车联网中基于区块链的分布式信任管理方案

张海波，曹钰坤，刘开健，王汝言

（1. 重庆邮电大学通信与信息工程学院，重庆 400065；2. 先进网络与智能互联技术重庆市高校重点实验室，重庆 400065；
3. 泛在感知与互联重庆市重点实验室，重庆 400065）

摘 要：针对车联网中恶意车辆识别效率低、识别准确率低带来的安全问题，提出了一种基于区块链的分布式车联网信任管理方案。通过聚合车辆的评分信息，结合贝叶斯推理模型设计了一种虚假信息识别策略。联合车辆历史交互信息以及交通事件信息设计了一种声誉值更新算法，并利用声誉阈值识别恶意车辆。通过路边单元构建区块链，实现了交通数据以及车辆声誉值的分布式存储。改进了传统的工作量证明共识机制，通过事件等级与参与评分车辆数量动态改变矿工节点的出块难度，并利用等待机制使近期出块的节点暂时停止参与矿工节点的选举过程，从而减少重复计算带来的资源消耗。仿真结果表明，所提方案能够有效识别虚假信息，抵御恶意车辆的欺骗行为，提升恶意车辆的识别效率，减少资源消耗，在车联网的分布式信任管理方面是有效可行的。

关键词：车联网；区块链；信任管理；声誉值；共识机制

中图分类号：TN92

文献标志码：A

DOI: 10.11959/j.issn.1000−436x.2023097

Distributed trust management scheme based on blockchain in Internet of vehicles

ZHANG Haibo, CAO Yukun, LIU Kaijian, WANG Ruyan

1. School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China
2. Advanced Network and Intelligent Connection Technology Key Laboratory of Chongqing Education Commission of China, Chongqing 400065, China
3. Key Laboratory of Ubiquitous Sensing and Networking in Chongqing, Chongqing 400065, China

Abstract: Aiming at the security problems caused by the low efficiency and accuracy of malicious vehicle identification in Internet of vehicles, a distributed trust management scheme based on blockchain in Internet of vehicles was proposed. A false information identification strategy was designed by aggregating the scoring information of vehicles, combined with Bayesian inference model. A reputation value updating algorithm was designed by combining the historical interaction information of vehicles and traffic information, malicious vehicles were identified by the reputation threshold. A blockchain was constructed roadside units to realize the distributed storage of traffic data and vehicle reputation values. The traditional proof of work consensus mechanism was improved to dynamically change the difficulty of miner node generating a block through the event level and the number of vehicles involved in scoring, and the waiting mechanism was used to temporarily stop the nodes that had recently blocked from participating in the election process of miner nodes, thus reducing the resource consumption caused by repeated calculations. The simulation results show that the proposed scheme can effectively identify false information, resist the deceptive behavior of malicious vehicles, improve the identification efficiency of malicious vehicles, reduce resource consumption, and is effective and feasible in distributed trust management for Internet of vehicles.

Keywords: Internet of vehicles, blockchain, trust management, reputation value, consensus mechanism

收稿日期：2022−11−01；**修回日期：**2023−01−04

基金项目：国家自然科学基金资助项目（No.61901071，No.62271094）；长江学者和创新团队发展计划基金资助项目（No.IRT16R72）；重庆市留创计划创新类基金资助项目（No.cx2020059）

Foundation Items: The National Natural Science Foundation of China (No.61901071, No.62271094), The Program for Changjiang Scholars and Innovative Research Team in University (No.IRT16R72), Chongqing Innovation and Entrepreneurship Program for the Returned Overseas Chinese Scholars (No.cx2020059)

0　引言

近年来，随着汽车保有量的急剧上升，交通运输系统面临严峻考验。车联网成为解决上述问题的有效途径[1]，在 5G 等新一代通信技术的支持下，车辆通过智能车载单元（OBU, on board unit）等传感设备来感知周围环境，同时使用通信模块与路边单元（RSU, roadside unit）或附近车辆进行通信[2]，实时获取周边道路和交通信息，并利用人工智能或自动驾驶技术智能规划最佳路线，从而提升交通效率和道路安全性[3]。由于车联网节点数量众多、分布范围广，且具有动态性，车辆收到的信息通常来自陌生车辆，其中可能存在部分恶意车辆，恶意车辆通过故意广播虚假消息的方式来扰乱其他车辆的正常行驶[4-5]，甚至造成严重的交通事故。因此，快速准确地识别虚假信息和恶意车辆成为保障车联网信息安全的重要研究内容。

许多研究提出信任管理是解决车联网信任问题的有效方式[6]。信任管理可以实现车联网信息的可信度计算，进而提高车辆判断事件的准确性，它还可以分配、计算和更新车辆的声誉值，有效解决车联网中存在虚假信息和恶意车辆的问题[7-8]。部分研究提出的信任管理方案以中央服务器为数据载体[9]，所有的声誉值、信任评分等数据都在中央服务器中存储和处理。由于车辆的动态性，服务器可能很难满足车辆对时延的要求，并且中央服务器可能存在单点故障等问题[10]。为了克服这些难题，部分学者提出使用如 RSU、基站等多个流量服务器对数据进行分布式存储和处理[11-12]，然而，由于 RSU 等设备可能存在故障或被入侵，其可靠性和信任服务方面仍存在挑战。

