计算机科学
COMPUTER SCIENCE

基于信用评价模型的Raft共识算法

刘炜, 郭灵贝, 夏玉洁, 佘维, 田钊

引用本文

刘炜, 郭灵贝, 夏玉洁, 佘维, 田钊基于信用评价模型的Raft共识算法[J]. 计算机科学, 2023, 50(6): 322-329.

LIU Wei, GUO Lingbei, XIA Yujie, SHE Wei, TIAN Zhao. Raft Consensus Algorithm Based on Credit Evaluation Model [J]. Computer Science, 2023, 50(6): 322-329.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.220500171

基于信用评价模型的 Raft 共识算法

刘　炜[1,2,3]　郭灵贝[1,2]　夏玉洁[1,2]　佘　维[1,2,3]　田　钊[1,2]
1 郑州大学网络空间安全学院　郑州 450000
2 郑州市区块链与数据智能重点实验室　郑州 450000
3 郑州大学互联网医疗与健康服务河南省协同创新中心　郑州 450000
(wliu@zzu.edu.cn)

摘　要　在车联网中,车辆节点间需要交通信息的共享和交互,但目前还存在着节点之间难以高效同步交通数据信息以及恶意节点传播虚假信息的问题。针对上述问题,提出了一种基于信用评价模型的 Raft 共识算法(CE-Raft)。首先构建信用评价模型,基于孤立森林异常检测算法检测拜占庭车辆节点并将其剔除,生成诚实节点编号表;然后进行领导者选举,通过修改跟随者节点的投票过程,实现诚实节点当选领导者;最后进行日志复制,领导者节点根据诚实节点编号表发送信息同步请求,确保正确的消息在节点间达成共识。实验结果表明,CE-Raft 算法能够有效排除拜占庭节点,提高了诚实节点预测准确率,具有较低的时延和较高的吞吐量,使车联网在存在恶意节点的情况下,仍然能安全高效地完成数据共享。

关键词:区块链;Raft;孤立森林;拜占庭容错
中图法分类号　TP302

Raft Consensus Algorithm Based on Credit Evaluation Model

LIU Wei[1,2,3],GUO Lingbei[1,2],XIA Yujie[1,2],SHE Wei[1,2,3] and TIAN Zhao[1,2]
1 School of Cyber Science and Engineering,Zhengzhou University,Zhengzhou 450000,China
2 Zhengzhou Key Laboratory of Blockchain and Data Intelligence,Zhengzhou 450000,China
3 Henan Collaborative Innovation Center for Internet Medical and Health Services,Zhengzhou University,Zhengzhou 450000,China

Abstract　In the Internet of Vehicles,the sharing and interaction of traffic information is required between vehicle nodes. However,at present,there are still problems such as the difficulty in efficiently updating traffic data information between vehicle nodes and the dissemination of false information by malicious vehicle nodes. Aiming at the above problems,this paper proposes a Raft consensus algorithm based on credit evaluation model(CE-Raft). First,the credit evaluation model is constructed,and Byzantine vehicle nodes are detected and eliminated based on the isolated forest anomaly detection algorithm,and then an honest node number table is generated. Then the leader election is performed,and the honest node is elected as the leader by modifying the voting process of the follower node. Finally,log replication is performed,the leader node send an information synchronization request according to the honest node number table to ensure that the correct message reaches a consensus among the nodes. Experimental results show that the CE-Raft algorithm can effectively exclude Byzantine nodes,improve the prediction accuracy of honest nodes,and has lower latency and higher throughput,so that the Internet of Vehicles can still complete data sharing safely and efficiently in the presence of malicious nodes.

Keywords　Blockchain,Raft,Isolated forest,Byzantine fault tolerance

到稿日期:2022-05-18　返修日期:2022-10-11
基金项目:河南省高校科技创新人才支持计划(21HASTIT031);河南省重大公益专项(201300210300);河南省高等学校青年骨干教师培养计划(2019GGJS018);河南省重点研发与推广专项(212102310039,212102310554);郑州大学教育教学改革研究与实践项目(2021ZZUJGLX168)
This work was supported by the Program for Science & Technology Innovation Talents in Universities of Henan Province(21HASTIT031),Major Public Welfare Project of Henan Province(201300210300),Training Plan for Young Backbone Teachers of Colleges and Universities in Henan(2019GGJS018),Key R & D and Promotion Project in Henan Province(212102310039,212102310554) and Zhengzhou University Education and Teaching Reform Research and Practice Project(2021ZZUJGLX168).
通信作者:田钊(tianzhao@zzu.edu.cn)

1　引言

随着信息通信技术的快速发展，汽车和道路日益智能化，越来越多的汽车和路边基础设施安装了通信设备[1]。车辆与车辆、车辆与人、车辆与道路之间都需要网络通信的连接，这使得车联网技术成为交通行业关注与研究的重点。但目前车联网采用传统的集中式服务器管理数据，存在中心化单点故障和安全性较低的问题，且车联网动态网络拓扑变化速度快、车辆节点移动速率快、通信时间长、易受恶意攻击[2]，使车联网系统的数据也难以实现安全高效的共享。而区块链作为一种去中心化的分布式账本的新技术[3]，其去中心化特性可以改善车联网传统的中心化管理问题，区块链中的共识机制又可以满足车联网中数据实时传递和共享的需求[4]。因此将区块链与车联网结合可以更好地推动车联网的发展。

在区块链和车联网的结合中，车辆之间的数据如何实现高效安全的共享是目前众多学者研究的方向。文献[5]使用区块链中传统的工作量证明算法来实现车辆之间数据的共享，但存在着严重的效率低下和资源浪费问题，文献[6]提出了一种增强验证的股权授权证明算法来实现车联网中车辆数据的共享，虽然在一定程度上解决了工作量证明算法资源消耗过高的问题，但会导致寡头优势，有失公平性。文献[7]在基于区块链技术的车联网安全通信策略中采用 Raft 共识算法来降低车辆数据共享的时延并提高吞吐量，但传统的 Raft 算法不能抵抗车联网内部的恶意节点。文献[8]在基于区块链的车联网架构中采用改进的实用拜占庭容错 PBFT 算法进行数据共享，虽然可以容忍一定的恶意节点，但却无法承载较大的通信量且算法效率较低。

