面向工业物联网的区块链高效拜占庭容错共识算法

李凤岐[1,2]，宋晴晴[1]，徐辉[1]，杜学峰[3]，高嘉隆[4]，佟宁[1,2]，王德广[1,2]
（1.大连交通大学软件学院，辽宁 大连 116028；2.大连市区块链技术与应用重点实验室，辽宁 大连 116028；
3.大连交通大学机械工程学院，辽宁 大连 116028；4.大连交通大学计算机与通信工程学院，辽宁 大连 116028）

摘　要：鉴于工业物联网多样性终端存在作恶风险，为满足共识过程中对高效率和安全可容错的需求，提出了基于信誉积分与双层动态的实用拜占庭容错（CD-PBFT）高效共识算法。信誉积分模型确保良好节点参与共识，移除故障节点；双层架构实现交易验证和读写操作的并行；自适应主节点算法随机选取信誉值高节点作为主节点并确保其安全性。实验结果表明，CD-PBFT在保持安全性与活性的基础上，相较于PBFT，网络交易时延平均降低34.8%，吞吐量平均提高25.2%，实现了对效率与安全容错性的双重要求。

关键词：工业物联网；信誉积分模型；双层动态；实用拜占庭容错；共识算法
中图分类号：TP393
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2024090

Blockchain efficient Byzantine fault tolerance consensus algorithm for IIoT

LI Fengqi[1,2], SONG Qingqing[1], XU Hui[1], DU Xuefeng[3], GAO Jialong[4],
TONG Ning[1,2], WANG Deguang[1,2]
1. School of Software, Dalian Jiaotong University, Dalian 116028, China
2. Key Laboratory of Blockchain Technology and Application in Dalian City, Dalian 116028, China
3. School of Mechanical Engineering, Dalian Jiaotong University, Dalian 116028, China
4. School of Computer and Communication Engineering, Dalian Jiaotong University, Dalian 116028, China

Abstract: Considering the malicious risks associated with diverse terminals in the industrial Internet of things (IIoT), a practical Byzantine fault tolerant (PBFT) efficient consensus algorithm based on credit score and dynamic double layer (CD-PBFT) was proposed to meet the requirements of high efficiency and security fault tolerance in the consensus process. The participation of good nodes in the consensus and the removal of faulty nodes were ensured by the credit score model. The parallelism of transaction verification and read write operations was achieved through the implementation of a double layer architecture. Nodes with high credit were randomly selected as the master node by the adaptive master node algorithm, ensuring its security. Experimental results show that CD-PBFT not only can maintain the safety and liveness of the consensus algorithm but also can reduce network delay by 34.8% and increase throughput by 25.2% compared with PBFT, which meets the double requirements of efficiency and security fault tolerance.

Keywords: IIoT, credit score model, dynamic double layer, PBFT, consensus algorithm

收稿日期：2023–09–05；**修回日期：**2024–02–01
通信作者：王德广，wdg@djtu.edu.cn
基金项目：辽宁省国际科技合作计划基金资助项目（No.2022JH2/10700012）；辽宁省应用基础研究计划基金资助项目（No.2022JH2/101300269, No.2023JH2/101300188）
Foundation Items: The International Science and Technology Cooperation Program Project of Liaoning Province (No.2022JH2/10700012), The Applied Basic Research Program Project of Liaoning Province (No.2022JH2/101300269, No.2023JH2/101300188)

0 引言

在第十四个五年规划和2035年远景目标纲要中，工业物联网（IIoT, industrial Internet of things）和区块链被明确提出，这2种新型基础设施和数字经济重点产业将推动关键技术创新和融合应用。区块链技术作为一种去中心化、分布式的信任机制，为实现点对点可靠的价值传递提供了解决方案[1-2]。然而，IIoT的数据高价值性、中心化网络架构以及终端协议的不互通性等特征对其上链过程中的安全性、数据的隐私提出了挑战。近年来，区块链技术为IIoT的安全提供了新的解决方案[3-5]，这也成为目前研究的热点问题。

在IIoT终端数据上链过程中，共识算法确保了系统的有序运行和公平性[6-7]。但由于终端设备的异构性、资源受限和中心化网络平台的不兼容性，可能会发生作恶行为，增加了数据泄露或篡改的风险，从而造成经济损失。因此，如何确保物联网（IoT, Internet of things）终端数据的安全一致性至关重要。Raft共识算法在终端作恶情况下难以确保正确数据安全上链[8]，而拜占庭容错（BFT, Byzantine fault tolerance）共识算法则可能降低数据上链效率，但其在解决恶意节点问题上具备独特优势。这使得在数据上链共识过程中，高效率和安全可容错之间存在难以协调的问题。在IIoT终端数据上链过程中，物联网终端设备作为区块链全节点负责数据打包和上链共享。为了确保在出现恶意终端时全网终端数据仍能安全上链，需要解决上链共识过程中的安全性和效率之间的平衡问题。

为解决这一问题，本文提出了一种基于信誉积分和双层动态的实用拜占庭容错（CD-PBFT, credit score and dynamic double layer practical Byzantine fault tolerance）高效共识算法，主要包括以下3个方面的创新工作。

1) 创新性地设计信誉积分模型以更新CD-PBFT高效共识算法中节点的信誉积分值。该模型在每轮共识后计算节点的信誉积分值，为确保良好状态的节点持续参与共识过程，剔除或重置出现拜占庭故障和频繁宕机的节点，降低恶意节点出现的频率，提高共识效率。

2) 提出双层架构拜占庭容错共识算法，将节点分为上下两层。下层节点负责验证客户端交易数据的合法性，上层节点负责生成区块并达成共识。共识后，将区块同步至下层节点进行存储。该并行处理方法有效缩短了验证时间，提升了算法性能。

3) 设计自适应主节点选择算法以提高共识效率。在CD-PBFT中，采用随机化方法选取信誉积分值高的节点作为主节点，优化视图转换的主节点选择方式。这提高了高信誉积分值节点成为主节点的概率，降低了视图转换风险，减少了资源消耗和作恶节点成为主节点时区块链的安全风险。

1 相关工作

近年来，为满足大量异构、资源有限的IIoT设备参与共识的需求，研究人员对区块链的共识算法进行了优化，以期提高其安全容错性和共识效率。

在安全容错性方面，Jiang等[9]和Douceur[10]针对传统实用拜占庭容错（PBFT, practical Byzantine fault tolerance）共识算法易受女巫攻击的问题，提出了一个防御sybil攻击的无线网络共识算法。同时，赖英旭等[11]通过建立信誉模型，基于信任值赋予节点权力，并在PBFT算法基础上加入预提交阶段以减少通信次数，提升算法性能并有效防御女巫攻击。Lao等[12]提出了利用地理信息固定IoT设备达成共识的共识算法，避免sybil节点攻击。Makhdoom等[13]提出了一个独特的基于诚实证明的共识算法，以减少区块链共识期间恶意行为发生的可能性。除此之外，Yang等[14]提出了一种高容错一致性算法，该算法使用一致的散列算法对一致性节点进行分组，并提出了节点决策广播模型和门限计票模型，使容错上限大于$\frac{1}{3}$，但提出的算法主要针对单层一致性网络，其可扩展性有待进一步提高。然而，尽管上述研究成果在安全容错性方面有所突破，但拜占庭容错共识算法可能导致效率下降。

在共识效率方面，Dorri等[15]提出了快速可扩展的共识算法树链，以解决低效的验证器选择问题，但该方法很难进行大量数据的共识。Xu等[16]提出了一种针对能量受限的IoT+区块链应用的PBFT高效共识协议。Thakker等[17]通过改进PBFT算法，提出了一种新的共识协议，采用随机哈希生成特性，并将哈希值匹配到一个预定义的阈值以减少拒绝服务（DoS, denial of service）攻击，提供高吞吐量从而在受到攻击时达到最终的共识，但是节