区块链技术[13]的兴起为车联网数据的分布式存储和管理带来了新的方向[14]，区块链中保存的数据具有高度的安全性与不可篡改性，使用区块链作为数据存储的载体能够改善车联网的数据安全问题。Yang 等[15]提出了一种基于区块链技术的数据可信度评估信誉系统，车辆通过观察交通环境对接收到的消息进行评级，将评级信息保存至车辆维护的区块链中，并以此作为更新车辆声誉值的凭证。但由于车辆存在计算效率低、数据存储空间不足等情况，无法保证区块链的稳定运行，且不同车辆之间的计算能力存在差异，更先进的车辆更容易成为矿工节点。Kang 等[16]提出了一种基于声誉值的数据共享方案，基于边缘节点设备建立了一个联盟链用于存储车辆的感知数据，相比于车辆作为全节点的方案更加可靠。Lu 等[17]提出了一种基于区块链的匿名声誉系统，使用关于车辆的直接历史交互信息和其他车辆的间接意见作为车辆声誉值的证据，并设计了三条区块链分别用来存储车辆证书信息、已注销公钥信息和网络中的广播信息。Yang 等[18]使用 RSU 构建区块链来存储车辆的声誉值变化量信息，并利用工作量证明（PoW, proof of work）机制与权益证明（PoS, proof of stake）机制组合的共识机制进行共识，优先添加包含最大声誉值变化量的块到区块链中。Zhang 等[19]提出了一种信誉值更新算法，包括消息可信度计算、评级机制和基于评级的信誉值计算，并通过 RSU 构建区块链，将声誉值和评级信息存入区块链中，同样采取了 PoW 与 PoS 结合的共识机制。但是该共识机制在运行过程中会浪费大量计算资源，在交通事件频发的环境下，容易出现单个节点持续出块的情况，增大了矿工节点的计算压力和被入侵的风险。

综合上述讨论，许多学者将区块链技术应用于车联网信任管理系统中，实现了车联网信息的分布式存储，但是在构建区块链时，选取车辆作为区块链的全节点，并未考虑到车辆的计算能力和存储能力，部分研究中提出的共识机制会产生大量的计算开销，并且矿工节点的选取随机性不强。在验证车联网信息正确性时，大部分方案忽略了除声誉值以外的其他因素对车辆信息可信度的影响，在车联网中可能存在通过正常运作获取高声誉值的恶意车辆，所以仅依靠声誉值作为判断标准是不完全可靠的。为了解决上述问题，本文基于区块链存储技术建立了一种分布式的车联网信任管理方案，主要工作如下。

1) 构建了一个车联网场景下的信任管理方案，并使用区块链存储交通事件信息与车辆声誉值信息；提出了一种车联网虚假信息识别策略，联合声誉值、地理位置以及发送信息耗费的时间作为评估事件信息可信度的指标，利用贝叶斯推理模型判定事件信息真实性，从而准确识别虚假信息。

2) 设计了一种车辆声誉值更新算法，根据车辆历史行为设置惩罚轮次，以此来限制车辆在恶意行

为后的声誉值的大小和恢复速度，利用事件等级设定声誉值的更新比重，最后通过声誉阈值来识别恶意车辆。

3) 针对传统 PoW 共识机制效率低、资源浪费等问题，根据车联网的实际应用需求，提出了哈希门限值更新机制和等待机制。改进后的共识机制根据 RSU 创建的历史区块的时间、事件的等级以及车辆的评分活跃程度来更新 RSU 的哈希门限值，并使近期出块的 RSU 暂时停止参与矿工选举过程，在保证网络公平性的同时，减少计算资源的消耗，确保对车辆声誉值影响更大、影响范围更广的区块优先加入区块链中，从而提升车辆声誉值数据的更新效率以及恶意车辆的识别效率。

1 问题建立

1.1 系统模型

本文设计的车联网信任管理方案模型如图 1 所示，主要由四部分组成，包括车辆、RSU、区块链和监管部门（LEA, law enforcement agency）。

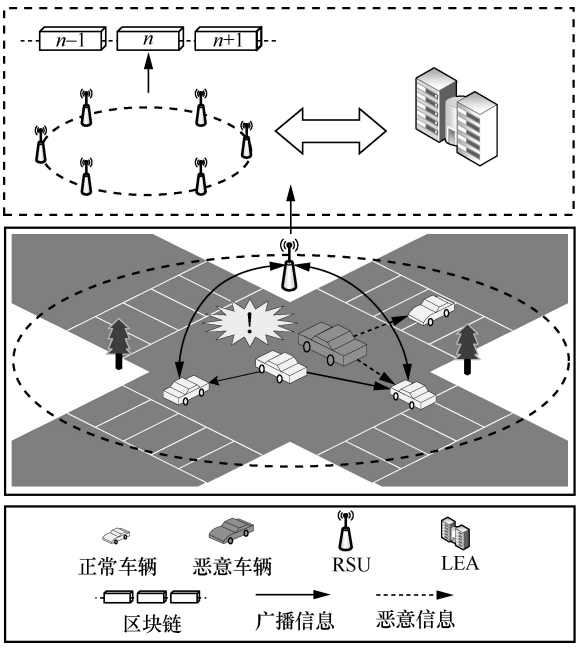


图 1 车联网信任管理方案模型

1) 车辆配备了基本的计算模块、OBU 以及感知模块，能够自动感知周围环境，对交通事件、环境条件等进行检测，并通过 OBU 通信模块将检测到的数据发送给周围的车辆[10]。信息的接收方需要对接收到的交通事件信息进行评分，最后将评分的结果上传到附近的 RSU 中。