针对目前车联网中数据共享采用的共识算法存在的效率较低或者不能抵抗恶意节点的问题，本文提出了一种基于孤立森林构建信用模型的 Raft 共识算法（Raft Consensus Algorithm Based on Credit Evaluation Model，CE-Raft）。引入孤立森林异常检测算法构建信用评价模型，对节点信用度划分指标进行评估加权计算，在节点参与共识过程中将恶意节点排除，使 CE-Raft 共识算法可以应用于具有拜占庭车辆节点的车联网网络环境中，且具备低时延、高吞吐量的特性。

2　相关工作

车辆节点能够对产生的大量数据进行安全共享是车联网发展的前提和保障。为解决车联网数据共享安全的问题，文献[9]在车辆节点互发消息中使用对称加密算法，发送方用私钥对消息进行签名，接收方使用从证书颁发机构获得的发送方的公钥对其进行解密；文献[10]中车辆之间使用应答协议，通过 RSU 来检查消息的正确性和发送消息的车辆节点的安全性；文献[11]提出了一种异构资源智能动态匹配的车联边缘网络系统架构，以防止恶意节点篡改伪造真实交易记录，确保车联网数据共享的安全性；文献[12]提出了一种用于车辆数据认证的四级分层信任模型，使用化名方案来解决车辆跟踪问题，以匿名化车辆名称和证书颁发代理的方式，防止车辆发送虚假数据。上述方法都是传统的集中式中心化的车联网解决数据共享所采用的方法，当中心服务器节点发生故障时，数据将无法安全地共享。

而区块链作为一种分布式的、链上数据难以篡改的数据存储系统[13-14]，可以实现车联网去中心化的数据安全共享[15]。文献[16]提出了 3 种通用数据共享模型，利用区块链技术结合车联网实现数据安全共享，并详细分析了区块链应用于车联网的优势。其中车联网利用区块链中的共识机制[17]对促进车辆间数据共享和保证数据安全有着重要意义，但目前区块链主流共识机制仍然需要在安全[18]和效率[19]上有所提升才能更好地适应车联网。

Raft 算法是用来管理复制日志的一致性协议。相比车联网中常用的 PBFT 算法，Raft 算法资源消耗少、效率高，但不能容忍拜占庭错误。为了使其能够在具有拜占庭节点的网络中得到使用，越来越多的学者在拜占庭容错方面对 Raft 算法进行了优化研究。文献[20]提出了 Raft 算法的改进算法 CRaft，通过删除校正码对日志消息进行容错。文献[21]提出了一种基于验证的拜占庭容错共识协议 VBBFT-Raft，通过引入数字签名和嵌套哈希机制，使 Raft 拜占庭容错。文献[22]提出了一种拜占庭容错算法 B-Raft，其将 Raft 与 BLS 签名机制相结合来对抗恶意节点。文献[23]提出了一种结合 Schnorr 签名机制的拜占庭容错 B-Raft 算法，防止拜占庭节点伪造选票。文献[24]提出了一种基于信用模型的区块链一致性 CRaft 算法，该算法引入支持向量机（SVM）算法，防止拜占庭节点参与共识过程。文献[25]提出了一种基于验证组的改进拜占庭容错算法 VG-Raft，通过节点的信任值和通信延迟选择验证者组成验证组检查共识过程来保证一致性。文献[26]将 PoB 算法与 Raft 算法相结合，提出了一种基于行为的复杂网络快速区块链协议 Beh-Raft-Chain。根据节点的资金和行为进行加权，设计均衡的分配算法，激励诚实的行为并压制恶意攻击。文献[27]提出了一种基于 Raft 集群的拜占庭容错共识机制 RBFT。RBFT 对网络节点进行分组，组内采用改进的 Raft 机制进行共识，组间选出领导者组成网络委员会，采用 PBFT 机制进行共识。文献[28]提出了一种改进的一致性算法 C-Raft-PBFT，通过将 Raft 算法和 PBFT 算法与信用机制相结合，设计节点信用评估和分级协议，增加基于反馈机制的拜占庭式节点检测的方法来防止拜占庭节点行为。

上述方法在拜占庭容错方面的优化研究中，将 Raft 算法在节点共识过程中与数字签名或其他容错算法相结合，对消息进行签名和加密来防止恶意节点传输错误信息。但是加解密过程中秘钥产生的过程繁琐，与其他容错算法相结合会增加算法复杂性并产生额外的开销，因此本文提出了一种基于孤立森林构建信用模型的 CE-Raft 共识算法。该算法在共识之前根据信用评价模型生成的诚实节点编号表筛选出诚实节点，保证只有诚实节点当选领导者进行日志复制的共识过程，防止恶意节点传输错误信息，使 CE-Raft 共识算法在车联网系统中实现车辆节点之间数据安全高效的共享。

3　CE-Raft 算法

3.1　算法概述

本文基于 CE-Raft 算法构建一种车联网系统模型，系统

模型如图 1 所示。模型包括两种通信类别：车辆与车辆之间的通信和车辆与路边设备之间的通信。车辆和路边设备都由管理者进行维护和注册。车辆节点数量多，但是存储能力有限，不能存储完整的道路交通信息，路边设备等这类节点具有稳定的供电和较高的存储空间，可以用来存储整个路况交通信息。