点出现异常时并不能保障共识算法顺利完成。Zhou 等[18]提出一种改进的拜占庭容错算法，在一致性效率和吞吐量等方面均优于其他 BFT 算法。Zhang 等[19]提出一种可以应用在车联网中并基于 IoT 的 lattice 有向无环图（DAG, directed acyclic graph）结构的并行共识算法，以解决因共识节点过多和节点移动性导致的PBFT算法共识效率低下的问题，该算法在区块链添加、时延、吞吐量、一致性成功率和获得交易的时间等方面均优于其他同类方案，但未能将安全容错性充分考虑在内。刘峰等[20]提出以 Pedersen 承诺和 Schnorr 协议为基础的安全多方计算协议，在保障区块链数据安全性基础上节省时间成本进而提升了区块链的交互效率，但同样未能将安全容错性考虑在内。

可见，这些方法都未能完美兼顾安全容错性和效率。本文提出的CD-PBFT共识算法在兼顾共识效率和安全容错性方面有所创新。

2　PBFT 共识算法简介

1999 年，Castro 等[21]提出 PBFT 共识算法，该算法解决了早期 BFT 算法[22]效率不高的问题。PBFT 共识算法的网络结构中最多允许存在 f 个拜占庭节点，并且对于系统要求，需满足 $f < \frac{n-1}{3}$，PBFT 共识算法将时间复杂度从 $O(n^{f+1})$ 降低至 $O(n^2)$，这一优化使得在实际系统应用中基于 BFT 算法的解决方案变得更为可行。PBFT 是一种以状态机副本复制为基础的分布式一致性算法，由一致性协议、视图转换协议以及检查点协议构成[23]。PBFT 算法的一致性协议和视图转换协议在下文进行详细介绍；检查点协议是定时触发的一种在分布式系统中进行垃圾回收的机制，可以清理本地消息日志文件中的旧消息，防止系统的存储资源过多而造成损失。

2.1　一致性协议

一致性协议确保整个网络中各节点所保存数据的一致性，其运作机制依赖于分布式节点之间的三阶段相互通信。一致性协议作为 PBFT 算法实现共识的核心协议，是构成完整共识过程的关键。该完整共识过程包括 5 个阶段，分别为请求、预准备、准备、提交以及回复。

以四节点网络为例详细描述 PBFT 共识过程，在系统中，1 个节点被指定为主节点，其他 3 个则为从节点，系统中坏节点的数量为 f。图 1 展示了从节点 3 发生故障的共识过程。PBFT 共识算法要求网络中的节点总数为 n，且应满足 $n \geqslant 3f$。若取 $n = 4$，则可得出 $f \leqslant 1$，即该算法在节点总数为 4，主节点为良性节点时能够容忍 1 个节点发生故障，仍能够保障网络的正常、合规运行。

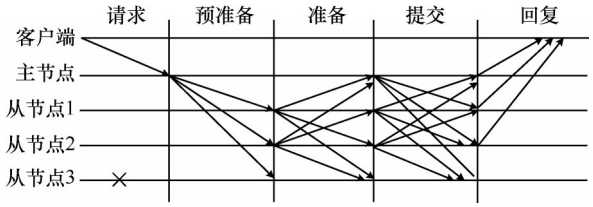


图 1　从节点 3 发生故障的共识过程

2.2　视图转换协议

在考虑节点总数 $n = 4$ 的情况下，PBFT 视图转换过程如图 2 所示。每个节点从被选为主节点开始，直至由于故障而被其他节点代替，这个完整的周期被称作一个视图。在一致性协议的执行过程中，当主节点发生故障（无响应或出现错误）时，将会启动视图转换协议，以完成主节点的替换过程。视图转换也是一个三阶段协议，其中包含视图转换、视图转换信息广播和新视图阶段。当视图 v 中主节点出现错误时，视图将会更新至 $v + 1$，同时切换到下一个主节点。

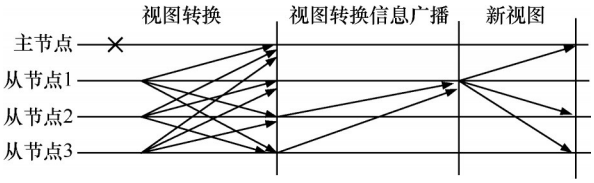


图 2　PBFT 视图转换过程

在视图 $v + 1$ 下，主节点的计算式为

$$\text{Primary} = (v + 1) \bmod n \tag{1}$$

其中，n 表示节点总数，Primary 表示主节点的 ID。

3　模型

3.1　网络模型

在大规模 IIoT 的场景下，数据感知层中 IIoT 设备产生的大量数据被传输到相应的边缘服务器节点。不同的边缘服务器节点分别控制和管理相应的 IIoT 域。IIoT 域的数据通过使用边缘服务器作为区块链的节点在共识层中共享数据。随着高价值的 IIoT 大量数据不断提交和记录在区块链上，有必要

实施一种能够平衡效率和拜占庭容错要求的区块链共识机制。

大规模IIoT数据共享场景如图3所示。在IIoT终端数据上链共享的过程中，数据将作为区块链网络中的全节点，通过打包的方式上链进行数据共享。数据共享的过程既确保数据的可追溯性和不可篡改性，也为各参与方提供透明度和信任度。为了保障数据共享的一致性和准确性，需要对这些大规模IIoT数据进行深度分析，进而实现对数据含义和价值的理解，避免在上链过程中数据出现错误或不一致的情况。应用层实现对客户端的服务请求进行验证，以确保其合法性和符合性。

3.2　系统模型

CD-PBFT共识算法模型如图4所示。采用多进程模拟边缘服务器节点，信誉积分值较低的服务器节点被放置在下层，下层节点对交易数据的合法性进行验证。一般情况下，系统中有n个节点和f个恶意节点，并且满足$\frac{n}{2} \geqslant 3f+1$。下层节点的总数为$\frac{n}{2}$，其中包含$f$个恶意节点。系统上层有$\frac{n}{2}$个节点，下层有$\frac{n}{2}$个节点，上下层节点总数可以实现动态平衡。通过实现CD-PBFT共识算法，系统可以容忍拜占庭故障。因此在IIoT场景中，根据网络和终端状态需要，CD-PBFT共识算法可实现效率和容错性之间的平衡。

4　CD-PBFT共识算法

4.1　算法思路

4.1.1　信誉积分模型

本文首先建立信誉积分模型，用于更新CD-PBFT共识算法中各节点的信誉积分值。信誉积分模型主要根据上层节点和下层节点分别设计，其中，下层节点的信誉积分评估指标是基于下层节点验证转发的写操作的准确性进行更新，上层节点的信誉积分评估指标是基于参与共识的节点行为进行更新。

下层节点i的信誉积分值计算式为

$$\mathrm{LT}_{\mathrm{cons}}(i,t)=\begin{cases}\min\left(1,(1+y_L)\mathrm{LT}_{\mathrm{cons}}(i,t-1)\right), & \text{良性状态}\\ \max\left(x_L\mathrm{LT}_{\mathrm{cons}}(i,t-1),0\right), & \text{宕机状态}\\ -1, & \text{作恶状态}\end{cases} \tag{2}$$

