基于信誉评分的共识网络重组机制设计

郑　儿[1]，陈麓竹[1]，赵　静[1]，姚旺君[1]，文　新[2]
（1. 华北计算机系统工程研究所，北京　100083；
2. 中国电子信息产业集团有限公司，广东　深圳　518057）

摘　要：针对共识算法对良性节点占比的依赖，设计了一种基于信誉评分的共识网络重组机制，使得网络能在遭受攻击或发生故障时迅速自我修复和重组，显著提升了抗攻击能力和服务连续性。首先基于信誉机制理论，开发了一个分布式信誉评分系统，实时评估节点信誉，有效处理潜在恶意节点。此外，提出了一种基于信誉评分的共识网络重组机制，通过识别和隔离恶意节点来增强网络的弹性和安全性。该机制设计了网络弹性重组算法，整合了冗余设置、故障诊断和服务节点重新配置功能，确保网络稳定运行和高可靠性。该研究对金融服务、云计算和物联网等广泛使用共识技术的高安全需求领域具有重要应用价值。

关键词：信誉机制；分布式系统；网络重组
中图分类号：TP309　　**文献标识码：**A　　**DOI：**10.19358/j.issn.2097-1788.2024.06.001
引用格式：郑儿，陈麓竹，赵静，等. 基于信誉评分的共识网络重组机制设计[J]. 网络安全与数据治理，2024，43(6)：1-7，15.

Design of a consensus network reorganization mechanism based on credibility score

Zheng Er[1]，Chen Luzhu[1]，Zhao Jing[1]，Yao Wangjun[1]，Wen Xin[2]
（1. National Computer System Engineering Research Institute of China，Beijing 100083，China；
2. China Electronics Corporation，Shenzhen 518057，China）

Abstract：In view of the dependence of the consensus algorithm on the proportion of benign nodes，a consensus network reorganization mechanism based on credit score is designed，so that the network can quickly repair and reorganize when it suffers from attack or failure，which significantly improves the anti-attack ability and service continuity. In this paper，a distributed credit scoring system based on the theory of credit mechanism is developed to evaluate the node reputation in real time and effectively deal with potential malicious nodes. Furthermore，a consensus network reorganization mechanism based on credibility scoring is proposed to enhance the network resilience and security by identifying and isolating malicious nodes. This mechanism designs the network elastic reorganization algorithm，which integrates the redundant setting，fault diagnosis and service node reconfiguration functions to ensure the stable operation of the network and high reliability. This research has important application value in high security needs areas such as financial services，cloud computing and Internet of Things where consensus technologies are widely used.

Key words：credit mechanism；distributed system；network restructuring

0　引言

共识算法被广泛运用于各种最新的应用技术中，如区块链、物联网、云计算等，在不需要中心节点的情况下，为这些技术的实现提供了一种确保整个网络中数据的完整性和一致性的手段，是构建大型分布式系统的重要技术方法。共识算法的核心在于共识网络中的节点参与投票过程，通过统计投票多寡决定节点行为，最终达成一致状态转化。

在共识执行过程中，只要维持良性节点的占比不低于限定阈值，就能够保障系统安全[1]。共识算法的设计中没有考虑针对恶意节点的惩罚机制，而实际的分布式网络环境中，节点随时存在受到攻击转为恶意的可能，原有设计缺乏对网络韧性的考量。

近年来，许多研究工作提出通过信誉机制对共识算法进行改进，通过对节点进行信誉评分，来识别恶意节点并拒绝其参与共识。Lao 等人[2]提出了一种物联网环境中基

于位置的可扩展共识算法，该算法使用节点在同一位置的工作时间来衡量可信度，过滤 Sybil 节点，提升安全性。Tang 等人[3]提出了一种基于信任的实用拜占庭算法，该算法引入信用分数来评估节点可信度，选取一部分信用分数较高的节点参与共识过程，提高了通信开销、共识效率等方面的性能。涂园超等人[4]提出了一种基于信誉投票的 PBFT 改进方案，根据节点划分机制评估节点的可靠性，动态地选取高信誉值节点来参与共识，降低恶意节点成为共识节点的概率，增加系统的安全性。宁宇豪等人[5]提出了一种结合信誉跳跃一致性哈希的区块链分片协议，通过节点在网络中的行为赋予节点不同的信誉等级，降低拜占庭节点在网络中的话语权。李俊吉等人[6]提出一种基于信誉机制的改进 PBFT 共识算法，为每个节点分配不同的角色，包括收集器、普通共识节点和备选节点，并进行评分，评分过低的收集器节点被踢出。不同角色的设置和信誉机制的设计，起到提升算法效率和安全性的作用。

上述研究方案存在一定的安全设计缺陷。在这些方案中，为降低误报率，通常在若干共识轮次后才会依据信誉评分对恶意节点进行处理，恶意节点从表现出异常行为到被清除的过程中，仍然会参与共识，对系统安全造成潜在威胁，存在一定的安全隐患。