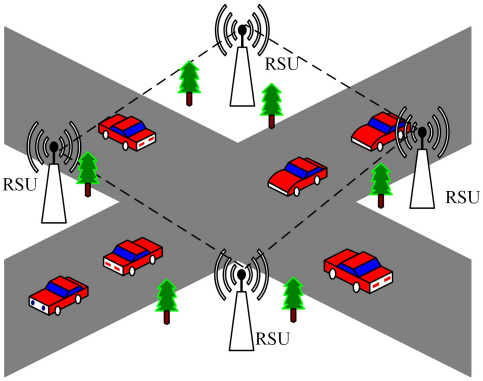

图 1 车联网系统模型

Fig. 1 IoV system model

模型各部分功能如下：

(1)车辆节点：车联网系统模型中的轻量节点，代表车辆，用来分享道路交通信息，且与距离最近的路边设备进行通信。

(2)路边设备：路边设备作为车联网系统模型中的全节点，收集和接收路上车辆节点提供的交通信息，同步并记录完整的信息。

(3)管理者：交通管理部门，维护车辆和路边设备的正常运行。

车辆节点之间使用 CE-Raft 算法来达成对交通数据信息的共识，并与路边设备进行信息的同步，路边设备再将达成共识的交通数据信息上链。CE-Raft 算法共分为 3 个阶段：信用评价模型构建阶段、领导者选举阶段、日志复制阶段。其流程图如图 2 所示。

(1)信用评价模型构建阶段：对参与共识的节点进行信用评估，引入孤立森林异常检测算法，排除拜占庭行为的节点，获取到诚实节点的编号表。为领导者选举阶段和日志复制阶段做准备。

(2)领导者选举阶段：节点根据时间超时设置转变为候选者状态，并发起投票请求，各跟随者节点根据诚实节点编号表投票选举出领导者。

(3)日志复制阶段：领导者节点接收客户端发送的日志信息，并将该日志条目复制追加到系统中诚实节点编号表中的节点，达成一致性共识。

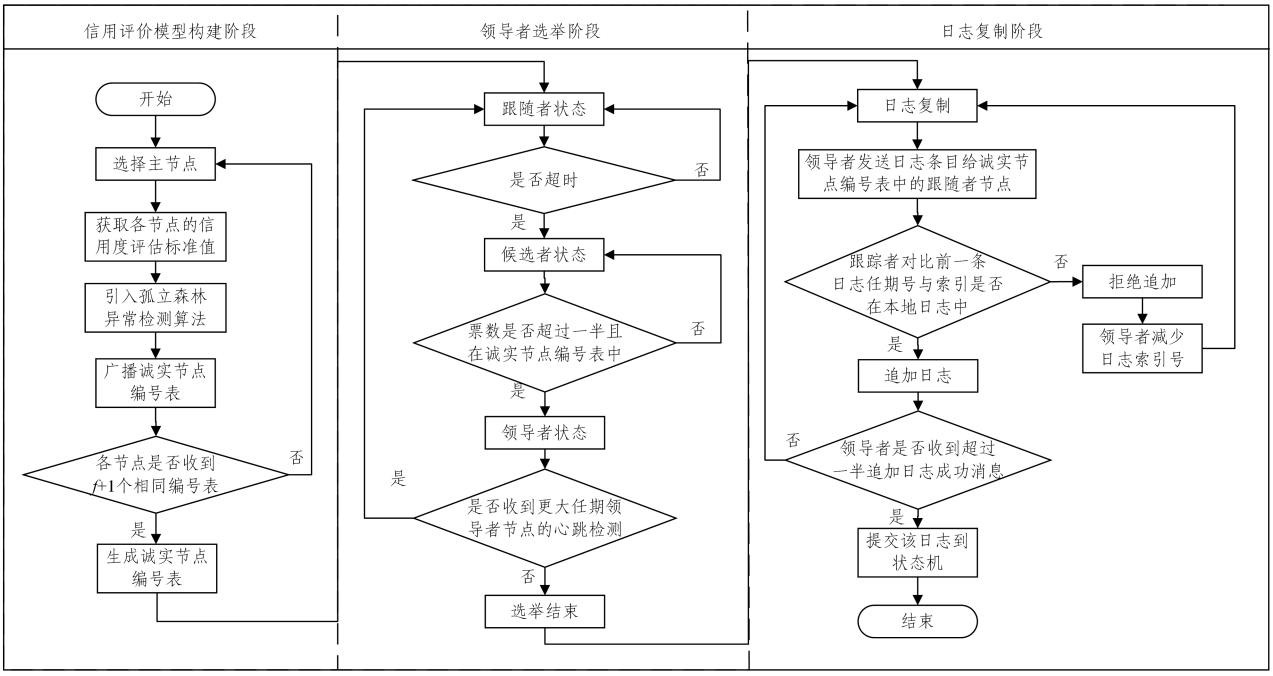

图 2 CE-Raft 算法流程

Fig. 2 CE-Raft algorithm flow

3.2 算法过程

3.2.1 信用评价模型构建阶段

本文算法通过构建一个信用评价模型来过滤系统中的拜占庭节点。先建立一个节点信用度评估标准表，把节点信用度评估指标分为三大类：节点表现、节点诚实度和节点交易能力。再把这三大类中的每一类分成不同的指标，如表 1 所列。

节点编号由节点加入网络的时间确定。主节点首先根据此标准获取各个节点的信用度评估表，然后对每个节点的信用度评估表中各个指标的数据进行标准化处理，根据表 1 构建信用度评估指标集，$X=\{x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8\}$。其中，$x_1$ 为网络延时时间，x_2 为节点离线次数，x_3 为节点离线时间，x_4 为节点加入网络持续时间，x_5 为是否提供无效事务，x_6 为节点上一轮是否诚实，x_7 为共完成多少事务交易，x_8 为上一轮完成多少事务，正向指标为 x_4,x_6,x_7,x_8，负向指标为 x_1,x_2,x_3,x_5。

$$\text{利用公式：}y_{ij}=\begin{cases}\dfrac{x_{ij}-\mathrm{Min}(X_j)}{\mathrm{Max}(X_j)-\mathrm{Min}(X_j)}, & j=4,6,7,8\\ \dfrac{\mathrm{Max}(X_j)-x_{ij}}{\mathrm{Max}(X_j)-\mathrm{Min}(X_j)}, & j=1,2,3,5\end{cases} \tag{1}$$