其中，x_L代表下层节点信誉积分值下降的幅度值，y_L代表下层节点信誉积分值上升的幅度值，可根据实际需求设置。

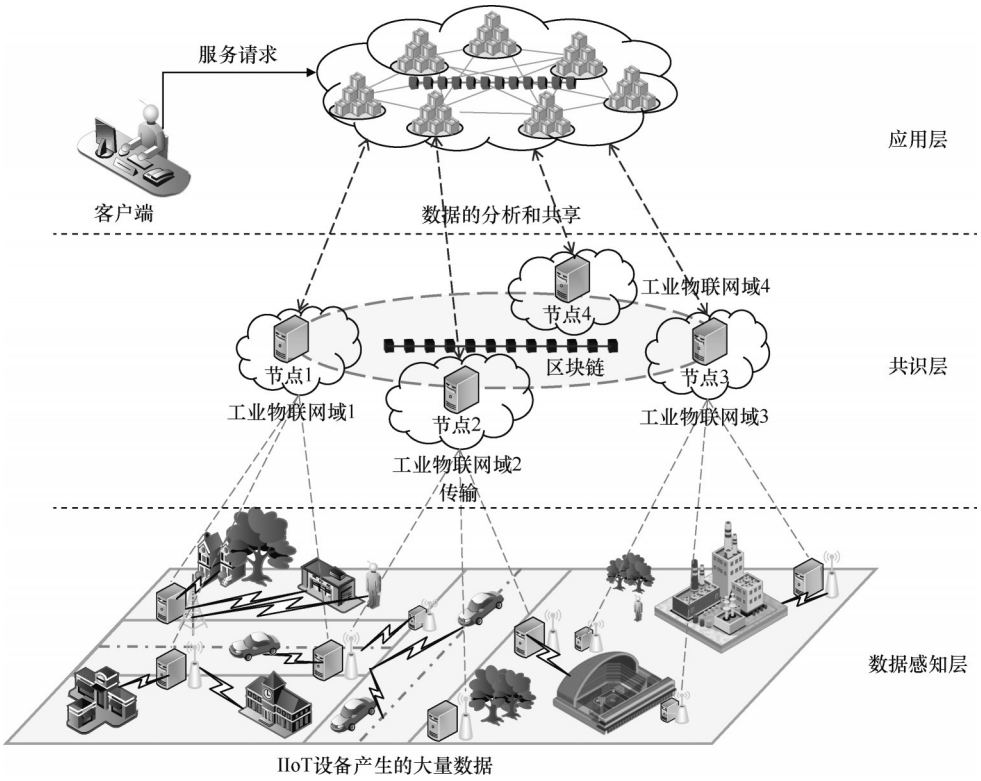


图3　大规模IIoT数据共享场景

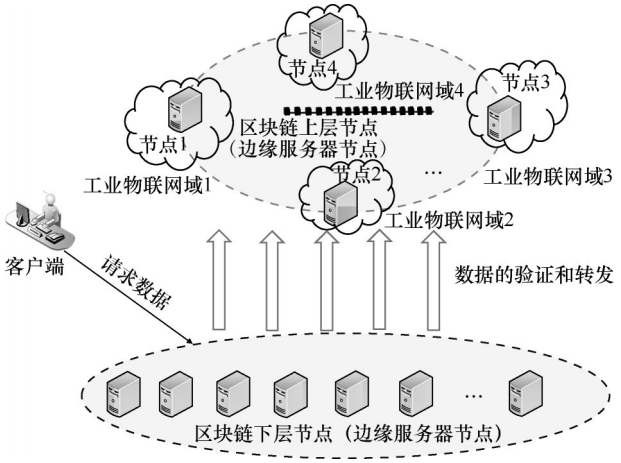


图4　CD-PBFT共识算法模型

由于主节点与从节点的行为对共识结果有着不同程度的影响，将采用不同的计算方式计算它们的共识行为信誉积分值。上层节点i在第t轮的共识行为信誉积分值计算式如下。

若上层节点i为主节点，则有

$$\mathrm{UT}_{\mathrm{cons}}(i,t)=\begin{cases}\min(1,(1+y_p)\mathrm{UT}_{\mathrm{cons}}(i,t-1)), & \text{良性状态}\\ \max(x_p\mathrm{UT}_{\mathrm{cons}}(i,t-1),0), & \text{宕机状态}\\ -1, & \text{作恶状态}\end{cases}\tag{3}$$

若上层节点i为从节点，则有

$$\mathrm{UT}_{\mathrm{cons}}(i,t)=\begin{cases}\min(1,(1+y_b)\mathrm{UT}_{\mathrm{cons}}(i,t-1)), & \text{良性状态}\\ \max(x_b\mathrm{UT}_{\mathrm{cons}}(i,t-1),0), & \text{宕机状态}\\ -1, & \text{作恶状态}\end{cases}\tag{4}$$

其中，x_p与x_b分别代表上层主节点与从节点信誉积分值下降的幅度值，可根据实际需求设置，y_p与y_b分别代表上层主节点和从节点信誉积分值上升的幅度值，一般情况下$y_b<y_p$，即完成参与共识过程时的主节点信誉积分值增加比从节点快。信誉积分模型算法的伪代码如算法1所示。

算法1　信誉积分模型算法

输入　CD-PBFT上层节点的ID$U(\mathrm{id})$，CD-PBFT下层节点的ID$L(\mathrm{id})$，标记节点是否故障$F(\mathrm{id})$，系统中节点总数n

输出　节点的信誉积分值$C(\mathrm{id})$

1) 计算节点的信誉积分值
2) for i = 1 to $U(\mathrm{id})$.length do
3)　$C(\mathrm{id})$ == 0.6
4)　if $F(\mathrm{id})$ then
5)　$C(\mathrm{id})$ − 0.1
6)　else
7)　$C(\mathrm{id})$ + 0.05
8)　end if
9) end for
10) for i = 1 to $L(\mathrm{id})$.length do
11)　$C(\mathrm{id})$ == 0.3
12)　if $F(\mathrm{id})$.then
13)　$C(\mathrm{id})$ − Random(0.04,0.08)
14)　else
15)　$C(\mathrm{id})$ + Random(0.02,0.04)
16)　end if
17) end for

节点的信誉积分T_{cons}根据物联网终端设备在共识过程中每一轮的行为和表现，在每一轮结束时对节点进行信誉评估。将节点分为良性、宕机以及作恶3种状态。良性状态是指在这一轮共识中，若节点i为上层主节点，则节点i产生了有效的区块，并能够正确地达成一致；若节点i为上层从节点，则节点i广播了相同的消息并与大部分节点保持一致；若节点i为下层节点，则节点i转发的写请求与其他大多数下层节点转发的写请求一致。宕机状态是指在这一轮共识中，若节点i为上层主节点，则节点i不生成新区块；若节点i为上层从节点，则节点i由于崩溃无法广播消息；若节点i为下层节点，则上层节点没有收到下层节点i转发的写请求但是收到了其余下层节点转发的写请求。作恶状态是指在这一轮共识中，若节点i为上层主节点，则节点i在这轮共识中生成了一个无效的区块；若节点i为上层从节点，则节点i广播的信息互不相同或者节点i广播的信息与大部分节点不同；若节点i为下层节点，则上层节点收到与其他大部分节点不一致的写请求。

根据节点上一轮参与共识之后的3种状态，信誉积分模型将在每一轮共识之后进行节点的信誉积分值计算，以确保在系统中，保持良好状态的节点能持续参与共识过程。而发生拜占庭故障的节点或频繁崩溃等非拜占庭故障的节点，其信誉积分值将逐渐减至−1或0。当上层节点的信誉积分值降至设定阈值以下时，将其降级至下层，不再直接参与共识。同时，在下层节点中会挑选信誉积分值较高且数据完全同步的节点加入上层节点，以保持共识机制的正常运作。当下层节点的信誉积分值低于设定

阈值时，会将其从系统中排除或者进行强制重置。

4.1.2　双层并行PBFT共识算法

如图5所示，本文在PBFT的基础上提出了一种双层架构，将节点划分为上层和下层。在这一双层架构中，客户端所提交的交易数据将被传送至下层节点，由下层节点对交易数据的合法性进行验证。读操作会直接读取后返回客户端读取结果，写操作由下层节点将请求转发至上层节点。在上层交易数据会经过打包，生成区块参与共识过程。完成共识后，所生成的区块将被同步至下层节点进行存储。通过将交易验证与读写操作并行化，缩短验证时间，降低系统时延，从而显著提升了算法的性能。