为此，本文提出了一种基于信誉评分的共识网络重组机制，通过两阶段网络重组，解决恶意节点隔离不及时的问题，提升共识安全，确保网络稳定运行和高可靠性。本文所提方案基于节点执行共识算法的历史交互行为评估节点信誉，在异常行为首次发生时就进行一阶网络重组，对风险节点进行隔离，随后动态更新信誉分，界定风险节点性质，进行二阶网络重组。本文主要贡献总结如下：

（1）针对共识算法对良性节点占比的依赖，及现有研究工作对风险节点隔离不及时的问题，设计了一种基于信誉评分的共识网络二阶重组机制，使得网络能动态识别遭受的攻击或故障，迅速自我修复和重组，显著提升了抗攻击能力和服务连续性。

（2）设计分布式信誉评分机制，涵盖数据收集与处理，通过加权平均计算直接信任度，采用时间衰减因子更新信任度，并使用 PageRank 算法扩展间接信任度，整合共识网络交互信息，实现恶意节点识别。

（3）设计了网络弹性重组算法，具备冗余设置、故障诊断和服务节点重新配置功能，实现二阶段重组，确保网络稳定运行和高可靠性。

1　相关工作

1.1　信誉机制

信誉机制是一个用于评估和管理实体信誉的技术框架，通过收集、处理和分析节点的历史行为数据来计算信誉评分。这些评分反映了节点的可信度和行为质量，帮助网络系统识别和隔离潜在的恶意节点，有效地减少了信息不对称和欺诈行为的发生。信誉机制在许多领域，特别是在线交易、社交网络、多代理系统和 P2P 网络中，都发挥着关键作用。

信誉机制的运作基于四个核心过程：数据的收集、信誉的计算、信誉评分的更新和信誉的可视化展示。数据收集包括用户反馈、交易历史和行为日志等，为信誉评估提供基础。信誉算法处理这些数据并输出信誉评分。为了保证信誉评分的时效性和准确性，需要定期根据新的数据和交互对其进行动态更新。

信誉算法是信誉机制实现的核心，用于计算和更新实体的信誉评分，基于实体过去的行为和交互来预测其未来行为的可靠性和信任度，涵盖从简单的数学模型到复杂的机器学习方法。

简单平均法计算所有评分的平均值作为信誉评分，实现简单，但不能有效区分新老用户，也不能防止评分刷单等恶意攻击。加权平均法考虑评分的权重，使得信誉高的用户的评分影响更大，较新的评价比旧的评价影响力更高。贝叶斯信誉系统[7]提供统计手段来计算信誉评分，基于概率模型，考虑历史数据中的不确定性和变异性，动态地更新信誉评分，能够处理复杂的信誉评估问题，如考虑不同类型的评价和行为的影响。

群体推理系统[8-9]基于群体智慧，采用类似于协同过滤的技术，分析用户间的相似性来推断用户信誉。群体推理系统特别适用于社交网络和电商场景，用户间的相互作用和相似性可以有效地被利用来评估信誉。

随着数据量的增加，决策树、随机森林、支持向量机或神经网络等机器学习方法[10]在信誉机制中越来越受欢迎，它们从大量的历史数据中学习复杂的模式，更准确地预测用户行为；还可以自动调整其参数以适应行为模式的变化，提高信誉评估的准确性和可靠性。

在信誉系统中，信任度[11]通常被分为直接信任度和间接信任度。直接信任度基于主体与被评估对象之间直接交互的历史来评定信任评分。其优点在于基于第一手的交互经验，更精确和可靠；局限性在于，当缺乏足够的直接交互数据时，评估可能会不够全面。间接信任度通过第三方的评价或网络中其他实体的推荐形成，能够在缺乏直接交互经验的情况下提供信誉评估，使得评估更加全面和多元化。它的挑战在于如何验证这些间接信息的准确性和可靠性，以及如何处理可能的信息失真或偏见。在实际应用中，正确地结合和应用直接信任度和间接信任度，可以显著提高信誉系统的效果和可靠性。

1.2 PageRank 算法

PageRank 算法由谷歌创始人拉里·佩奇和谢尔盖·布林在 1996 年提出[12]，该算法基于网络的超链接结构来进行计算，评估网页的重要性或权威性。网页的 PageRank 值取决于指向它的其他网页的数量和质量。每个网页都会通过其链接传递一部分权重，即 PageRank 值，给它链接的页面。

PageRank 算法的实现包括以下步骤：

（1）初始化：通常给予所有网页一个相同的初始 PageRank 值，如 1.0。

（2）迭代过程：每个网页会将其 PageRank 值平均分配给它指向的网页，然后，每个网页基于收到的来自其他网页的 PageRank 值之和更新其 PageRank 值。