其中，x_{ij} 为第 i 个节点第 j 个指标的数据值，$\mathrm{Min}(X_j)$ 为第 j 个指标所有节点数据的最小值，$\mathrm{Max}(X_j)$ 为第 j 个指标所有节点数据的最大值。

表 1　节点信用度评估标准

Table 1　Node credit evaluation standard

Index	Explanation
节点表现	网络延时时间
	节点离线次数
	节点离线时间
节点诚实度	节点加入网络持续时间
	是否提供无效事务
	节点上一轮是否诚实
节点交易能力	共完成多少事务交易
	上一轮完成多少事务

首先计算车辆节点的每一个指标数据得出标准化数据。例如节点网络延时时间最小为 5 ms，最大为 50 ms，则网络延时时间为 20ms 的标准化数据为 $y=0.66$。

其次求出各指标的信息熵：

$$E_j=-\frac{1}{\ln n}\sum_{i=1}^{n}p_{ij}\ln p_{ij} \tag{2}$$

其中，y_{ij} 为标准化数据，$p_{ij}=y_{ij}/\sum_{i=1}^{n}y_{ij}$，若 $p_{ij}=0$，则定义 $\lim\limits_{p_{ij}\to 0}p_{ij}\ln p_{ij}=0$。

最后由上一步计算出的各个指标的信息熵 $E_1,E_2,\cdots,E_k$ 可以得出各指标权重：

$$W_j=\frac{1-E_j}{k-\sum_{j=1}^{k}E_j} \tag{3}$$

其中，k 为指标的个数，E_j 为第 j 个指标的信息熵。

在信用评价模型中引入孤立森林作为异常检测方法，以解决网络中拜占庭节点的问题。孤立森林算法可用来挖掘异常数据，在大量数据中，随机选取维度，递归分割数据集，找出与其他数据规律不符合的数据，直到所有的样本点都是孤立的。在这种随机分割的策略下，异常点在树中具有较短的路径。

主节点根据节点信用度评估标准表的状态数据集得出各指标的权重，并执行孤立森林异常检测算法对预处理后的数据进行训练。首先构建一棵孤立树，其训练过程如图 3 所示，具体步骤如下：

步骤 1　从所有节点的信用度数据集中随机选择 Ψ 个点作为子样本，放入一棵孤立树的根节点。

步骤 2　随机选择一个维度和分割值 p，分割值产生于该维度数据中的最大值和最小值之间。

步骤 3　以此分割值生成一个超平面，数据被切分成两个部分，将值小于 p 的数据放在当前节点的左分支上，将值大于 p 的放在当前节点的右分支上。

步骤 4　在当前节点左分支和右分支的节点中递归地进行步骤 1 和步骤 2，不断构造新的叶子节点，直到树达到限制高度，或者叶子节点上只剩下一个数据（无法继续分割）。

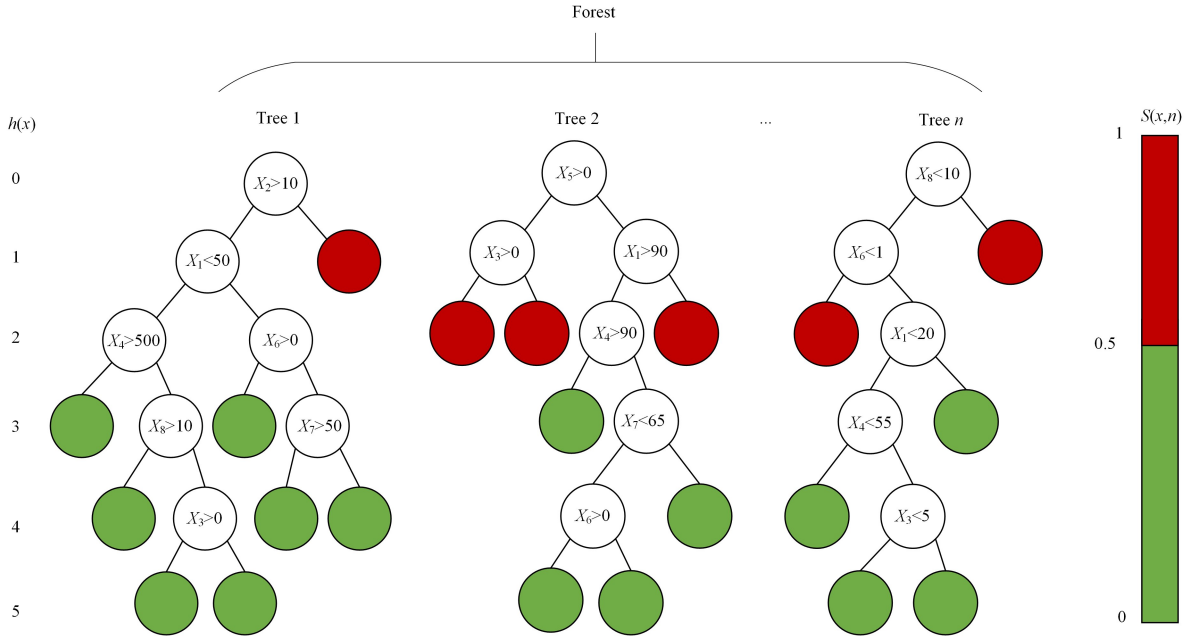

图 3　孤立森林训练过程

Fig. 3　Isolation forest training process

整个算法分为训练和预测两个步骤，通过随机采样节点信用度评估标准表的数据对每一棵树进行训练，建立 t 棵孤立树，t 棵孤立的树组成孤立森林；再将每个测试数据 x 在每一棵孤立的树上沿着分支往下走，直到达到叶子节点，并记录所经过的路径长度 $h(x)$，通过异常函数 $s(x,n)$ 来判断并记录 x 是否为异常节点。