2) RSU 拥有较强的计算能力和存储能力，担任区块链中的矿工节点，负责维护区块链、收集车辆发送的评分信息、更新本地车辆声誉值等任务，RSU 可以通过向 LEA 发送访问信息来获取指定车辆的声誉值等信息。

3) 区块链通过 RSU 维护，用于存储网络中车辆的声誉值、车辆之间的交互信息以及交通事件信息。

4) LEA 属于完全可信的机构，负责管理网络中的车辆信息。LEA 通过访问区块链来更新全局声誉值信息。

1.2 交通事件分类

本文将交通事件分为 3 个等级，通过事件等级对车辆进行不同程度的奖惩，从而抑制恶意车辆的非法行为。

1) 一级事件为普通交通事件，例如，交通拥堵、路线检修等危险程度较低的事件。

2) 二级事件为道路异常预警，例如，车辆检测到其覆盖范围内存在深坑、结冰等道路异常状况。

3) 三级事件为车辆紧急信息，例如，车辆在运行中出现紧急情况或交通事故等紧急事件。

1.3 攻击模型

在车联网系统中，车辆以及 RSU 都有可能受到恶意攻击，这些攻击可能对系统的安全性和正常运行产生负面影响。本文方案主要考虑两方面的攻击，分别是恶意车辆以及受到攻击的 RSU。

1.3.1 恶意车辆

车联网中可能会出现部分恶意车辆，它们会出于某种目的去扰乱系统的正常运行。这些恶意车辆存在三类攻击，分别如下。

1) 广播虚假信息。恶意车辆会故意广播虚假信息从而扰乱其他车辆的正常运行，影响交通安全和效率。

2) 恶意评分。在其他车辆广播交通事件信息时，恶意车辆通过恶意评分，影响 RSU 和其他用户对事件信息真实性的判断。

3) 延迟发送信息。恶意车辆在遇到交通事件或者需要参与评分时，通过故意延长信息发送的时间，降低整体系统的工作效率。

1.3.2 受到攻击的 RSU

由于 RSU 分布广，数量多，有时不能及时得到维护，可能受到攻击者的入侵，但由于攻击者的能力有限且入侵时间是短暂的，因此可以认为网络中的大部分 RSU 长时间处于正常工作状态。

2　方案设计

2.1　方案流程

本文设计的信任管理方案流程如图 2 所示，具体包括以下步骤：①车辆广播交通事件信息；②收到广播信息的车辆进行评分并上传至 RSU；③RSU 判定事件信息的真实性；④对本地车辆声誉值进行更新；⑤RSU 进行共识并上传区块至区块链；⑥LEA 通过区块链更新全局声誉值。

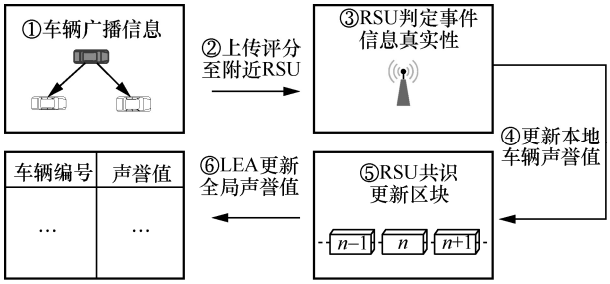


图 2　信任管理方案流程

2.2　车辆评分的产生

车辆 i 遇到交通事件，通过车载传感器设备感知事件，并立即通过通信模块向附近的车辆集群广播信息。系统中所有广播的交通事件信息构成的集合记为 $E=\{e_1,e_2,\cdots,e_j\},\cdots,e_J$。

接收到车辆 i 的广播信息的车辆群体可以对信息进行信任评分 $\{1,-1\}$，信任评分表示车辆对广播信息的意见，“1”表示认同广播信息，“–1”表示反对广播信息。评分完成后车辆将结果转发给附近的 RSU 进行判定，为了更加准确地判定广播的事件信息的真实性，需要结合车辆的评分可信度。可信度主要来源于以下几个方面。

1) 评分车辆与事件发生地点的距离

车辆 k 在发送其对某一事件的评分时，会将自身运行位置以及运行状态发送给 RSU，通过计算事件发生地点与车辆所处位置的距离来决定其评分的可信度，即

$$d_k^j=\mathrm{e}^{-\omega_1\mathrm{dis}_k^j} \tag{1}$$

其中，d_k^j 表示评分车辆与事件 e_j 发生地点的距离对评分可信度的影响值。dis_k^j 表示评分车辆 k 与事件 e_j 发生地点之间的距离，ω_1 表示距离参数的变化率。

2) 评分车辆的声誉值

车辆的声誉值决定了车辆的可信程度，车辆广播信息的可信程度以及评分的可信度与声誉值呈正相关。

$$r_k^j=\frac{r_k}{r_{\max}} \tag{2}$$

其中，r_k^j 表示声誉值对评分可信度的影响值；r_k 表示车辆 k 当前的声誉值，且 $r_k\in[0,1]$；$r_{\max}$ 表示所有参与评分车辆中声誉值的最大值。