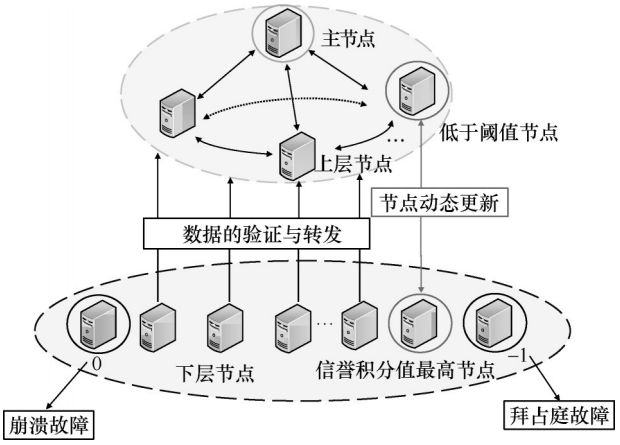


图5　双层架构

结合信誉积分模型实现对发生拜占庭故障节点赋值–1进行定位剔除系统，对崩溃故障等非拜占庭类节点赋值0进行定位重置。通过信誉积分值的奖励与惩罚实现上层共识节点的加入与退出，上层节点低于信誉积分值阈值可以被下层信誉积分值高的节点替换，实现共识节点的动态更新，打破共识节点集群固定、不可动态调整的问题，增加了CD-PBFT算法的稳定性和可靠性。与PBFT相比，CD-PBFT的基于信誉积分模型的双层架构在确保原有安全性基础的同时，进一步提升了共识算法的性能，并增强了可扩展性，使其在面对设备数量众多、数据量庞大的IIoT场景时更具优势。

4.1.3　自适应主节点选取算法

对比PBFT和BFT完成一轮共识过程的通信负荷，主节点的引入可以极大地降低通信量，从而有效地提升系统效率。CD-PBFT中自适应的主节点选取算法实现以随机化的方式在共识节点集群中选取信誉积分值高的节点作为主节点，优化视图转换的主节点选择方式，以保证具有较高信誉积分值的节点成为主节点的概率更大，从而降低主节点发生视图转换的概率，有效减少在共识过程中的资源消耗以及作恶节点成为主节点时区块链更容易遭受攻击的情况发生。

上层共识节点i在第t轮共识中被选为共识主节点的概率为

$$P_{\text{primary}}(i,t)=\frac{\text{UT}_{\text{cons}}(i,t)}{\sum_{j=1}^{N}\text{UT}_{\text{cons}}(j,t)} \tag{5}$$

其中，$\text{UT}_{\text{cons}}(i,t)$表示上层节点$i$在第$t$轮共识行为信誉积分值，$N$表示状态为诚实的共识节点总数。

为了保证主节点选取过程不可预测，生成一个分布在区间[0,1]上的随机数RNum。通过SHA256对最新块的块头进行哈希处理，转换为整数之后对N取余来生成RNum。

$$\text{RNum}=\frac{\text{strTo int}(\text{SHA256}(\text{blockhead}))\bmod N}{N} \tag{6}$$

若节点i被选为新一轮共识的主节点，它需要满足以下条件。

$$\sum_{j=1}^{i-1}P_{\text{primary}}(j,t)\leqslant\text{RNum}\leqslant\sum_{j=1}^{i}P_{\text{primary}}(j,t) \tag{7}$$

选出主节点后，上层共识节点中的其余节点则为从节点，随后所有IoT终端设备节点互相发送验证消息请求达成共识。在所有节点进行一轮完整的共识后，系统会根据整体信誉积分模型将节点重新分类，并重新选择主节点，以保证在共识中综合表现良好的节点可以更换为主节点。主节点选取算法保证了在CD-PBFT共识中信誉积分值高的节点大概率当选主节点。

4.2　CD-PBFT共识算法流程

在PBFT共识过程中包括2次全节点广播，每次数据提交都必须经过两个或多个共识过程。随着网络中节点数增加，单次共识所需的通信次数呈多项式级别增长，大量的通信开销很容易导致算法效率急剧下降。与PBFT不同的是，CD-PBFT在PBFT的基础上设计了双层架构，将所有节点根据网络状态表现划分为上下两层。CD-PBFT共识算法的下层节点验证和发送数据，上层节点完成共识过程。因此时延更低、效率更高。CD-PBFT共识算法流程如图6所示。所有下层节点将验证后的数

据发送给上层各节点，上层各节点接收所有下层节点的数据，通过对比下层节点的数据判断是否为恶意。

CD-PBFT 共识算法包括请求、数据的验证转发、预准备、准备、提交、回复和更新节点信誉积分值 7 个阶段，具体步骤如下。

步骤 1　客户端存储所有下层节点的地址，并向每个下层节点发送请求。请求数据类型可分为读请求和写请求。下层节点在收到客户端发送的请求后，对请求信息的正确性、时间戳、交易数据的重复和冲突等进行验证。验证通过后，对于读请求，下层节点会回复请求执行结果至客户端；对于写请求，下层节点会将消息多播至上层节点。客户端在收到来自多个下层节点的回复后，会将这些消息视为读请求的有效执行结果。

步骤 2　上层节点收到下层节点发送的信息后将对其交易数据是否存在重复和冲突进行验证，验证通过后，对比所有来自候选节点的消息对下层节点验证及转发行为进行评估，同时计算下层节点的信誉积分值。

步骤 3　主节点多播预准备摘要消息到其他节点。

步骤 4　从节点收到预准备消息后验证节点签名，验证通过后将根据摘要寻找本地相对应的消息实体，若本地有相应的请求且与摘要一致，且视图也一致则进入预准备状态。同时多播准备消息，将预准备消息中的摘要记录在 RA [ ]中，RA [ ]是每个节点维护的一个记录表，用于记录节点行为以便于后续计算信誉积分值。

步骤 5　节点收到了 $2f+1$ 个预准备消息，且消息中的当前视图号，主节点分配给请求的编号，请求的摘要信息一致，称该节点进入准备状态，同时将收到的消息中的摘要分别记录在 RA [ ]中，随后多播消息到其他节点。

步骤 6　节点 i 对区块达成了准备状态且收到了 $2f+1$ 个提交消息，则称该节点进入提交状态，此时节点已经对区块达成了共识。

步骤 7　所有节点将会回复客户端消息。主节点将已经达成共识的区块多播到下层节点进行数据同步，以便于下层节点处理读请求。

CD-PBFT 共识算法的伪代码如算法 2 所示。

算法 2　CD-PBFT 共识算法

输入　故障节点的 IDfault_{ID}，节点 ID 的故障类型（0 表示节点发生崩溃故障，–1 表示节点发生拜占庭故障）fault_{ID} - type，系统中节点总数 n

输出　CD-PBFT 上层节点的 ID$U(\text{id})$，CD-PBFT 下层节点的 ID$L(\text{id})$，节点的信誉积分值 $C(\text{id})$

1)设置下层节点计数器 countLow = 0
2)设置上层节点计数器 countUpper = 0
3)设置随机数 Ra$U(\text{id})$
4)for id = 1 to n do
5) if id = fault_{ID}&&fault_{ID} - type = 0 then
6)　$C(\text{id}) == 0$
7)　发生崩溃故障直接对节点 i 进行重置
8)　$C(\text{id}) == 0.3$
9) else if id = fault_{ID}&&fault_{ID} - type = –1then
10)　发生拜占庭故障直接对节点 i 进行剔除
11)　$C(\text{id}) == -1$
12) else $C(\text{id}) == 0.6$
13) end if
14)end for
15)for i = 1 to $U(\text{id})$.length do
16)　if $U(\text{id})$ 发生故障 then

