导致大量关键节点突然性能下降并且无法访问,理论上单个节点也可以保持整个区块链块的运行。即使所有节点都断开连接,也只需要一个具有完整区块链历史记录的节点重新联机并再次访问所有数据。除了关键性节点以其数量之多可以给网络增添安全性之外,关键性节点会受到其他恶意计算机攻击,这可能会改变它们的功能,例如,剽窃者可能违反我们所讨论软件的安全性,并且在不改变区块链数据的情况下,它可以将所述节点的利润重定向到与其所有者的编程地址不同的地址,窃取地址攻击是此类软件最常见的攻击类型,这就是开发人员建议使用其区块链软件更新版本的原因。但这些安全漏洞中的一些问题很容易解决,可以使用创建安全机制的软件工具将区块链软件与我们的其他计算机系统隔离开来。

5　结　语

本文提出了一种针对区块链场景的节点关键性分析方法,拟议的方法利用了我们先前在频谱划分方面的工作,并为其引入了某些区块链流量指标。基于从所提出的方法获得的节点的关键性,在网络上模拟攻击,从而删除了该节点,比较了各种网络密度和跃点窗口对区块链的影响。然后根据网络中通信受到影响的程度,将该方法与主要使用的现有方法(例如,中间性、紧密性和程度中心性)进行比较,证明了所提出的方法优于现有方法,在识别关键节点方面效果更好。

参　考　文　献

[1] Sardar V P. Currency at a cryptic crossroads: Decrypted [M]. New York: SVP National Police Academy,2018:74.

[2] Ghimire S, Selvaraj H. A survey on bitcoin cryptocurrency and its mining[C]//26th International Conference on Systems Engineering,2018:1 - 6.

[3] Dorri A, Kanhere S, Jurdak R, et al. Blockchain for IoT security and privacy: The case study of a smart home[C]// IEEE International Conference on Pervasive Computing and Communications Workshops,2017:618 - 623.

[4] Khan M A, Salah K. IoT security: Review, blockchain solutions, and open challenges[M]. Future Generation Computer Systems,2018,82:395 - 411.

[5] Mengelkamp E, Notheisen B, Beer C, et al. A blockchain-based smart grid: Towards sustainable local energy markets [J]. Computer Science-Research and Development,2018, 33:207 - 214.

[6] Li C, Jiang W, Zou X. Botnet: Survey and case study [C]//4th International Conference on Innovative Computing, Information and Control,2009:1184 - 1187.

[7] Latora V, Marchiori M. A measure of centrality based on network efficiency[J]. New Journal of Physics,2007,9(6): 188.

[8] Asif W, Lestas M, Qureshi H K, et al. Spectral partitioning for node criticality[C]//IEEE Symposium on Computers and Communication,2015:877 - 882.

[9] Decker C, Wattenhofer R. Information propagation in the bitcoin network[C]//IEEE P2P Proceedings,2013:1 - 10.

[10] Courtois N T, Mercer R. Stealth address and key management techniques in blockchain systems[C]//3rd International Conference on Information Systems Security and Privacy, 2017:559 - 566.

(下转第 383 页)

由于银行间市场交易是动态的,在后续工作中,将探索在交易数据日益增长的情况下,如何实现高效用项集的自动维护与更新,进一步提高方法的实用性。

参 考 文 献

[1] 李政,梁琪,方意. 中国金融部门间系统性风险溢出的监测预警研究——基于下行和上行 ΔCoES 指标的实现与优化[J]. 金融研究,2019(2):40 - 58.

[2] 蔡奕. 解读《证券法》关于市场操纵的法律规范[J]. 证券市场导报,2005(5):19 - 23.

[3] 刘凤元,陈俊芳. 股票价格操纵研究与政策建议[J]. 价格理论与实践,2003(7):52 - 53.

[4] 独道刚. 规划识别在监测股市个股主力资金流向中的应用[D]. 镇江:江苏科技大学,2011.

[5] 王楠. 银行间市场现券交易价格偏离度研究——以中小型商业银行为例[J]. 金融理论与教学,2020(1):56 - 59,62.

[6] Golmohammadi K, Zaiane O, Díaz D. Detecting stock market manipulation using supervised learning algorithms[C]// 2014 International Conference on Data Science and Advanced Analytics,2014:435 - 441.