$$s(x,n)=2^{-\frac{E(h(x))}{c(n)}} \tag{4}$$

其中，$h(x)$ 表示数据 x 的路径长度，为数据 x 从子树的根节点到叶子节点所经过的边的数量；$E(h(x))$ 为 x 在多棵树中的路径长度的期望值；$c(n)$ 为一个包含 n 个样本的数据集，表示树的平均路径长度。

$$c(n)=2H(n-1)-\left(\frac{2(n-1)}{n}\right) \tag{5}$$

其中，$H(*)=\ln *+\xi$ 为调和函数，$H(*)$ 为调和数，ξ 为欧拉常数，约为 0.577 215 664 9。

由式(5)可得：

(1)当 $E(h(x))\to c(n)$ 时，即数据 x 在多棵孤立树中路径长度的期望值 $E(h(x))$ 与树的平均路径长度 $c(n)$ 相近时，$s\to 0.5$，此时不能区分是否异常。

(2)当 $E(h(x))\to 0$ 时，即数据 x 在多棵孤立的树中路径长度的期望值 $E(h(x))$ 越短，异常分数越接近 1，$s\to 1$，判定为异常。

(3)当 $E(h(x))\to n-1$ 时，即数据 x 在多棵孤立的树中路径长度的期望值 $E(h(x))$ 越长，异常分数越接近 0，$s\to 0$，判定为正常。

主节点发送信用评估请求后，每个节点向主节点发送自己的信用度评估标准数据表，主节点接收到其他节点的状态数据后，计算出来节点信用度评估标准表中的每个指标权重，并把每个节点状态数据表作为孤立森林异常检测算法的输入，执行诚实节点编号表生成算法，输出一个具有诚实节点编号的表。由于系统中存在拜占庭节点，因此会出现主节点恰好为拜占庭节点的情况。若拜占庭节点当选主节点后会恶意更改诚实节点编号表，此时需要进行多轮主节点的选举，生成多轮诚实节点编号表并广播。设系统中拜占庭节点数为 f，不超过节点总数的 1/3，则当参与共识的节点收到 $f+1$ 次相同的诚实节点编号表，即可得到正确的诚实节点编号表。具体算法如算法 1 所示。

算法 1 诚实节点编号表生成算法

```
Input:(n,c1,c2,…,cn)
Output:Honest_Table
c1,c2,…,cn:n 个节点的信用度评估数据值
Si:第 i 轮的主节点
1. While i≤n do
2. {
3.   Si根据c1,c2…cn数据执行信用评价模型
4.     Si广播生成的诚实节点编号表honest_tablei
5.   if count(honest_tablei)≥ f+1 then
6.   {
7.     Honest_Table ←honest_tablei
8.     break
9.   }
10.    else
11.      i++
12.}
```

在构建信用评价模型阶段，基于信用评估标准表，引入孤立森林异常检测算法对节点数据进行训练，构建出信用评价模型。在车联网中，主节点利用该模型可以检测出拜占庭车辆节点，并输出诚实车辆节点编号表 Honest_Table，所有诚实节点将共同维护此表，并参与共识过程。在领导者选举阶段，使投票节点能分辨出恶意节点并让其无法当选领导者；在日志复制阶段，领导者只需要给诚实节点编号表中的节点发送追加日志请求，使车联网系统在车辆共识过程中能够排除恶意节点，即可达到车辆间数据安全共享的目的。

3.2.2 领导者选举阶段

CE-Raft 算法与 Raft 算法一样有领导者 Leader、候选者 Candidate、跟随者 Follower 这 3 个角色。领导者节点处理客户端的请求；候选者节点选举成为领导者节点；与原算法不同的是，跟随者节点不是无条件向领导者投票，它在领导者节点发出投票请求时会对比诚实节点编号表并决定自己的投票权。3 个角色的转换过程如图 4 所示。

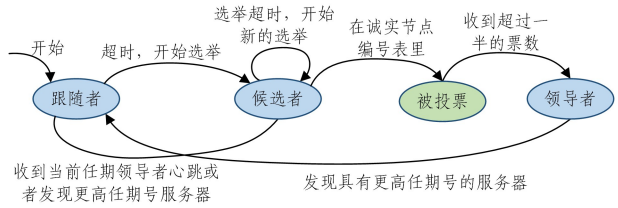

图 4 角色转换图

Fig. 4 Role transition diagram

本文算法在时间分割上与原 Raft 相同，领导者选举的过程由心跳机制触发，选举超时时间在一个固定的区间(150～300 ms)中随机选择，把整个算法的时间分为多个任意长度的任期 term，任期用连续的整数标记。一段任期分为领导者选举阶段和领导者任期阶段。

当服务器启动时，所有节点都是跟随者节点状态，节点之间使用 RPC 进行通信，若跟随者节点在自身的计时器超时后还没有接收到候选者节点的投票请求或者领导者发送的心跳检测，则首先增加自己当前的任期号并将自己从跟随者状态转换为候选者状态，再投票给自己且并行地向其他服务器节点发出投票请求 RequestVoteRPC。其他跟随者节点收到候选者的 RequestVoteRPC 后，首先对比自己与候选者节点的日志信息，如果候选者节点存储的日志信息最后一条的索引值和任期号小于本地最后一条日志，则会拒绝该投票请求。然后查看此候选者节点是否在诚实节点编号表 Honest_Table 中，若不在，则同样拒绝该投票请求。在等待投票期间，如果候选者节点接收到领导者发出的 AppendEntries RPC 请求或心跳检测，并且自身任期号小于该领导者任期号，则会确认该领导者的地位并返回跟随者状态。如果候选者接受了超过一半节点的投票，就把自己转换为领导者状态，并立即向其服务器节点发出心跳检测，来广播自身的领导地位和防止新一轮的投票产生。