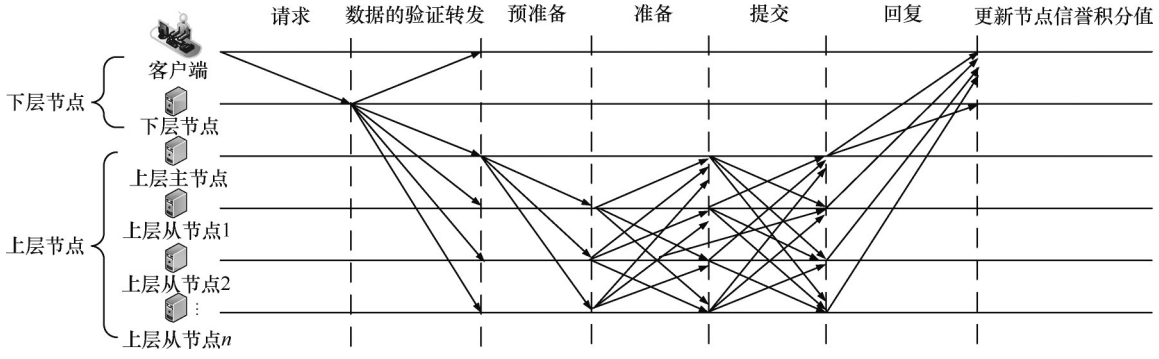


图 6　CD-PBFT 共识算法流程

17) $U(\mathrm{id})$变为下层节点

18) $L'(i)=L(i)$

19) QuickSort$(L'(i),0,n-1)$

20) $L'(0)$变为上层节点

21) end if

22)end for

5 分析

5.1 安全性分析

安全性问题分为2种：抵抗外部攻击和共识安全。安全性的定义是所有无故障节点对本地达到提交状态的区块达成共识并成功执行，在共识算法运行过程中，节点之间存储的数据是一致的。

5.1.1 安全性

外部攻击主要有重放、篡改和分布式拒绝服务（DDoS, distributed denial of service）攻击3种攻击类型，分析对3种主要攻击类型的防御以此来说明CD-PBFT共识算法的安全性。

1) 重放攻击是指攻击者利用先前已合法存在的交易，再次将其传输至网络，旨在误导其他节点和系统。CD-PBFT上层节点可以在准备阶段验证数据的合法性和时效性，抵御重放攻击。

2) 篡改攻击是指利用篡改交易数据的手段来获取账本信息，在持续收集和提交IIoT数据的过程中，可能会频繁发生篡改攻击，而且其破坏性十分严重。在CD-PBFT共识算法中，验证过程可以验证最新消息和消息的一致性，基于哈希算法的抗碰撞性，可以使用消息摘要来检测消息是否被篡改。

3) 分布式拒绝服务攻击是指来自多个不同地理位置的攻击者同时向一个或多个目标发起攻击，或者一个攻击者操纵分布于不同地理位置的多台计算机，利用这些计算机对受害目标进行协同攻击。由于成本和计算能力有限，攻击者控制的上层节点数量不能超过$\frac{1}{3}$。CD-PBFT共识算法可以检测网络中被攻击的恶意节点，保证最终数据的正确性。

本文分别模拟女巫攻击、双重支付、双重投票和DDoS攻击100次，使用Wireshark和Loic测试工具分别测试CD-PBFT与PBFT的抗攻击能力，安全性对比如表1所示，CD-PBFT的抗攻击能力明显优于PBFT。

表1 安全性对比

共识	女巫攻击	双重支付	双重投票	DDoS攻击
PBFT	91%	87%	81%	90%
CD-PBFT	97%	96%	93%	98%

5.1.2 数据一致性

数据一致性指网络中各节点在处理和记录数据过程中达成的共同一致状态。假设节点总数为n，上层和下层有$\frac{n}{2}$个节点，下层节点可以容忍最多f个恶意节点，当存在f个恶意节点发送不一致的消息，同时存在f个节点宕机不发送任何消息，此时需要至少$f+1$个正确的节点正常验证并转发消息到上层节点才可以保证下层节点的正常工作，即$\frac{n}{2}-f-f\geqslant f+1$。CD-PBFT上层节点的共识和PBFT类似。因此，在CD-PBFT中可以保证节点数据的一致性。

5.1.3 数据完整性

在CD-PBFT共识算法中，下层节点对数据的验证阶段可以验证消息的时效性和一致性，基于哈希算法的抗碰撞性可以使用消息摘要来检测消息是否被篡改。CD-PBFT上层节点的共识和PBFT类似，在预准备阶段和准备阶段，上层节点中备份节点会验证主节点的身份和消息的合法性，以防止恶意节点篡改数据。在提交阶段，备份节点通过广播提交消息来保证其他节点执行相同的请求，并达成一致的执行结果。

与数据一致性分析同理，当系统中的下层节点数量满足$\frac{n}{2}-f-f\geqslant f+1$时，CD-PBFT算法下层节点能够容忍最多$f$个拜占庭故障节点，并保证数据的完整性。

5.2 活性分析

活性指在系统中的任何时间点，只要大多数节点是活跃的并且能够正常运行，系统就能继续进行进一步的操作并最终达成共识。为了保持活性，共识应该最小化转换过程和视图转换的频率，避免共识不断转换过程中的无限延迟。

1) 在CD-PBFT中，通过设置等待时间T，可以有效地减少不必要的视图转换频率。在假设当前共识轮未能达成一致的情况下，节点会向网络广播RA[]消息。如果在时间T内，节点收到了$2f+1$个来自不同节点的RA[]消息，系统将直接进入下一

轮共识。然而，如果收到的RA[]消息数量少于$2f+1$，节点将再次向网络广播以获取缺失的RA[]消息，同时将等待时间设置为$1.5T$或$2T$，以减缓过于频繁的视图转换。这种设计可以有效地抵御恶意从节点通过频繁的视图转换来干扰共识过程。

2) 当上层节点中的主节点发生拜占庭故障时，该主节点将因未发出消息或发送恶意消息而触发视图转换，进而进入新的视图并选取新的主节点。在整个系统中，总共存在n个节点，故障主节点为$p=\text{view}\bmod|n|$。由于系统内最多存在$\frac{f}{2}$个拜占庭节点，主节点不会持续处于拜占庭故障状态，因此系统的活性依然可以维持。

6　实验

本节将具体评价本文提出的CD-PBFT共识算法的性能，包括相关方案共识对比、交易时延、吞吐量和信誉积分模型。本文所提共识算法CD-PBFT将与2个具有代表性的共识算法进行比较，即Castro等[21]提出的PBFT共识算法和Wang等[24]提出的基于信誉积分的实用拜占庭容错（CPBFT, practical Byzantine fault tolerance based on credit）共识算法，在相同的实验条件下分别测试其性能。

6.1　设置

使用GoLand集成开发工具，以Go编程语言为基础，构建了一个规模适中的多节点区块链实验系统。本文采用多进程模拟边缘服务器节点，上下层节点信誉积分奖励值和惩罚值可以根据实际需求进行设置，为了使故障节点的信誉积分值快速下降，下降幅度均设为上升幅度的两倍。在此系统中，根据$\frac{n}{2}\geqslant 3f+1$，$f$为恶意节点数，$n$为所有节点数。将PBFT、CPBFT和CD-PBFT这3种共识算法中的拜占庭故障节点数分别设置为1、2、3、4、5个，节点数分别设置为8、14、20、26、32个，当区块包含交易数为1 000、1 500和2 000个时，比较30轮共识后3种共识算法的交易时延和吞吐量。实验配置如表2所示。