3) 评分所花费的时间

车辆对某一事件评分所花费的时间反映了车辆在网络中的积极程度，一般情况下，正常车辆在网络中的行为都是积极且正确的，因此车辆各项操作所花费的时间也是决定其评分可信度的关键因素之一。

$$\tau_k^j=\frac{1}{t-t_k^j} \tag{3}$$

其中，τ_k^j 表示评分花费时间对评分可信度的影响值，t 表示车辆 k 发送评分信息的时间，t_k^j 表示车辆 k 收到事件 e_j 的时间。

最后，通过加权求和的方式获得车辆 k 对事件 e_j 的评分可信度为

$$c_k^j=\omega_2 d_k^j+\omega_3 r_k^j+\omega_4\tau_k^j \tag{4}$$

其中，ω_2、ω_3 和 ω_4 用于控制上述 3 个因素对车辆评分可信度的影响，并且满足

$$\omega_2+\omega_3+\omega_4=1 \tag{5}$$

考虑到声誉值为证明车辆身份的唯一重要信息，车联网广播信息的可信程度总体与信息发送者的声誉值呈正相关，声誉值对于验证车辆评分可信度的重要程度是大于其他 2 种因素的，因此 ω_2、ω_3 和 ω_4 应满足 $\omega_3>\omega_2$ 和 $\omega_3>\omega_4$，为了保证 d_k^j 和 τ_k^j 能够有效地对评分可信度产生影响，在后续的仿真过程中设 $\omega_2=\omega_4$。

2.3　判定事件信息真实性

车辆将评分上传至 RSU 后，RSU 对事件信息的真实性进行判定，RSU 获取所有车辆的评分可信度信息，构成集合 $C_j=\{c_1^j,c_2^j,\cdots,c_q^j\}$，基于该集合，通过贝叶斯推理模型来计算事件 e_j 的信任值，即

$$P(e_j\mid C_j)=\frac{P(e_j)\prod_{k=1}^{q}P(c_k^j\mid e_j)}{P(e_j)\prod_{k=1}^{q}P(c_k^j\mid e_j)+P(\overline{e}_j)\prod_{k=1}^{q}P(c_k^j\mid \overline{e}_j)} \tag{6}$$

其中，$P(e_j\mid C_j)$ 为事件 e_j 的信任值，即事件 e_j 发生的概率；事件 $\overline{e}_j$ 是事件 e_j 的对立事件；$P(e_j)$ 和

$P(\overline{e}_j)$ 分别为事件 e_j 和事件 $\overline{e}_j$ 发生的先验概率。

如果车辆的评分为 1，则 $P(c_k^j \mid e_j)=c_k^j$，$P(c_k^j \mid \overline{e}_j)=1-c_k^j$；否则 $P(c_k^j \mid e_j)=1-c_k^j$，$P(c_k^j \mid \overline{e}_j)=c_k^j$。

最后，将计算结果与定义的事件信息真实性判定阈值 thr_1 进行对比，如果事件 e_j 发生的概率 $P(e_j \mid C_j)$ 大于设定的阈值，则认定该信息为可信信息，否则为虚假信息。当确定信息的真实性后，将信息及其真实性广播至服务范围内的所有车辆，并根据声誉值更新算法对所有参与交互的本地车辆进行声誉值的更新，最后将更新后的声誉值和事件内容作为区块内容存储在 RSU 的资源池中等待上链。若上链时间过长，期间部分数据未更新到区块链中，为保障系统应用的正常运行，RSU 会优先访问资源池中未上链的区块内容，获取参与交互车辆的最新声誉值，以确保数据的准确性。在新一轮车辆交互过程结束后再将更新后的声誉值、事件内容添加到区块中并等待上链。

2.4 声誉值更新算法

在判断事件信息真实性后，需要对广播交通信息的车辆和参与评分的车辆群体进行声誉值的更新，以此来排除恶意车辆。本文设计了联合历史交互信息以及事件信息的声誉值更新算法。算法会根据车辆历史行为对车辆声誉值进行不同程度的更新，若车辆以前存在恶意行为，则降低车辆正常运行时的声誉值奖励或增大其错误行为的惩罚，且声誉值的变化与交通事件的等级呈正相关，高等级的事件对车辆声誉值会产生更大的影响。此外，可以根据实际系统需求来设定声誉值奖励系数 RF 和惩罚系数 PF。当车辆的声誉值低于系统设定的声誉阈值 thr_2 时，将被踢出网络，并且无法获得网络提供的所有服务。具体的声誉值更新算法伪代码如算法 1 和算法 2 所示。

算法 1 声誉值奖励算法

输入 声誉值奖励车辆列表 $\mathrm{List}_{\mathrm{reward}}$、声誉值 rep、奖励系数 RF、事件等级 level、惩罚轮次 flag

输出 车辆声誉值 rep

1) for v in $\mathrm{List}_{\mathrm{reward}}$ do
2) if $v.\mathrm{flag}==0$ do
3) $v.\mathrm{rep}=\min(v.\mathrm{rep}+\mathrm{level}\cdot\mathrm{RF},1)$
4) else do
5) $v.\mathrm{rep}=\min\left(v.\mathrm{rep}+\dfrac{\mathrm{level}\cdot\mathrm{RF}}{\sqrt{1+v.\mathrm{flag}}},1\right)$
6) $v.\mathrm{flag}=v.\mathrm{flag}-1$
7) end if
8) end for

算法 2 声誉值惩罚算法

输入 声誉值惩罚车辆列表 $\mathrm{List}_{\mathrm{punish}}$、声誉值 rep、惩罚系数 PF、事件等级 level、惩罚轮次 flag、区块链 BC