3.2.3 日志复制阶段

在 CE-Raft 算法中的日志的组织方式如图 5 所示，每个日志条目存储两个属性，一个日志信息和一个收到该指令信息时领导者的任期号。每个日志信息中包含一条让复制状态机执行的指令，任期号用来检查领导者发出的日志条目是否是最新的，日志条目上方的整数序列表示每个日志条目在日志中的索引值。

算法严格限制日志提交的顺序，领导者节点接收到来自客户端的请求后，首先将客户端发来的指令封装为日志项并追加到自己的日志条目中，保存到本地日志中，随后将发起日志复制请求 AppendEntries RPC 给在 Honest_Table 中的跟随者服务器，让它们复制并同步该日志条目。若 AppendEntries RPC 中日志条目为空，则是领导者节点为了说明自己的领导者地位发送的心跳检测；若不为空，跟随者节点将对比日志条目的任期号和索引号，若其在自身的日志中找到包含相同任期值和索引号的条目，将同意追加该新的日志条目，然后

向领导者节点回复追加该日志成功，否则回复追加失败。当领导者收到超过一半的跟随者追加成功的消息，即日志复制到了过半的服务器上，便可提交该日志条目到状态机，并向客户端回复操作成功，且该日志条目之前的日志条目都是被提交状态，其中也可能包含其他领导者创建的条目。

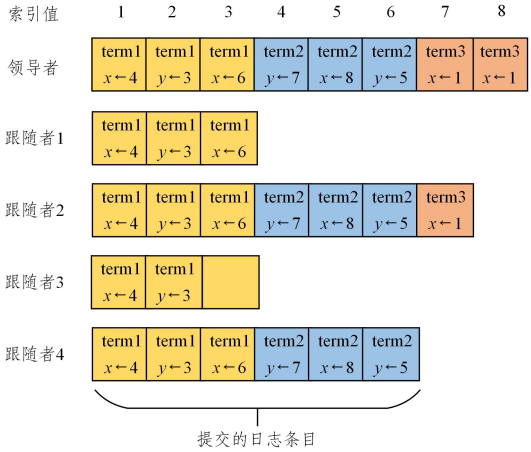

图 5　日志组织方式

Fig. 5　Log organization

如图 5 所示，跟随者节点 3 在复制索引值为 3 的日志条目时宕机，在索引值为 4 时又恢复正常，并收到领导者节点发送的 AppendEntries RPC 请求，其中包括索引位置 4 和任期号 2 的日志条目，若该跟随者发现在自己的日志中找不到相同索引位置和任期号的日志条目，就会拒绝此请求。领导者节点在每次被拒绝后，都会减小一个索引位置的日志条目重试 AppendEntries RPC 请求，直到最终与跟随者节点日志达成一致，即当领导者发送索引位置为 2、任期号为 1 的 AppendEntries RPC 请求时，跟随者节点 3 才接受请求，然后领导者将跟随者节点此日志条目之后的日志条目与自己保持一致。

4　实验分析

4.1　实验环境

实验环境系统采用 Windows10，内存 32 GB，Intel I7-9400F CPU，使用开发版本 V1.15.3 的 Go 语言实现 CE-RAFT 算法和 PBFT 算法的共识过程，完成共识仿真模拟实验。每个节点对应不同端口号，多线程模拟区块链节点进行共识仿真实验。实验结果使用 Matlab 进行处理和分析。

4.2　信用评价模型预测准确率分析

拜占庭节点预测准确率指 CE-Raft 算法中信用评价模型可以排除的拜占庭节点数量占系统中拜占庭节点总数量的比值。诚实节点预测准确率指 CE-Raft 算法中信用评价模型预测得出的诚实节点数量占系统中诚实节点总数量的比值。

本实验用 Go 语言模拟实现区块链通信过程，从中采集需要的节点数据状态信息作为信用评价模型的训练集，将信用评价模型 $n\_estimators$ 变量（孤立森林中树的数量）设置为 10000 进行训练测试，以 200～2000 个节点数量的状态数据作为信用模型的训练集，以 100 个节点的数据作为测试集，其中包含 95 个诚实节点和 5 个拜占庭节点。取 10 次评估的平均值，结果如图 6 所示，拜占庭节点预测准确率稳定在 100%。但考虑到可能会出现诚实节点被误分为拜占庭节点的情况，我们对诚实节点的准确率也做了测试。从图中可以看出，当训练样本数为 200 时，诚实节点预测准确率为 92.32%，此时诚实节点误分率较大，但随着训练样本数的增加，诚实节点预测准确率逐渐提高，稳定在 99%左右。这是因为孤立森林是一种适用于连续数据的无监督异常检测方法，其递归地随机分割数据集。总数据量越多，训练集越大，孤立森林孤立异常点的能力越强，检测的准确率就越高。由于 CE-Raft 算法共识阶段需要一个完全可信的网络模型，因此需要将拜占庭节点全部检测出来，即使会有一定误分率导致某些诚实节点没有参与共识，但只要共识阶段没有拜占庭节点存在就可以达成最终的共识，从而保证车联网数据能够安全地共享。

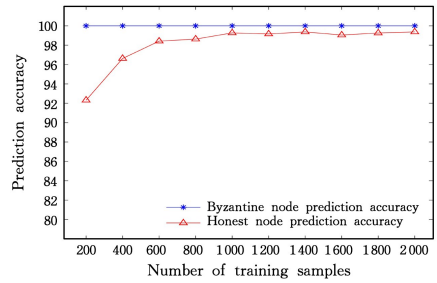

图 6　信用评价模型预测准确率

Fig. 6　Prediction accuracy of credit evaluation model

图 7 给出了 CE-Raft 算法与 CRaft 算法[24]提出的信用模型诚实节点预测准确率的对比，可以看出本文提出的信用评价模型诚实节点准确率在 90%～100%之间。在训练样本数相同的情况下，本文提出的信用评价模型对诚实节点的预测准确率高于 CRaft 算法，即本文模型将诚实节点误分为拜占庭节点的概率更小。