（3）阻尼因子：实际算法中引入了阻尼因子，通常设为 0.85。这是基于一个假设：用户在浏览时，有 85% 的概率通过链接继续浏览下一个页面，有 15% 的概率随机跳到网络中的任意一个页面。这帮助算法模拟真实的用户行为，并确保算法的收敛。

（4）收敛：重复迭代过程，直到所有网页的 PageRank 值变化非常小或达到预设的迭代次数。

PageRank 算法的一个关键特点是它的自我增强性质：高 PageRank 值的网页更可能被新的网页链接，从而进一步增强其 PageRank 值。这种算法在早期的互联网搜索引擎中帮助谷歌快速准确地识别重要的网页并改善搜索结果的相关性。

2 方法

2.1 模型概述

为了解决共识算法缺乏恶意节点惩罚机制，改善现有基于信誉机制的解决方案中对风险节点隔离不及时的问题，本文以共识算法中的投票历史记录为支撑，提出了一种基于恶意节点识别的网络弹性重组方法，通过两阶段网络弹性重组增强共识网络的安全性和弹性，模型整体架构如图 1 所示。

网络弹性重组算法具备三大优势功能：冗余设置、故障诊断以及服务节点重新配置，通过两阶段网络重组保障鉴权服务网络清洁健壮。服务节点的重配分为两个阶段，也称两阶段的网络重组。一阶网络重组发生在单次共识投票后，冗余节点替代风险节点。二阶网络重组会跨越多个投票轮次，直至基于信誉机制判定风险节点性质，进而恢复风险节点信誉或是将其隔离。冗余设置主要体现为为共识网络设置一定的备份，以便在重组过程中实现对风险节点的功能替代。故障诊断在一阶重组过程中体现为依据单次共识投票对风险节点进行识别；在二阶重组过程中主要体现为依赖信誉机制实现风险节点的性质界定。

为实现二阶重组过程中的风险节点性质界定，基于信誉机制理论，构建一个分布式信誉评分系统，该系统可以实时评估网络中各节点的信誉，进而有效甄别分布式集群环境中潜在的恶意节点，实现故障诊断功能，为弹性重组算法赋能。

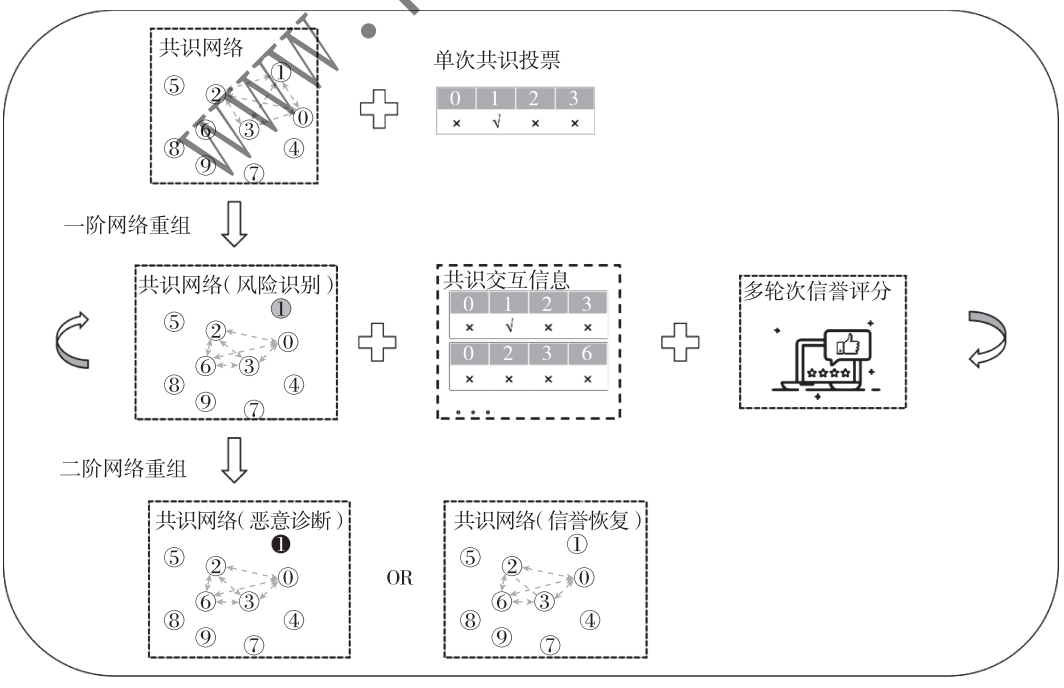

图 1 基于恶意节点识别的网络弹性重组方法模型架构

2.2 弹性重组

为保证充足的良性节点参与共识，设计网络重组算法实现对恶意或故障节点的清洗和替换，以确保共识算法可靠运行。

实现重组算法的前提是设置一定数量的冗余节点作为备份，以便及时补充失效节点被清洗后的空缺，保证参与共识投票的法定人数（quorum）完备可靠。为实现冗余设置，将分布式系统中具有参与共识能力的节点标记为四类；被信任并参与共识的活跃节点，共识投票过程意见占少数的风险节点，由信誉机制识别出的恶意节点，以及充当冗余功能的备份节点。