输出 车辆声誉值 rep

1) for v in $\mathrm{List}_{\mathrm{punish}}$ do
2) if $v.\mathrm{flag}==0$ do
3) $v.\mathrm{rep}=\max(v.\mathrm{rep}-\mathrm{level}\cdot\mathrm{PF},0)$
4) $v.\mathrm{flag}=\mathrm{level}$
5) if $v.\mathrm{rep}<\mathrm{thr}_2$ then
6) remove v in BC
7) end if
8) else do
9) $v.\mathrm{rep}=\max(v.\mathrm{rep}-(v.\mathrm{flag}+\mathrm{level})\mathrm{PF},0)$
10) $v.\mathrm{flag}=v.\mathrm{flag}+\mathrm{level}$
11) if $v.\mathrm{rep}<\mathrm{thr}_2$ then
12) remove v in BC
13) end if
14) end if
15) end for

2.5 共识机制

在比特币的区块链系统中，节点通过不断计算获得代币奖励，然而算力较高的节点往往能一直获得奖励，且节点间的竞争会不断造成计算资源的浪费。

在本文设计的车联网区块链系统中，节点之间不存在利益竞争关系，可以适当降低出块难度从而减少计算资源的浪费并提高区块链的出块速度。因此，本文基于 PoW 共识机制提出了一种哈希门限更新机制和等待机制，前者能够确保对车辆声誉值影响更大、影响范围更广的区块更快地上传到区块链中，从而提升恶意车辆的识别效率；后者能够减少 RSU 计算资源的损耗，并避免单个 RSU 持续出块。具体实现方式如下。

所有 RSU 都计算 RSU 的编号 $\mathrm{ID}_{\mathrm{rsu}}$、前一个区块的哈希值 prehash、时间戳 timestamp 和一个随机数 nonce 组合得到的数据的哈希值，并不断改变随机数来获得不同的计算结果，直到该结果满足设定的哈希门限值，当某个 RSU 获得了符合式(7)要求

的随机数 nonce，就被选为矿工节点[20]。

$$\mathrm{Hash}(\mathrm{ID}_{\mathrm{rsu}}\|\mathrm{prehash}\|\mathrm{timestamp}\|\mathrm{nonce})<T_j \quad (7)$$

$$T_j=2^{N_j} \quad (8)$$

$$N_j=N_m-\sum_{\zeta=1}^{3}\mathrm{param}_{\zeta}^{j}-\mathrm{Dparam} \quad (9)$$

其中，N_m 取决于哈希算法，本文采用 SHA-256 算法，则 N_m=256；param 是哈希门限的影响参数；Dparam 是难度调节参数，用于调节系统整体的难度水平，控制出块的速度[21]。

首先，根据事件的等级调整哈希门限值，事件等级越高，对车辆声誉值的影响越大，对应获得的哈希门限值更高，如式(10)所示。

$$\mathrm{param}_1^j=-2^{\mathrm{level}_j-1} \quad (10)$$

其中，param_1^j 是事件等级对哈希门限值的影响，level_j 是事件 e_j 的等级。

其次，根据事件参与评分车辆的数量来调整哈希门限值，参与评分的车辆数量能够反映网络中车辆对事件信息的重视程度。参与评分的车辆越多，更新的车辆声誉值信息也就越多，因此对应的哈希门限值更高，如式(11)所示。

$$\mathrm{param}_2^j=\mathrm{e}^{-\omega_5\mathrm{num}_j+b_1} \quad (11)$$

其中，param_2^j 为参与评分车辆的数量对哈希门限值的影响，num_j 为参与事件 e_j 评分的车辆数量，ω_5、b_1 分别为参与评分车辆数量对哈希门限值的调控因子和调控参数。

本文提出的等待机制如图 3 所示。

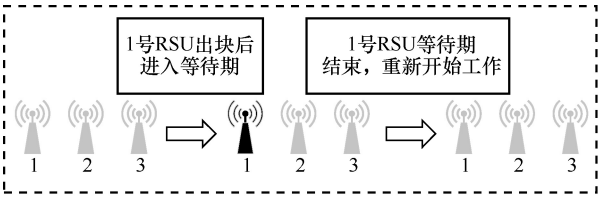


图 3　等待机制示意

定义当前区块编号与历史区块编号的差值为区块距离，如果某个 RSU 生成的历史区块与当前区块的区块距离小于或等于 n，等待机制会根据区块距离的大小增加 RSU 的出块难度，具体实现方式如式(12)所示。

$$\mathrm{param}_3^j=\begin{cases}\sum_{h=m-n}^{m-1}2^{\delta_j}\,\mathrm{check}(m,h),\ m-n>0\\ \sum_{h=0}^{m-1}2^{\delta_j}\,\mathrm{check}(m,h),\ m-n\leqslant 0\end{cases} \quad (12)$$

$$\delta_j=\mathrm{Max}-\frac{\mathrm{Max}-\mathrm{Min}}{n}(m-h) \quad (13)$$

$$\mathrm{check}(m,h)=\begin{cases}1,\ B_m=B_h\\ 0,\ B_m\neq B_h\end{cases} \quad (14)$$

其中，param_3^j 为区块距离对哈希门限值的影响，n 为区块链历史区块对当前哈希门限值的影响范围，m 为当前区块的序号，h 为历史区块的序号，δ_j 为历史区块对当前区块产生的哈希门限值的影响值，Max、Min 分别为历史区块对哈希门限值的最大影响值和最小影响值，check(m,h) 用于检验区块 h 是否由创建区块 m 的 RSU 所创建，B_m 为创建区块 m 的 RSU。