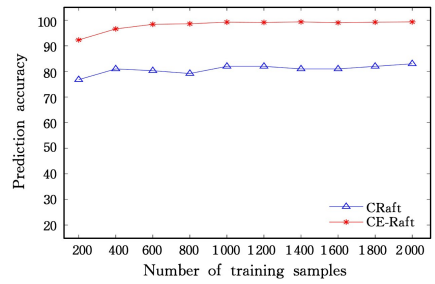

图 7　诚实节点准确率对比

Fig. 7　Accuracy comparison of honest nodes

4.3　时延分析

本文提出的 CE-Raft 算法在 Raft 算法的基础上进行改进，具有了容错能力，而 PBFT 算法是基于拜占庭容错的一致性算法，是车联网与联盟链中常用的共识算法。PBFT 算法和 Raft 算法都是主节点与客户端交互，从节点与主节点交互，从而达成一致，因此，将本文提出的 CE-Raft 算法与 PBFT 算法在性能上进行实验对比分析。

时延指单笔交易从发送到提交达成共识所需要的时间。图 8 给出了 PBFT 算法与 CE-Raft 算法的时延对比。从图中

可看出，本文提出的 CE-Raft 算法比 PBFT 算法时延更低，随着节点数量的增加，PBFT 算法的时延急剧增加，且节点数量越多时延差距越大。这是由于在 PBFT 算法中，每个节点都要从其他节点中接受请求，通信次数为 $2n(n-1)$，时间复杂度为 $O(n^2)$，而 CE-Raft 算法只需要主节点接收超过一半的投票就可达成共识，其他节点之间无须沟通，在日志复制阶段通信次数为 $2(n-1)$，时间复杂度为 $O(n)$。

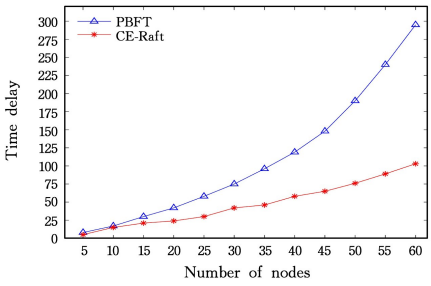

图 8 时延对比

Fig. 8 Latency comparison

4.4 吞吐量分析

吞吐量指在一段时间内节点之间达成共识处理的交易数量，计算公式为：

$$TPS=\frac{num}{t} \tag{6}$$

其中，num 为达成共识所需的这段时间能够处理的交易数量，t 为达成共识需要的时间。

实验结果如图 9 所示，图中给出了在有 5～60 个节点的情况下两种算法的吞吐量对比。可以看出 CE-Raft 算法的吞吐量优于 PBFT，且当节点增加到 30 个后，PBFT 算法的吞吐量迅速下降，而 CE-Raft 算法的吞吐量呈线性下降。这是由于节点增多后，PBFT 算法在传输消息时，每个节点之间的沟通变多，达成共识的时间变长，导致吞吐量急剧下降，而 CE-Raft 算法一直都是领导者给每个跟随者传输消息，不需要节点之间互相传递消息，因此随着节点数量的增多，吞吐量逐渐地降低。相比 PBFT 算法，CE-Raft 算法能使车辆之间更加高效地共享数据。

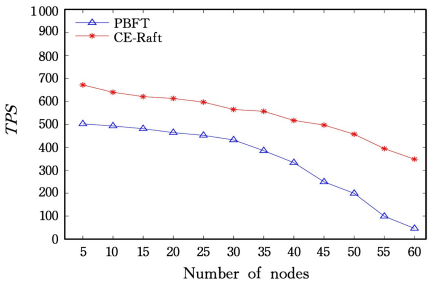

图 9 吞吐量对比

Fig. 9 Throughput comparison

综上所述，对不同共识算法在检测拜占庭节点、预测准确率、时间复杂度等方面进行对比，结果如表 2 所列。本文提出的 CE-Raft 算法相比 Raft 算法能够检测出拜占庭节点，相比 CRaft 算法具有更高的诚实节点预测准确率，相比 PBFT 算法时间复杂度更低，性能更优。

表 2 共识算法对比

Table 2 Consensus algorithm comparison

共识算法	是否能检测出拜占庭节点	信用模型诚实节点预测准确率	性能	时间复杂度
CE-Raft	是	高	优	$O(n)$
CRaft	是	较高	优	$O(n)$
Raft	否	—	优	$O(n)$
PBFT	是	—	良	$O(n^2)$

结束语 针对车联网网络中存在拜占庭车辆节点导致各车辆节点之间的消息难以高效安全地共享和达成共识的问题，本文提出了一种基于孤立森林异常检测算法构建信用评价模型的 CE-Raft 共识算法。CE-Raft 算法首先通过信用评价模型检测出拜占庭节点，使其不能当选领导者，随后再进行消息同步，使车联网中诚实车辆节点之间传送的消息达成一致。实验结果表明，CE-Raft 算法能够有效排除拜占庭节点，提高了诚实节点预测准确率，具有较低的时延和较高的吞吐量，满足了车联网中数据安全高效共享的需求。但本文提出的 CE-Raft 算法在领导者选举阶段会出现投票分裂的情况，浪费选举时间，在时间效率上仍有进一步提升的空间。在接下来的研究工作中可以改进领导者选举阶段投票机制，缩短选举时间，进一步提高算法效率。

参 考 文 献

[1] LI X H, ZHONG C, CHEN Y, et al. Overview of Internet of Vehicles Security [J]. Journal of Information Security, 2019, 4(3): 17-33.

[2] CHENG G, GUO D. Research on the current situation and development of the Internet of Vehicles [J]. Mobile Communication, 2011, 35(17): 23-26.