重组算法需要实现对故障或恶意节点的诊断，该功能依赖于信誉评分机制的结果。在一轮表决过程中，投票占优的活跃节点会将持有相反意见的节点诊断为受到恶意攻击或存在故障的风险节点。在动态更新的信誉评分作用下，风险节点会随时间推移被判定为恶意节点，或是逐渐恢复信誉，转为备份节点。

包括服务节点重配的节点管理功能本质上就是针对四类节点创建并维护四个队列，即活跃节点队列、风险节点队列、恶意节点队列及备份节点队列。

活跃节点队列中存放着参与共识的节点信息，共识算法描述的执行流程就是对这些活跃节点之间交互通信的描述，因此也可以将活跃节点队列中的节点集称为仲裁组。在通信过程中通过读取该队列信息，可以限制广播消息收发的范围，确保只有被信任的活跃节点能够参与共识投票。在 quorum = 4 的情况下，活跃节点队列长度也为 4。活跃节点队列的初始化发生在网络拓扑创建时，各节点向全局广播地址信息，响应速度占先的 4 个节点成为活跃节点，参与后续的共识。

备份节点队列存放着暂且被信任但并未参与共识的节点信息。备份节点队列的初始化同样发生在网络拓扑创建时，未抢占成为活跃节点的其他节点自动划归备份节点队列。

风险节点队列存放着投票总数占劣势的节点信息。该队列初始默认为空，允许风险节点队列中的节点继续表达共识意见，但该意见不被仲裁组参考，仅作为信誉评分的依据。通过设置风险队列，同时削减了漏判的风险和误判的影响。一方面，及时隔离风险节点可以避免恶意节点在后续的共识轮次中输出错误意见；另一方面，风险节点队列为恶意节点识别提供缓冲时间，通过若干轮次的信誉评分更新，避免“误伤好人”。

恶意节点队列可以被认为是一种黑名单机制，通过信誉机制从风险节点中筛选出的恶意节点被归入此队列，从此不被任何其他节点信任，等待管理维护人员进一步处理。

共识算法执行到 REPLY 阶段，各节点在向客户端回复最终投票结果的同时，触发对故障节点的识别和处理操作，网络重组开始。投票占优的节点将持有相反意见的节点诊断为风险节点，移出活跃节点列表，并从备份节点列表中顺次挑选一个新的节点替补加入，如图 2 所示。

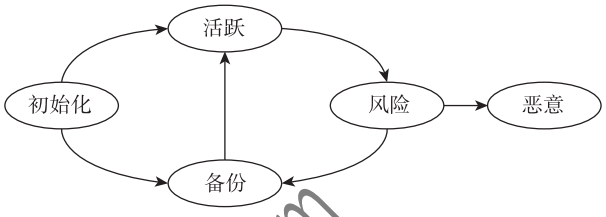

图 2　节点网络重组过程的自动状态机表示

2.3 信誉机制

信誉机制的核心理念在于通过信誉评分反映节点的可信度和行为质量，从而帮助网络系统识别和隔离潜在的恶意节点。设计合理的信誉评分方案是实现信誉机制的关键。

2.3.1 评分方案概述

本文提出的分布式信誉评分方案总体架构如图 3 所示，共分为以下几个部分：

（1）数据收集与处理：持续监控网络中节点间的投票互动行为和节点状态转化信息，将这些数据转化为选定的评价指标，以便于进一步的处理和分析。

（2）直接信任度：基于选定的评价指标，定义一个直接信任度的综合评分方案，通过加权平均的方式评价直接信任度。

（3）时间衰减因子：更新直接信任度时，引入滑动窗口和时间衰减因子以确保评分体现最近的信任信息，减少历史数据的直接影响。

（4）间接信任度：利用 PageRank 算法，扩展了信任度的影响，使之能够通过网络的连通路径传播，从而计算出基于整个网络结构的综合信任度。

2.3.2 评价指标选择

本文基于先验知识，将投票一致性、状态转换次数、活跃度作为衡量信任度的基本评价指标，用于动态更新直接信任度。

（1）投票一致性

投票一致性是指测量节点的投票行为是否与大多数节点的群体决策一致，是直接信任度的一个重要指标，因为它反映了节点在共识算法共识决策中与其他节点的一致程度。节点的投票一致性越高，可信度就越高。投票一致性计算方法如下：