当矿工节点创建区块后，等待机制生效，使其下一次创建块的难度变得相当大，所以该节点的不断尝试实际上是在浪费计算资源。因此，允许 RSU 在创建区块后进入等待期，等待时间取决于 RSU 当前的哈希门限值。如果哈希门限值小于设定的哈希阈值 thr_3，则 RSU 依旧处于等待期，直到哈希门限值大于或等于 thr_3。在此期间，矿工节点由其他 RSU 参与选举，其他系统应用依旧正常运行。这种方式避免了处于车辆高密度区域的 RSU 持续成为矿工节点，既保证了区块链网络中矿工选择过程的公平性，又减少了部分节点计算资源的损耗。如果某个 RSU 长时间未创建区块，则其下一次成功创建区块的概率就会得到提升。

一旦某个 RSU 被选为矿工节点，就会把资源池中收到的事件信息以及参与交互的车辆的声誉值打包成区块，矿工节点将产生的新区块广播给网络中的所有其他 RSU，在收到矿工节点发来的新区块以后，所有的 RSU 都要对区块中的字段进行检验以验证数据的完整性。最后，将区块添加到最长链中。LEA 则根据区块链中新生成的区块更新全局车辆的声誉值。

2.6　区块结构

区块链的区块结构如图 4 所示，一个区块包含了当前的区块编号、RSU 编号、时间戳等信息。本文基于传统区块结构进行修改，使一个区块包含 2 个子块，即事件内容块和声誉值块。事件内容块包含事件的详细信息，对信息数据进行哈希运算后作为树干单元，依次向上取哈希值，从而构建默克尔树，并使其默克尔根作为区块头中的一个子块。声誉值块按照同样的方式构建声誉值的默克尔树。当树中任何一项数据被篡改时，顶层的哈希值就会改变，通过这一方式可以保障区块中的数据不被篡

改。相比于构建两条区块链分别存储交通事件信息和车辆声誉值，仅需在增加一部分数据量的情况下进行一次共识，通过该区块结构能够减少系统的计算资源和存储资源。

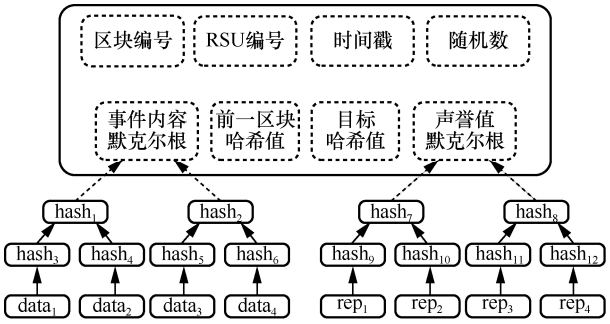


图 4 区块结构

3 仿真分析

本文在处理器为 Intel(R) Core TM i5-9500，RAM 为 8 GB 的 Win10 操作系统环境下使用 Python 语言进行实验仿真，仿真参数如表 1 所示。仿真内容主要包括四部分，第一部分模拟了正常车辆、恶意车辆、RSU 在交通环境下的信息共享以及交互过程，对本文设计的虚假信息识别策略进行了仿真对比；第二部分对本文提出的声誉值更新算法进行了实验，模拟了车辆正常行为、恶意行为后的声誉值变化；第三部分验证了本文设计的区块链哈希门限更新机制和等待机制的有效性；第四部分计算了区块链中的共识机制在不同场景下的区块生成时间，以及难度调节参数对区块生成时间的影响。

表 1 仿真参数

参数	取值
事件信息真实性判定阈值 thr_1	0.5
车辆声誉阈值 thr_2	0
哈希阈值 thr_3	2^{237}
距离参数调控因子 ω_1	0.001
车辆与事件发生地点的距离对评分可信度的影响权重 ω_2	0.3
车辆声誉值对评分可信度的影响权重 ω_3	0.4
车辆评分所花费的时间对评分可信度的影响权重 ω_4	0.3
参与评分车辆数量对哈希门限值的调控因子 ω_5	0.05
参与评分车辆数量对哈希门限值的调控参数 b_1	3
难度调节参数 Dparam	7
车辆声誉值奖励系数 RF	0.03
车辆声誉值惩罚系数 PF	0.03

3.1 虚假信息识别策略的有效性分析

为了分析本文提出的虚假信息识别策略的有效性，本节引入使用车辆与事件发生地点的距离作为信息可信度的方案[18]与基于距离与车辆声誉值共同作为信息可信度的方案[19]进行对比实验，这 2 种方案均应用于车联网的信息真实性判断中，具有很好的代表性，适合作为本文基准。在一个半径 500 m 范围内的区域中模拟 30 个交通事件的广播，对于每个交通事件，负责判断该事件的 RSU 将收集 30 辆车辆的评分信息，并通过贝叶斯推理模型判定事件信息真实性，且 30 辆车中存在不同比例的恶意车辆，恶意车辆有 50%的概率做出恶意行为。本文对不同比例的恶意车辆分别进行了 10 次实验，对事件判断正确率取平均值，事件判断正确率对比如图 5 所示。从图 5 可以看出，本文方案的表现更加优异，在大部分情况下，事件判断正确率能达到 90%以上，这是由于本文方案在考虑车辆声誉值、车辆与事件发生地点的距离以外还考虑了时间对信息可信度的影响