6.2　相关方案共识对比

高效率的Raft共识算法无法在不可信的环境下容忍拜占庭故障，可容错的PBFT共识算法无法满足区块链对效率的需求，其中CPBFT共识算法在相关场景有较为广泛的应用。针对IIoT中大量数据同时共识的过程中既要高效又要可容错这两点难以兼顾的问题，如表3所示，本文提出的CD-PBFT共识算法双层架构的设计与其他PBFT类共识算法相比，能够有效降低网络通信开销，并且具有高容错性、节点动态调整的正向激励以及高效率的性能。

表2　　实验配置

参数类别	参数
CPU	Intel i9-12900H
节点数/个	8、14、20、26、32
区块包含交易数/个	1 000、1 500、2 000
信道模型	可靠信道
数据包大小/B	1 000
数据包产生模型	事件触发模型
通信中断概率	0.005%
通信协议	TCP-IP
上层节点初始化信誉积分值	0.6
下层节点初始化信誉积分值	0.3
上层节点信誉积分奖励值	0.05
上层节点信誉积分惩罚值	0.1
下层节点信誉积分奖励值	0.02~0.04
下层节点信誉积分惩罚值	0.04~0.08

表3　　相关方案共识对比

共识	网络通信开销	容错性	节点动态调整	效率
Raft	$2N-2$	不容错	否	高
PBFT	$2N^2+N$	$3f+1$	否	低
CPBFT	N^2-N	$3f+1$	否	较高
CD-PBFT	$\frac{1}{2}N^2+2N$	$6f+2$	是	高

6.3　交易时延

交易时延指客户端向主节点发送交易请求后到客户端确认完成共识所需的时间间隔。PBFT、CPBFT和CD-PBFT交易时延对比如图7所示，本实验同时设置了1 000、1 500和2 000个不同的区块打包交易数（batch），以便观测区块打包交易数对共识性能的影响。随着区块打包交易数的增加，交易时延逐步增大，但在相同条件下，CD-PBFT的交易时延始终低于PBFT和CPBFT。

从最值来看，在节点数为32、区块打包交易数为2 000个的条件下，CD-PBFT的交易时延达到了最高值7 146 ms，而同等条件下PBFT的交易时延达到了11 682 ms，CPBFT的交易时延达到了9 125 ms。相较于PBFT共识算法，CD-PBFT的打包交易时延降低了38.8%，而CPBFT的打包交易时

延降低了21.9%。在节点数为8、区块打包交易数为1 000个的条件下，CD-PBFT的交易时延达到了最低值468 ms，而同等条件下PBFT的交易时延达到了681 ms，CPBFT的交易时延达到了500 ms。相较于PBFT共识算法，CD-PBFT的打包交易时降低了31.3%，而CPBFT的打包交易时延降低了26.6%。从平均值来看，CD-PBFT共识算法平均打包交易时延相较于PBFT降低了34.8%，而CPBFT共识算法平均打包交易时延相较于PBFT降低了23.9%。另外，随着区块打包交易数和节点数的增加，CD-PBFT的交易时延增长速度都低于PBFT与CPBFT，这表明在大规模节点场景下，CD-PBFT的交易时延优于PBFT与CPBFT。

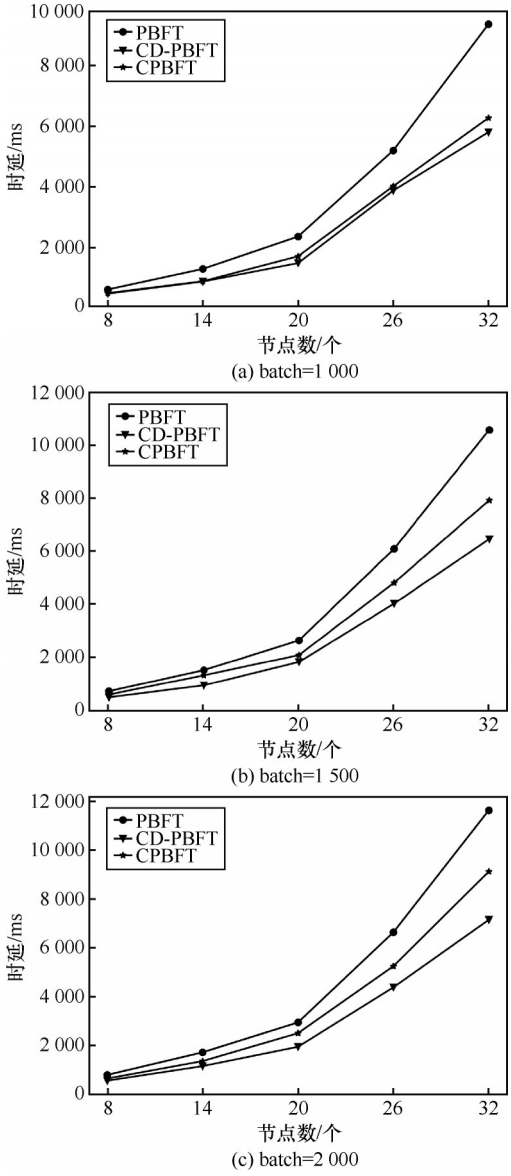


图7　PBFT、CPBFT和CD-PBFT交易时延对比

6.4　吞吐量

吞吐量指在特定时间单位内完成的交易数。PBFT、CPBFT和CD-PBFT吞吐量对比如图8所示。测量吞吐量的实验设置与时延一致。随着区块打包交易数的增加，吞吐量逐步增大，但在相同条件下，CD-PBFT的吞吐量始终高于PBFT和CPBFT。

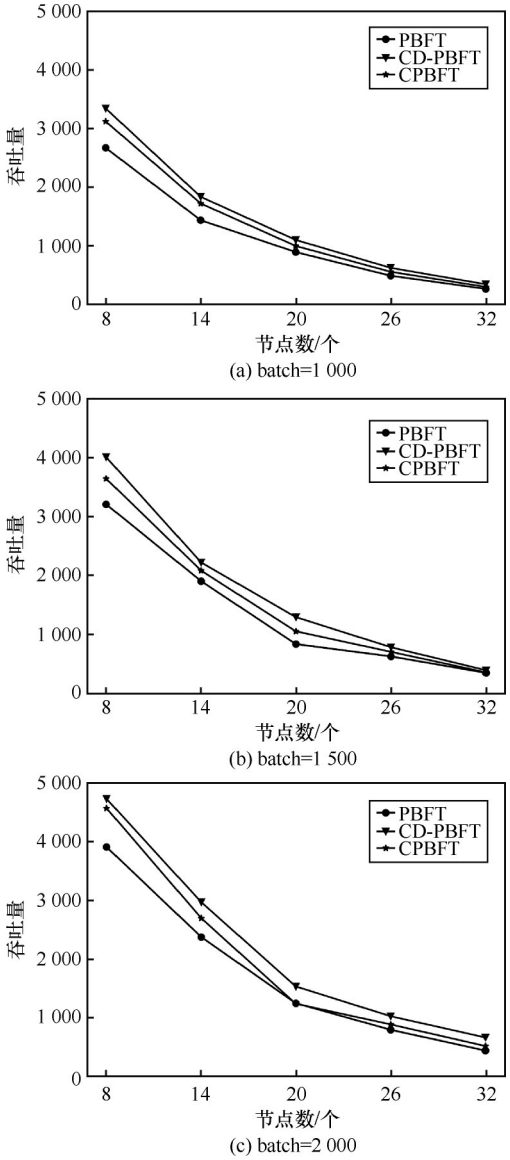


图8　PBFT、CPBFT和CD-PBFT吞吐量对比

从最值来看，在节点数为8、区块打包交易数为2 000个的条件下，CD-PBFT的吞吐量达到了最高值4 732，而同等条件下PBFT的吞吐量只有3 911，CPBFT的吞吐量为4 572。相较于PBFT共识算法，CD-PBFT的吞吐量提升了21.0%，而CPBFT的吞吐量提升了16.9%。在节点数为32，区块打包交易数为1 000个的条件下，CD-PBFT的吞