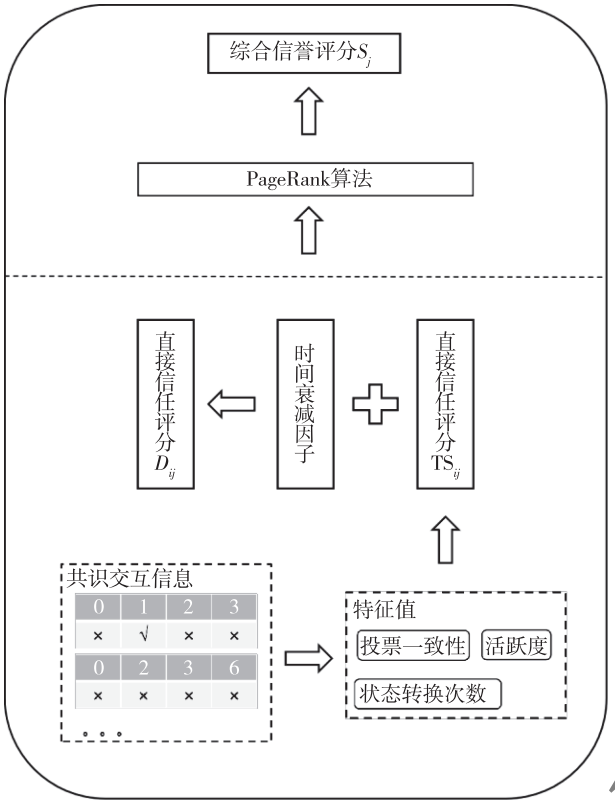

图 3　信誉评分方案架构

$$C_{ij}=\frac{A_{ij}}{R_{ij}} \tag{1}$$

其中，C_{ij}代表在节点 i 的视角下节点 j 的投票一致性，R_{ij} 代表在节点 i 的视角下节点 j 参与的共识次数，A_{ij}代表在 i 与 j 共同参与的多次投票中节点 j 投出的选票与最终裁决一致的次数。

（2）状态转换次数

状态转换次数是指测量节点的状态从活跃转移到风险的次数，频繁的状态转换反映了节点行为不稳定的特性，暗示节点可能存在潜在的恶意行为。节点的状态转换次数越多，可信度就越低。状态转换次数是一个计数值，可以在后续将其归一化后与其他评价指标结合使用。用 ST_{ij}代表在节点 i 的视角下节点 j 发生的状态转换次数。

（3）活跃度

活跃度是指测量节点对投票行为的参与程度，反映了节点在共识决策过程中的贡献度。节点的活跃度越高，代表节点积极参与投票行为越积极，暗示了较高的可信度。活跃度计算方法如下：

$$\mathrm{AL}_{ij}=\frac{\mathrm{R}_{ij}}{\mathrm{TR}_i} \tag{2}$$

其中，AL_{ij}代表在节点 i 的视角下节点 j 的活跃度，TR_i 代表在节点 i 的视角下共识发生的总轮次，R_{ij}代表在节点 i 的视角下节点 j 参与的共识次数。

2.3.3　直接信任度

（1）评分方案

信誉评分的输入数据源于共识算法的交互式投票过程，因此理论上节点的信誉评分是一个从无到有并逐渐趋于收敛的过程。因此，需要设计一个符合评分变化机理的动态信誉评分更新机制。本文构建了一个信誉评分模型，通过投票一致性、状态转换次数、活跃度综合衡量节点的行为表现，对节点的直接信任度进行量化评估。直接信任度综合评分公式如下：

$$\mathrm{TS}_{ij}=w_{\mathrm{C}}\times C_{ij}+w_{\mathrm{ST}}\times\frac{1}{1+\mathrm{ST}_{ij}}+w_{\mathrm{AL}}\times\mathrm{AL}_{ij} \tag{3}$$

其中，TS_{ij}代表在节点 i 的视角下节点 j 的直接信任度，w_{C}、w_{ST}、w_{AL}分别表示投票一致性、状态转换次数、活跃度的相对权重。

为体现中立态度，初始时所有节点默认其他节点有一半概率为恶意，因此设置直接信任度的初始值为 0.5。

（2）时间衰减

在动态更新直接信任度时，考虑到恶意节点识别中，最新的交互信息对近期恶意节点识别可能更具备借鉴意义，同时，为了优化资源使用和保护隐私，节点不应存储庞杂的历史数据日志，因此引入滑动窗口结合时间衰减因子以确保评分体现最近的信任信息，减少历史数据的直接影响。定义考虑了时间衰减因素的直接信任度评分公式如下：

$$D_{ij}^{\mathrm{new}}=\alpha\times\left(w_{\mathrm{C}}\times C_{ijn}+w_{\mathrm{ST}}\times\frac{1}{1+\mathrm{ST}_{ijn}}+w_{\mathrm{AL}}\times\mathrm{AL}_{ijn}\right)C_{ij}+(1-\alpha)\times D_{ij}^{\mathrm{old}} \tag{4}$$