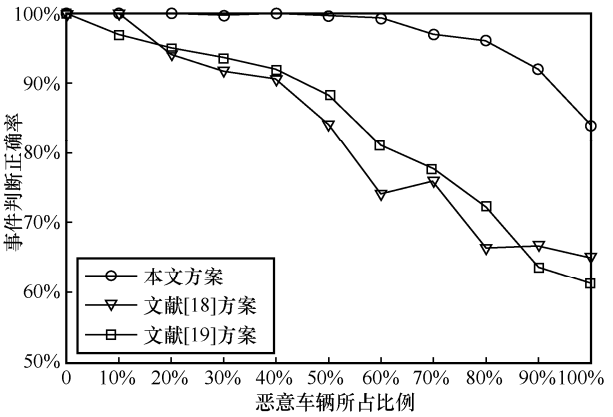


图 5 事件判断正确率对比

3.2 声誉值算法的有效性分析

本节实验模拟了车辆行为引起的声誉值的变化，并引入 Chen 等方案[8]和 Lu 等方案[17]作为参考。车辆声誉值初始值设定为 0.5，为了展示经过声誉值更新算法计算后的声誉值在值域[0,1]上的完整变化情况，系统的声誉阈值 thr_2 设定为 0，实际应用过程中会根据系统对恶意车辆的容忍度来具体调整声誉阈值，车辆声誉值变化对比如图 6 所示。车辆在第 0～6 周期内的行为表现正常，3 种方案的车辆声誉值均正常增加。在第 7～12 周期中，车辆出现了恶意行为，系统对其声誉值进行惩罚，3 种方案均对车辆声誉值进行了惩罚处理，由于本文方案考虑了车辆以往的交互信息，随着车辆发生恶意行为次数的增多，本文方案的

惩罚力度随之增加，在第 12 周期时，车辆的声誉值降低至 0.1 以下。在第 13～20 周期中，车辆行为表现正常，但由于车辆过往的恶意行为，其声誉值的恢复受到限制，本文方案的恢复速度明显慢于其他 2 种方案，能够防止车辆在发生恶意行为后的短时间内恢复其声誉值。综上所述，本文方案能够根据车辆行为对声誉值进行更新，并且对车辆的恶意行为具有较高的防欺骗能力。

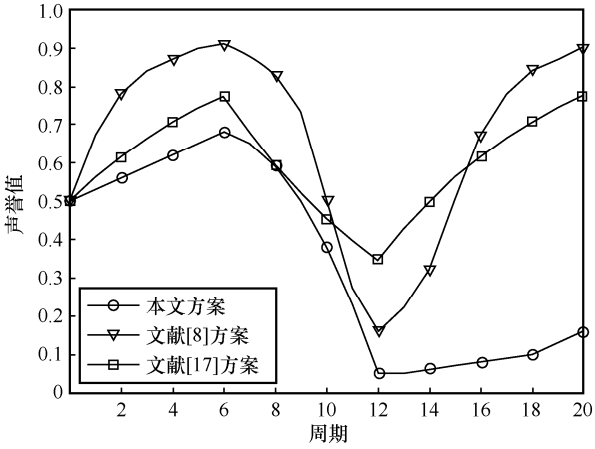


图 6　车辆声誉值变化对比

3.3　共识机制有效性分析

为了更直观地反映哈希门限值对 RSU 创建区块的影响，使用 RSU 成为矿工节点的概率 P 作为目标参数来进行仿真，即

$$P=\frac{T_j}{2^{N_m}} \tag{15}$$

本节分别对 3 种不同组合的 Max 和 Min 进行了对比实验，分别观察这 3 组数据在不同区块距离下出块概率的对数值，出块概率与区块距离的关系如图 7 所示。对于每一种 Max 与 Min 的组合，区块距离与出块概率的对数值保持正相关。Max 和 Min 作为历史区块对当前生成区块的最大影响系数和最小影响系数，Max 与 Min 越小，出块概率越大。由于不同地区不同车辆密度下的业务需求不同，系统追求的出块速度也不相同，因此，可以通过设置 Max 与 Min 来限制哈希门限值的变化范围，进而控制 RSU 成功出块的概率。

另一方面，本文设计的等待机制使最近成为矿工节点的 RSU 的出块概率变得极小，该 RSU 可以停止“矿工选举工作”从而进入等待阶段，系统中的资源消耗也因此得到降低，且进入等待期的时间越久，RSU 在下一次竞争出块的过程中可以获得的出块概率越高。

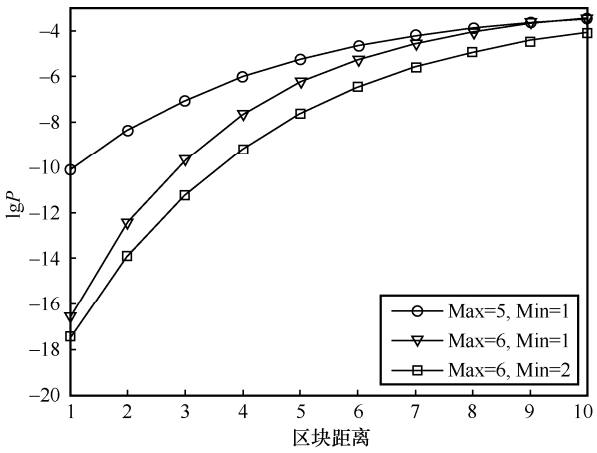


图 7　出块概率与区块距离的关系

为了分析参与评分车辆数量以及事件等级对出块概率的影响，本节还设计了如下实验，固定 Max 与 Min 的值不变，在 3 种不同事件等级的情况下分析参与评分车辆数量对出块概率的影响，结果如图 8 所示。从图 8 可以看出，当参与评分车辆数量一定时，事件等级与出块概率呈正相关；在事件等级一定的情况下，随着参与评分车辆数量的增多，出块概率呈递增趋势。实验结果符合“确保对车辆声誉值影响更大、影响范围更广的区块更快地上传到区块链中”的设计思想。