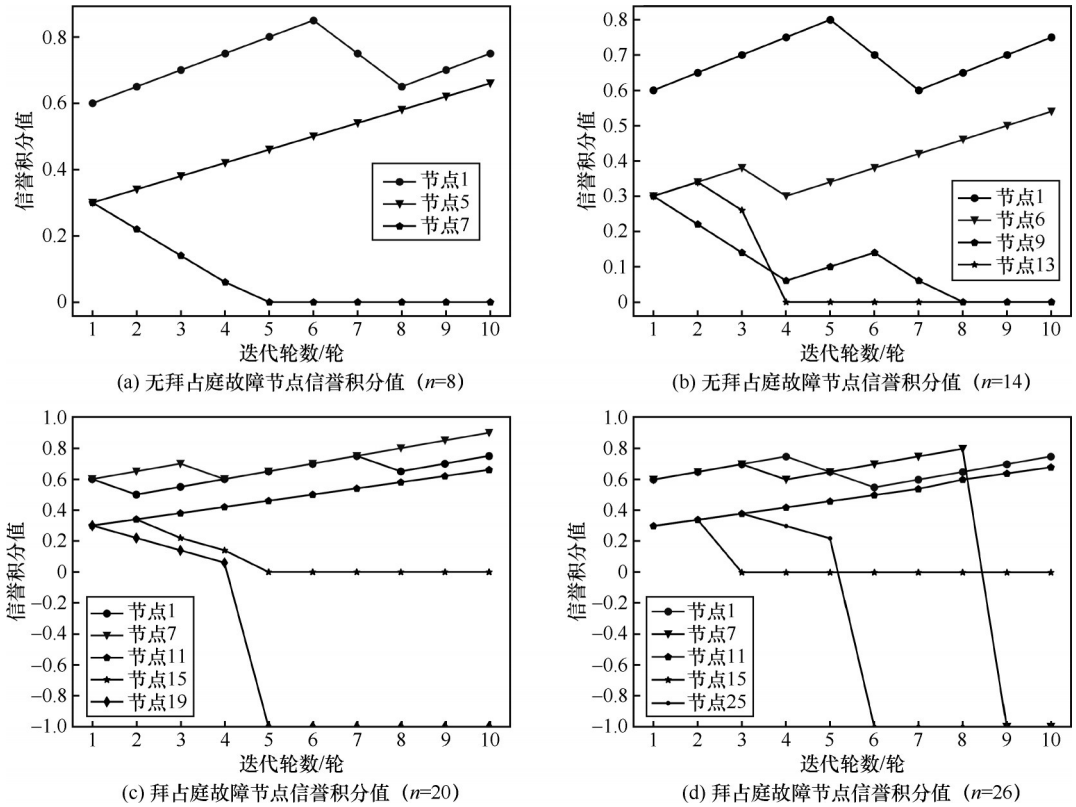
吐量达到了最低值344，而同等条件下PBFT的吞吐量只有263，CPBFT的吞吐量为296。相较于PBFT共识算法，CD-PBFT的吞吐量提升了30.8%，而CPBFT的吞吐量提升了12.5%。从平均值来看，CD-PBFT共识算法平均吞吐量较PBFT提升了25.2%，而CPBFT共识算法平均吞吐量较PBFT提升了14.8%。另外，随着区块打包交易数和节点数的增加，CD-PBFT的吞吐量下降速度都低于PBFT与CPBFT，这表明在大规模节点场景下，CD-PBFT的吞吐量优于PBFT与CPBFT。

在CD-PBFT共识算法中，读写操作得以独立执行，上层节点专注于写操作执行，并且不需要对交易的合法性进行验证。这种操作分离实现了从串行验证转变为并行验证，进而节约了验证所需时间，从而有效提升了系统的吞吐量。

6.5　信誉积分模型评估

Timer表示拜占庭故障在随机节点发生的时间。在实验中，将Timer设定在5~6 s。设置任意节点i在Timer指定的时间向不同节点发送不一致的消息，以模拟拜占庭故障。

图9记录了节点的信誉积分值变化。上层节点的初始信誉积分值为0.6，下层节点的初始信誉积分值为0.3。图9(a)和图9(b)分别为节点数为8和14时，系统中无拜占庭故障节点信誉积分值的变化情况。图9(c)和图9(d)分别为节点数为20和26时，系统中拜占庭故障节点信誉积分值的变化情况。在图9(a)中，节点1是上层的从节点，可以看出，节点1在第6~8轮时有短暂的宕机行为，信誉积分值下降，从第9轮开始恢复正常，所以在9~10轮信誉积分值增加。节点5正确地验证消息并将消息发送到上层节点，如果一直正常工作，信誉积分值会稳步上升到1。节点7处于崩溃状态或不发送任何消息，节点7的信誉积分值迅速下降，经过5轮迭代，信誉积分值变成了0。在图9(b)中，节点1和节点6虽然有短暂的宕机行为，但是恢复正常后信誉积分值继续上升。而节点9和节点13的信誉积分值会因为持续的崩溃而下降，直至变为0。在图9(c)中，节点15没有正确执行验证并转发消息，信誉积分值降低了，由于节点15处于崩溃或不工作状态，信誉积分值持续下降至0。节点19在共识过程中的第5轮发生拜占庭故障，导致节点19的信誉积分值直接变为–1。图9(d)中的节点15在第3轮信誉积分



(a) 无拜占庭故障节点信誉积分值（n=8）　(b) 无拜占庭故障节点信誉积分值（n=14）

(c) 拜占庭故障节点信誉积分值（n=20）　(d) 拜占庭故障节点信誉积分值（n=26）

图9　节点的信誉积分值变化

值直接降为0，节点7和节点25分别在第9轮和第6轮发生拜占庭故障，信誉积分值直接降至–1。

本文通过信誉积分模型提高共识节点的参与度，高信誉积分值的共识节点更有动力积极参与区块链网络的共识过程、交易处理和交易验证，节点通过积极地参与共识过程来维护或提高本身的信誉积分值。信誉积分模型采用奖励和惩罚机制来激励节点的良好行为和惩罚节点的不良行为，从而达到正向激励。高信誉积分的节点会获得更多的奖励，直接参与共识或当选主节点，低信誉积分的节点会受到惩罚，减少权益或限制参与度。

无论系统中是否发生拜占庭故障，信誉积分模型均能检测并及时更新节点的信誉积分值。通过信誉积分值的动态调整，更高效地识别不稳定节点与恶意节点，并将其从共识群组中剔除或强制重置，这一措施有效地应对了PBFT中难以排除故障节点的问题。

7 结束语

本文提出了一种基于CD-PBFT的共识算法，用于解决IIoT场景中的网络和终端数据可信共享存在的问题。通过信誉积分模型评估网络中各个节点的状态，降低恶意节点出现的频率，保证系统安全性；采用双层架构，将节点分为上下两层，实现交易验证和读写操作的并行处理；基于节点的信誉积分值进行自适应主节点选取算法，提高信誉积分值高的节点当选主节点的概率。仿真结果表明，CD-PBFT能够有效节省验证时间，提升算法性能及稳定性。

在未来的工作中，可围绕以下几个方面进行下一步的研究工作。1) 在信誉积分模型中的节点奖励与惩罚机制方面，引入博弈论思想以改进信誉积分的计算方法，从而更精准地评估网络状态，并逐步降低CD-PBFT算法在时间消耗方面的代价；2) 增强节点检测功能，实现对节点表现的动态评估，以更准确地反映节点状况，防止节点实时作恶；3) 结合IoT的身份认证、数据加密和访问控制技术，解决IoT终端设备不可信可能带来的安全性问题。

参考文献：

[1] MERMER G B, ZEYDAN E, ARSLAN S S. An overview of blockchain technologies: principles, opportunities and challenges[C]//Proceedings of the 2018 26th Signal Processing and Communications Applications Conference (SIU). Piscataway: IEEE Press, 2018: 1-4.