其中，D_{ij}代表考虑了时间衰减因素后的直接信任度，右上角标注的 old 和 new 分别代表更新前以及更新后；n 代表滑动窗口大小，表示节点 i 在计算节点 j 直接信任度的评价指标时仅统计近 n 轮共识算法共识的历史交互数据；α 为时间衰减因子。通过限定滑动窗口和时间衰减因子，在不完全抛弃陈旧数据的同时，逐渐削弱旧的共识交互信息对现有信任度的影响。

2.3.4　间接信任度

共识网络模型是一种基于 P2P 的网络架构方案，在设计信誉机制时，需考虑到网络的去中心化特性和节点间直接交互的动态性。在计算信誉分时，基于节点间直接交互的评估可以得出直接信任度，基于网络中其他节点的评估可以得出间接信任度，系统需要综合考虑直接信任度和间接信任度，从而得到更为全面的评分依据。通过分布式信誉评分机制的设计，共识网络的每个节点都具有对其他节点进行直接信任度评估的能力。为了使

对信任的评估更为全面，需要综合考虑其他非直接交互节点对待观测节点的信任度。PageRank 算法能够根据网页之间的链接关系通过迭代计算来评价网页的重要性，为将间接信任度引入信誉评分机制提供了解决方案。

类比 PageRank，分布式信誉评分系统中的每个节点都可以视为网络中的一个网页，节点间的信任关系类似于网页之间的链接，可以基于共识网络构建起一个信任网络，在每次迭代中，节点的信誉分数会根据其收到的信任“链接”的数量和质量进行更新，最终趋向稳定收敛。

综合使用 PageRank 算法，在分布式信誉评分系统中可以有效地评估和管理节点信誉，使每个节点在进行信誉评分时不仅考虑直接的交互信任，而且将通过网络中其他节点传递的间接信任纳入考虑。利用 PageRank 进行全面动态评分的步骤如下：

（1）信任矩阵构建

首先，需要定义信任矩阵 $\boldsymbol{T}$，经过直接信任度的计算，节点 i 对节点 j 的直接信任度 D_{ij} 已知，则通过令 $T_{ij} = D_{ij}$，为矩阵 $\boldsymbol{T}$ 赋值，矩阵 $\boldsymbol{T}$ 反映了各个节点的直接信任度。

（2）归一化信任矩阵

为了方便后续 PageRank 的迭代计算，对信任矩阵 $\boldsymbol{T}$ 进行归一化，形成转移概率矩阵 $\boldsymbol{P}$。归一化的实现方式为对每一个 P_{ij} 进行如下计算和填充：

$$P_{ij} = \frac{T_{ij}}{\sum_{k=1}^{N} T_{ik}} \tag{5}$$

其中 P_{ij} 表示随机游走模型中，从节点 i 到节点 j 的概率。$\sum_{k=1}^{N} T_{ik}$ 表示节点 i 对每个节点的信任度总和。通过这种方式，可以确保每一行转移概率总和为 1。

（3）PageRank 计算

通过信任矩阵的构建和归一化，信任网络建立完成，在此基础上可应用 PageRank 公式进行信任度计算：

$$\mathrm{PR}(j) = \frac{1-d}{N} + d\sum_{i \in M(j)} P_{ij} \times \mathrm{PR}(i) \tag{6}$$

其中，PR（j）是节点 j 的 PageRank 值，是指向节点 j 的信任节点集合，d 是用来模拟随机信任跳转的阻尼因子，常用取值为 0.85。在迭代开始前，为所有节点的 PageRank 赋初值为 $1/N$。此后，对每个节点应用上述 PageRank 公式进行计算，计算将重复迭代多轮，直到趋于稳定收敛。最终趋近收敛的即为结合了直接与间接信任度的综合信誉分，记 $S_j = \mathrm{PR}(j)$。

值得注意的是，在代入 PageRank 公式前，首先会基于直接信任度 D_{ij} 形成概率转移矩阵 $\boldsymbol{T}$，随后 $\boldsymbol{T}$ 归一化生成概率转移矩阵 $\boldsymbol{P}$ 用于 PageRank 计算。在对 $\boldsymbol{T}$ 的赋值过程中，实际上已经综合考虑了直接信任度和通过网络路径推导的间接信任度。因此，通过 PageRank 计算得到的趋于稳定的 S_j 可以被视为节点 j 的综合信誉分，其中包括了直接和间接的信任信息。

在（0，1）区间选定一个合理阈值，一旦 S_j 低于该阈值则认为是恶意节点，被归入恶意节点队列，并全局通告。例如，可假定（0，0.1］为恶意节点区间，而［0.9，1）为足够可信节点区间。