[7] Martínez-Miranda E, McBurney P, Howard M. Learning unfair trading: A market manipulation analysis from the reinforcement learning perspective[C]//2016 IEEE Conference on Evolving and Adaptive Intelligent Systems,2016:103 - 109.

[8] 廖志良,潘文娣. 我国证券业洗钱风险分析与防范措施[J]. 海南金融,2010(5):55 - 57.

[9] 刘俊. 西藏矿业:对倒交易分析师当"托"[J]. 股市动态分析,2009(3):14,39.

[10] 金升平,刘钊. 银行异常交易检测方法研究[J]. 武汉金融,2018(2):61 - 66.

[11] Han J, Pei J, Yin Y. Mining frequent patterns without candidate generation[C]//2000 ACM SIGMOD International Conference on Management of Data,2000:1 - 12.

[12] Liu M, Qu J. Mining high utility itemsets without candidate generation[C]//21st ACM International Conference on Information and Knowledge Management,2012:55 - 64.

[13] Agrawal R, Imielinski T, Swami A. Database mining: A performance perspective[J]. IEEE Transactions on Knowledge and Data Engineering,1993,5(6):914 - 925.

[14] Zhang F, Zhao X, Li Y, et al. Based on FP-Growth algorithm to excavate medication rule of Chinese materia medica for radiation esophagitis[J]. World Journal of Integrated Traditional and Western Medicine,2020,6(7):31 - 38.

[15] 何望,林果园. 基于 FP-Growth 改进算法的云服务器故障数据分析[J]. 计算机工程与科学,2020,42(5):770 - 775.

[16] Jia Y, Liu L, Chen H, et al. A Chinese unknown word recognition method for micro-blog short text based on improved FP-growth[J]. Pattern Analysis and Applications,2019,23:1011 - 1020.

[17] 黄伟,李国和,吴卫江,等. 基于 FP_Growth 的消费行为关联分析系统设计与实现[J]. 计算机应用与软件,2015,32(8):34 - 37,79.

[18] Van L, Huong P, Thuan L, et al. Improving the feature set in IoT intrusion detection problem based on FP-Growth algorithm[C]//2020 International Conference on Advanced Technologies for Communications,2020:18 - 23.

[19] 刘琰,张进,陈静,等. 基于最大频繁项集挖掘的微博炒作群体发现方法[J]. 计算机工程与应用,2017,53(4):90 - 97.

[20] 吴玉佳,李晶,宋成芳,等. 基于高效用神经网络的文本分类方法[J]. 电子学报,2020,48(2):279 - 284.

[21] 穆晓芳,邓红霞,郭虎升,等. 基于快速高效用项集挖掘的大规模消息流预测算法研究与应用[J]. 计算机应用与软件,2019,36(11):243 - 249.

[22] Liu Y, Liao W, Choudhary A. A two-phase algorithm for fast discovery of high utility itemsets[C]//Pacific-Asia Conference on Knowledge Discovery and Data Mining,2005:689 - 695.

[23] Ahmed C, Tanbeer S, Jeong B, et al. Efficient tree structures for high utility pattern mining in incremental databases[J]. IEEE Transactions on Knowledge and Data Engineering,2009,21(12):1708 - 1721.

[24] Fournier-Viger P, Wu C, Zida S, et al. FHM: Faster high-utility itemset mining using estimated utility co-occurrence pruning[C]//International Symposium on Methodologies for Intelligent Systems,2014:83 - 92.

(上接第 359 页)

[11] Kosba A, Miller A, Shi E, et al. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts[C]//IEEE Symposium on Security and Privacy,2016:839 - 858.

[12] Cachin C, Vukolic M. Blockchain consensus protocols in the wild[EB]. arxiv:1707.01873,2017.

[13] Hazari S, Mahmoud Q H. A parallel proof of work to improve transaction speed and scalability in blockchain systems[C]//9th Annual Computing and Communication Workshop and Conference,2019:916 - 921.

[14] Asif W, Lestas M, Qureshi H K, et al. Spectral partitioning for node criticality[C]//IEEE Symposium on Computers and Communication,2015:877 - 882.

[15] Fiedler M. Algebraic connectivity of graphs[J]. Czechoslovak Mathematical Journal,1973,23(98):298 - 305.