[2] 邵奇峰, 金澈清, 张召, 等. 区块链技术: 架构及进展[J]. 计算机学报, 2018, 41(5): 969-988.
SHAO Q F, JIN C Q, ZHANG Z, et al. Blockchain: architecture and research progress[J]. Chinese Journal of Computers, 2018, 41(5): 969-988.

[3] 徐蜜雪, 苑超, 王永娟, 等. 拟态区块链: 区块链安全解决方案[J]. 软件学报, 2019, 30(6): 1681-1691.
XU M X, YUAN C, WANG Y J, et al. Mimic blockchain:solution to the security of blockchain[J]. Journal of Software, 2019, 30(6): 1681-1691.

[4] ZHANG F, DING Y. Research on the application of Internet of things and block chain technology in improving supply chain financial risk management[C]//Proceedings of the 2021 International Conference on Computer, Blockchain and Financial Development (CBFD). Piscataway: IEEE Press, 2021: 347-350.

[5] CHEN X Y, LIU S, ZHU W T, et al. Transition to the intelligent services ecosystem: integration of block chain and Internet of things in supply chain management[C]//Proceedings of the 2020 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA). Piscataway: IEEE Press, 2020: 1166-1170.

[6] WU D, ANSARI N. A trust-evaluation-enhanced blockchain-secured industrial IoT system[J]. IEEE Internet of Things Journal, 2021, 8(7): 5510-5517.

[7] LUCAS B, PÁEZ R V. Consensus algorithm for a private blockchain[C]//Proceedings of the 2019 IEEE 9th International Conference on Electronics Information and Emergency Communication (ICEIEC). Piscataway: IEEE Press, 2019: 264-271.

[8] ONGARO D, OUSTERHOUT J. In search of an understandable consensus algorithm[C]//Proceedings of the 2014 USENIX Annual Technical Conference (USENIX ATC 14). Berkeley: USENIX Association, 2014: 305-319.

[9] JIANG Z Y, CAO Z X, KRISHNAMACHARI B, et al. SENATE: a permissionless Byzantine consensus protocol in wireless networks for real-time Internet-of-things applications[J]. IEEE Internet of Things Journal, 2020, 7(7): 6576-6588.

[10] DOUCEUR J R. The sybil attack[C]//International Workshop on Peer-to-Peer Systems. Berlin: Springer, 2002: 251-260.

[11] 赖英旭, 薄尊旭, 刘静. 基于改进PBFT算法防御区块链中sybil攻击的研究[J]. 通信学报, 2020, 41(9): 104-117.
LAI Y X, BO Z X, LIU J. Research on sybil attack in defense blockchain based on improved PBFT algorithm[J]. Journal on Communications, 2020, 41(9): 104-117.

[12] LAO L, DAI X H, XIAO B, et al. G-PBFT: a location-based and scalable consensus protocol for IoT-blockchain applications[C]//Proceedings of the 2020 IEEE International Parallel and Distributed Processing Symposium (IPDPS). Piscataway: IEEE Press, 2020: 664-673.

[13] MAKHDOOM I, TOFIGH F, ZHOU I, et al. PLEDGE: an IoT-oriented proof-of-honesty based blockchain consensus protocol[C]//Proceedings of the 2020 IEEE 45th Conference on Local Computer Networks (LCN). Piscataway: IEEE Press, 2020: 54-64.

[14] YANG J, JIA Z H, SU R G, et al. Improved fault-tolerant consensus based on the PBFT algorithm[J]. IEEE Access, 2022, 10: 30274-30283.

[15] DORRI A, JURDAK R. Tree-chain: a lightweight consensus algorithm

for IoT-based blockchains[C]//Proceedings of the 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). Piscataway: IEEE Press, 2021: 1-9.

[16] XU X Q, SUN G, YU H F. An efficient blockchain PBFT consensus protocol in energy constrained IoT applications[C]//Proceedings of the 2021 International Conference on UK-China Emerging Technologies (UCET). Piscataway: IEEE Press, 2021: 152-157.

[17] THAKKER J, PARK Y. Resilient and efficient blockchain consensus protocol for Internet-of-things[C]//Proceedings of the 2020 IEEE International Conference on Consumer Electronics (ICCE). Piscataway: IEEE Press, 2020: 1-6.

[18] ZHOU S M, YING B D. VG-Raft: an improved Byzantine fault tolerant algorithm based on Raft algorithm[C]//Proceedings of the 2021 IEEE 21st International Conference on Communication Technology (ICCT). Piscataway: IEEE Press, 2021: 882-886.

[19] ZHANG X D, LI R, ZHAO H. A parallel consensus mechanism using PBFT based on DAG-lattice structure in the Internet of vehicles[J]. IEEE Internet of Things Journal, 2023, 10(6): 5418-5433.

[20] 刘峰, 杨杰, 李志斌, 等. 一种基于区块链的泛用型数据隐私保护的安全多方计算协议[J]. 计算机研究与发展, 2021, 58(2): 281-290.
LIU F, YANG J, LI Z B, et al. A secure multi-party computing protocol for universal data privacy protection based on blockchain[J]. Journal of Computer Research and Development, 2021, 58(2): 281-290.

[21] CASTRO M, LISKOV B. Practical Byzantine fault tolerance[C]//Proceedings of the Third Symposium on Operating Systems Design and Implementation. New York: ACM Press, 1999: 173-186.

[22] 冯了了, 丁澔, 刘坤林, 等. 区块链BFT共识算法研究进展[J]. 计算机科学, 2022, 49(4): 329-339.
FENG L L, DING Y, LIU K L, et al. Research advance on BFT consensus algorithms[J]. Computer Science, 2022, 49(4): 329-339.

[23] 黄冬艳, 李浪, 陈斌, 等. RBFT: 基于Raft集群的拜占庭容错共识机制[J]. 通信学报, 2021, 42(3): 209-219.
HUANG D Y, LI L, CHEN B, et al. RBFT: a new Byzantine fault-tolerant consensus mechanism based on Raft cluster[J]. Journal on Communications, 2021, 42(3): 209-219.

[24] WANG Y, SONG Z, CHENG T. Improvement research of PBFT consensus algorithm based on credit[C]//International Conference on Blockchain and Trustworthy Systems. Berlin: Springer, 2019: 47-59.

[作者简介]

李凤岐（1974– ），男，满族，河北承德人，博士，大连交通大学教授，主要研究方向为区块链、工业物联网、智能信息系统等。

宋晴晴（1997– ），女，河北邯郸人，大连交通大学硕士生，主要研究方向为区块链共识算法。

徐辉（1999– ），男，安徽芜湖人，大连交通大学硕士生，主要研究方向为物联网安全、区块链共识算法。

杜学峰（1999– ），男，山西大同人，大连交通大学博士生，主要研究方向为分布式集群控制、无人机群体智能。

高嘉隆（1997– ），男，辽宁鞍山人，大连交通大学硕士生，主要研究方向为区块链共识算法。

佟宁（1981– ），女，辽宁盘锦人，博士，大连交通大学副教授，主要研究方向为网络安全、人工智能、区块链等。

王德广（1968– ），男，辽宁大连人，大连交通大学副教授，主要研究方向为区块链、信息安全、大数据等。