3　实验

实验环境配置为 Intel（R）Core（TM）i7 - 9750H，4 核处理器，16 GB 内存，256 GB 硬盘，Linux5. 8. 0 - 48 - generic #54 ~ 20. 04. 1 - Ubuntu 操作系统。初始设定共识网络由四个节点组成，设置一个冗余节点。

3.1　安全性分析

本文通过信誉机制的引入，为共识算法提供界定恶意节点的方法，再通过二阶网络重组实现恶意节点的清除，解决了传统共识算法中缺乏惩罚机制的问题。

在网络构成为初始设定的情况下，设计实验对网络重组过程进行仿真模拟，假设恶意节点以 100% 的概率发布共识意见。当取 $w_{\mathrm{C}} = 0.9$，$w_{\mathrm{ST}} = 0.05$，$w_{\mathrm{AL}} = 0.05$ 时，D_{ik} 会逐渐趋稳于 0.1，P_{ik} 会逐渐趋稳于 0.2，S_k 亦趋稳于 0.1，将这一评分对照阈值设定进行比较，可认定节点 k 为恶意节点，从而被列入“黑名单”。

在实际应用中，可设计监控系统，对被识别出的恶意节点输出工单通告，由运维管理人员择机对其进行进一步处理。这一流程确保系统对恶意节点具有足够的自洁能力，即在可预期的有限时间内能够完成恶意节点的清洗、替换与处理。

3.2　时间开销分析

二阶段网络弹性重组设计会带来时间开销的增长，因此需要设计实验分析其时间开销情况，论证方案的实用性。在网络重组过程中，有三个重要的时间节点：风险节点检出、仲裁组重构完成以及风险节点恢复信誉或被界定为恶意节点列入“失信黑名单”。网络重组的效率主要与两个时间差相关。

设置实验测试重组算法的时间开销是否在可接受的范围内。具体测试方法为在程序执行过程中设置时间记录功能，分别记录存在恶意或受损节点的情况下，共识网络环境检出风险节点的时间点、仲裁组重构的时间点以及风险节点性质界定完成的时间点，计算两个时间差。

随机选取不多于 f 个节点作为恶意或受损节点执行

持续鉴权操作。记录所有节点的观测结果及时间开销情况，结果如表 1 ~ 表 3 所示。实验表明在总节点数为 4，恶意或受损节点数为 1 的测试环境下仲裁组重构完成的时间为 196 ms，远小于一轮共识投票所需时间。在仲裁组重建 6.5 s 后，风险节点界定完成，网络恢复清洁。该网络重组时间是可接受的，说明系统具有较好的鲁棒性。

表 1　$N=4$，$f=1$ 节点交互信息

节点编号	0	1	2	3
投票信息	False	False	False	True

表 2　$N=4$，$f=1$ 重组时间记录

事件	故障检出	一阶重组完成	二阶重组完成
时间	1685108567659	1685108567855	1685108574322

表 3　$N=4$，$f=1$ 重组时间差记录

时间差	时间差一	时间差二
时间/ms	196	6 467

网络一阶重组的主要操作是各节点对于自身维护的多个节点队列进行更新，与鉴权并发进行，这使得参与共识的节点规模与一阶重组耗时关联性不大。在不同规模的共识网络下记录网络重组所花费的时间，实验证明推测正确。图 4 展示了不同节点规模下一阶网络重组耗时，可以发现节点规模对重组时间开销无显著影响，一阶重组时间均稳定于 1 000 ms 内。

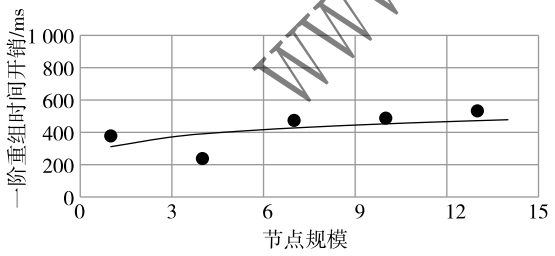

图 4　不同节点规模下一阶网络重组时间开销

网络二阶重组的主要操作是随共识投票持续发生，逐渐更新风险节点信誉评分，直至到达阈值，这使得二阶重组耗时与共识时间开销关联紧密，即与仲裁组的节点规模强相关。在不同规模的共识网络下记录网络重组所花费的时间，实验证明推测正确。图 5 展示了不同节点规模下二阶网络重组耗时，可以发现二阶重组时间开销随节点规模增长缓慢增长，与共识时间开销增长同频，在节点规模较小的情况下维持在秒级。且在实际工作中，通常采用分层、分片乃至委托共识的方式限制单个共识组的规模，以提高共识系统性能，故本方案具备一定的可行性。