[3] HUANG Z Z, ZHANG X D, ZHAO J H. Design of Knowledge Sharing Mechanism Based on Blockchain [J]. Journal of Chongqing University of Technology (Natural Sciences), 2021, 35(9): 143-151.

[4] YUAN Y, WANG F Y. Development Status and Prospect of Blockchain Technology [J]. Acta Automatica Sinica, 2016, 42(4): 481-494.

[5] ZHANG L, LUO M, LI J, et al. Blockchain based secure data sharing system for Internet of vehicles: A position paper[J]. Vehicular Communications, 2019, 16: 85-93.

[6] KANG J, XIONG Z, NIYATO D, et al. Toward secure blockchain-enabled internet of vehicles: Optimizing consensus management using reputation and contract theory[J]. IEEE Transactions on Vehicular Technology, 2019, 68(3): 2906-2920.

[7] LI Z J, ZHANG G A, CHEN W W. Security Communication Strategy of Internet of Vehicles Based on Blockchain[J]. Computer Engineering, 2021, 47(10): 43-51.

[8] CHEN W W, CAO L, SHAO C H. An efficient anonymous authentication scheme for the Internet of Vehicles based on blockchain technology [J]. Computer Applications, 2020, 40(10): 2992-2999.

[9] HASROUNY H, SAMHAT A E, BASSIL C, et al. VANet security challenges and solutions: A survey[J]. Vehicular Commu-

nications，2017，7：7-20.

[10] PARKINSON S，WARD P，WILSON K，et al. Cyber threats facing autonomous and connected vehicles：Future challenges[J]. IEEE Transactions on Intelligent Transportation Systems，2017，18(11)：2898-2915.

[11] ZHANG Y，ZHANG K，CAO J Y. Internet of Vehicles Driven by Edge Intelligence [J]. Journal of the Internet of Things，2018，2(4)：40-48.

[12] CHOWDHURY M，GAWANDE A，WANG L. Secure information sharing among autonomous vehicles in NDN[C]// 2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation(IoTDI). IEEE，2017：15-26.

[13] LIU F，WANG Y F，YANG J，et al. A High-Threshold Signature Protocol Integrating DKG and BLS Based on Blockchain [J]. Computer Science，2021，48(11)：46-53.

[14] HUANG D. Electronic Evidence Authentication and Encryption Scheme Combining Blockchain and ring Signature [J]. Journal of Chongqing University of Posts and Telecommunications(Natural Science Edition)，2022，34(1)：16-23.

[15] ZHU X M，LIU B，BAI X，et al. Research on Wireless Blockchain Security of CSMA/CA Network Protocol [J]. Journal of Chongqing University of Posts and Telecommunications(Natural Science Edition)，2022，34(1)：6-15.

[16] XIONG X，LI L X，GAO J，et al. Research progress of blockchain in the field of Internet of Vehicles data sharing[J]. Computer Science and Exploration，2022，16(5)：1008-1024.

[17] ZHONG Z S. An Improved PoS Consensus Algorithm Based on Blockchain [J]. Journal of Chongqing Technology and Business University(Natural Science Edition)，2021，38(4)：36-41.

[18] LIU F，YANG J，LI Z B，et al. A Secure Multi-Party Computation Protocol Based on Blockchain for Universal Data Privacy Protection [J]. Computer Research and Development，2021，58(2)：281-290.

[19] GE L，JI X S，JIANG T，et al. IoT information sharing security mechanism based on blockchain technology [J]. Computer Applications，2019，39(2)：458-463.

[20] WANG Z，LI T，WANG H，et al. {CRaft}：An Erasure-coding-supported Version of Raft for Reducing Storage Cost and Network Cost[C]// 18th USENIX Conference on File and Storage Technologies(FAST 20). 2020：297-308.

[21] TAN D，HU J，WANG J. VBBFT-Raft：an understandable blockchain consensus protocol with high performance[C]// 2019 IEEE 7th International Conference on Computer Science and Network Technology(ICCSNT). IEEE，2019：111-115.

[22] WANG R，ZHANG L，ZHOU H，et al. A byzantine fault tolerance raft algorithm combines with BLS signature[J]. Journal of Applied Sciences，2020，38(1)：93-104.

[23] TIAN S，LIU Y，ZHANG Y，et al. A Byzantine Fault-Tolerant Raft Algorithm Combined with Schnorr Signature[C]// 2021 15th International Conference on Ubiquitous Information Management and Communication(IMCOM). IEEE，2021：1-5.

[24] CHEN Y，LIU P，ZHANG W. Raft consensus algorithm based on credit model in consortium blockchain[J]. Wuhan University Journal of Natural Sciences，2020，25(2)：146-154.

[25] ZHOU S，YING B. VG-Raft：An Improved Byzantine Fault Tolerant Algorithm Based on Raft Algorithm[C]// 2021 IEEE 21st International Conference on Communication Technology (ICCT). IEEE，2021：882-886.

[26] WANG L，BAI Y，JIANG Q，et al. Beh-Raft-Chain：A behavior-based fast blockchain protocol for complex networks[J]. IEEE Transactions on Network Science and Engineering，2020，8(2)：1154-1166.

[27] HUANG D Y，LI L，CHEN B，et al. RBFT：Byzantine Fault Tolerant Consensus Mechanism Based on Raft Cluster [J]. Journal of Communications，2021，42(3)：209-219.

[28] GAO W，MU W，HUANG S，et al. Improved Byzantine Fault-Tolerant Algorithm Based on Alliance Chain[J]. Wireless Communications and Mobile Computing，2021，2021：1-10.

LIU Wei，born in 1981，Ph.D，associate professor，is a member of China Computer Federation. His main research interests include blockchain，wireless mesh work and information security.

TIAN Zhao，born in 1985，Ph.D，lecturer. His main research interests include information security，blockchain and intelligent transportation.

（责任编辑：何杨）