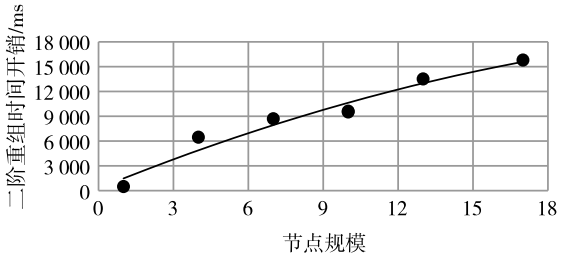

图 5　不同节点规模下二阶网络重组时间开销

4　结论

本文基于信誉机制理论，设计了一个分布式信誉评分系统，综合衡量节点直接信任度和间接信任度评估节点信誉，有效界定恶意节点；在此基础上，通过二阶段网络重组机制，及时隔离恶意节点，增强网络的弹性。经实验分析，所提模型能够有效识别共识网络中的恶意节点，缓解共识算法良性节点占比依赖，及缺乏惩罚机制的问题。同已有研究工作相比，模型能够有效降低漏报带来的不利影响；同时，由于重组机制独立于共识过程，能够削减引入信誉机制为共识带来的时间开销增长；网络重组的时间开销在节点规模较小的情况下与共识开销增长同频且增长缓慢，在实际应用场景下维持在秒级，本方案具备一定的现实意义和可行性。

参考文献

[1] 靳世雄，张潇丹，葛敬国，等. 区块链共识算法研究综述 [J]. 信息安全学报，2021，6 (2)：85 - 100.

[2] LAO L，DAI X H，XIAO B，et al. G - PBFT：a location-based and scalable consensus protocol for IOT-Blockchain applications [C]// Proc. of IEEE International Parallel and Distributed Processing Symposium. IEEE Press，2020：664 - 673.

[3] TANG S，WANG Z Q，JIANG J，et al. Improved PBFT algorithm for high-frequency trading scenarios of alliance blockchain [J]. Scientific Reports，2022，12 (1)：4426.

[4] 涂园超，陈玉玲，李涛，等. 基于信誉投票的 PBFT 改进方案 [J]. 应用科学学报，2021，39 (1)：79 - 89.

[5] 宁宇豪，黄建华 ，顾彬，等. 结合信誉跳跃一致性哈希的区块链分片协议 [J/OL]. 计算机工程与应用：1 - 14 [2024 - 04 - 22]. http：//kns. cnki. net/kcms/detail/11. 2127. TP. 20230920. 1031. 018. html.

[6] 李俊吉，张佳琦. 基于信誉机制的改进 PBFT 共识算法 [J/OL]. 计算机应用研究：1 - 9 [2024 - 04 - 22]. https：//doi. org/10. 19734/j. issn. 1001 - 3695. 2023. 11. 0517.

（下转第 15 页）

经网络的物联网流量异常检测［J］. 信息网络安全，2019（12）：53－63.

［14］ZOU B L，WEI Y，MA L，et al. Feature-attended multi-flow LSTM for anomaly detection in Internet of Things［C］//IEEE INFOCOM 2022－IEEE Conference on Computer Communications Workshops，New York，USA，2022：1－6.

［15］BLONDEL V D，GUILLAUME J L，LAMBIOTTE R，et al. Fast unfolding of communities in large networks［J］. Journal of Statistical Mechanics：Theory and Experiment，2008：P10008.

（收稿日期：2024－04－17）

作者简介：

靳文京（1991－），男，本科，工程师，主要研究方向：网络安全、信息通信。

周成胜（1982－），男，硕士，高级工程师，主要研究方向：网络安全、工业互联网安全、车联网安全、物联网安全。

刘美伶（1991－），通信作者，女，硕士，主要研究方向：网络安全、数据安全。

（上接第7页）

［7］侯辉广. 无线 Mesh 网络中信誉模型研究［D］. 哈尔滨：哈尔滨工业大学，2015.

［8］LATHIA N，HAILES S，CAPRA L. Trust-based collaborative filtering［C］// IFIP International Conference on Trust Management. Springer，2008：119－134.

［9］WANG X S，SU L，ZHOU Q H，et al. Group recommender systems based on members′ preferencefor trusted social networks［J］. Security and Communication Networks，2020，2020：1－11.

［10］黄艳蓉. 基于机器学习的众包参与者信誉评估研究［D］. 武汉：武汉大学，2020.

［11］陈海彪，黄声勇，蔡洁锐. 一个基于智能电网的跨层路由的信任评估协议［J］. 计算机科学，2021，48（S1）：491－497，503.

［12］李稚楹，杨武，谢治军. PageRank 算法研究综述［J］. 计算机科学，2011，38（S1）：185－188.

（收稿日期：2024－04－29）

作者简介：

郑儿（1984－），女，硕士，高级工程师，主要研究方向：网络安全。

陈麓竹（1997－），女，硕士研究生，主要研究方向：网络安全。

赵静（1983－），女，博士，主要研究方向：网络安全。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部