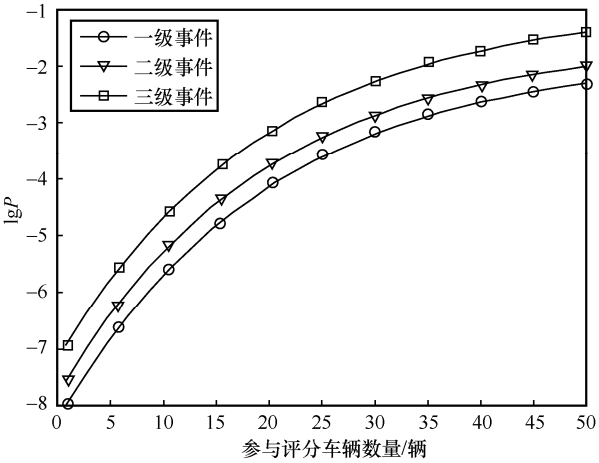


图 8　参与评分车辆数量对出块概率的影响

3.4　区块链区块生成时间分析

本节对区块链中的区块生成时间进行统计分析，由于各个 RSU 的计算能力大致相同，为直观反映参与评分车辆数量与事件等级对区块生成时间的影响，设定 RSU 的平均哈希速率为 2 000 Hash/s，

对比不同评分车辆数量以及不同事件等级下的平均区块生成时间 T（单位为 ms），结果如图 9 所示。从图 9 可以看出，当车辆数量大于 30 时，RSU 的平均区块生成时间相对较短，且当某个交通事件参与评分车辆数量越多以及事件等级越高时，负责该事件的 RSU 能够越快地成为矿工并发布区块。与传统 PoW 共识机制相比，本文设计的共识机制受到多个方面的影响，能够根据实际情况动态改变区块生成时间，而 PoW 共识机制中，区块生成时间只与 RSU 计算能力相关，因此各个 RSU 区块生成时间没有明显差别。

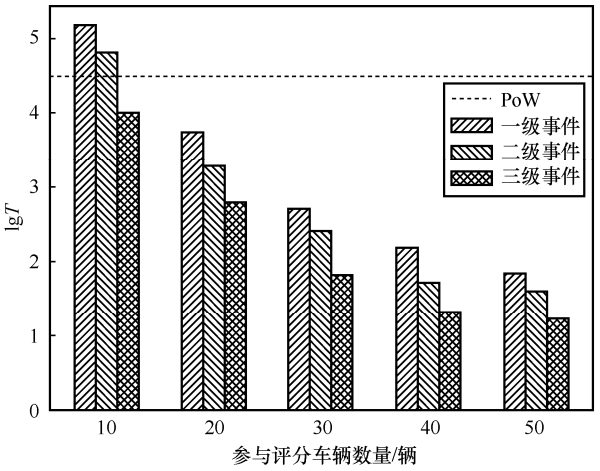


图 9 区块生成时间对比

本节还分析了难度调节参数 Dparam 对本文方案中区块链区块生成时间的影响，在参与评分车辆数量为 30、事件等级为二级的情况下，选取 Dparam =7～12 进行实验，结果如图 10 所示。从图 10 可以看出，区块生成时间会随着 Dparam 的增加而增加，在实际应用过程中，可以根据运行环境以及系统性能等条件对 Dparam 进行调节，以满足系统对区块生成时间的要求。

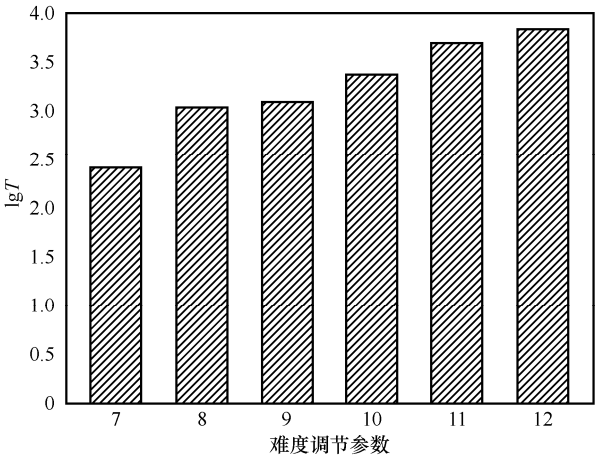


图 10 难度调节参数对出块时间的影响

4 结束语

本文针对车联网场景中可能出现的车辆信任问题，提出了基于区块链的信任管理方案。首先，本文设计了一种车联网虚假信息识别策略，利用贝叶斯推理模型结合多种判决因素提高了车联网中虚假信息的识别准确率，并联合基于车辆历史行为的声誉值更新算法排除恶意车辆。进一步地，通过由 RSU 构建的区块链网络对车辆声誉值以及交互信息等进行分布式存储。最后，设计了适用于车联网场景的共识机制，能够根据实际情况动态调整出块难度，并提出等待机制进一步减少区块链共识所带来的资源消耗，避免了单个 RSU 持续出块的情况。仿真结果表明，本文方案对车联网的信任管理是有效可行的。

参考文献：

[1] KIM D Y, JUNG M, KIM S. An Internet of vehicles (IoV) access gateway design considering the efficiency of the In-vehicle Ethernet backbone[J]. Sensors (Basel, Switzerland), 2020, 21(1): 98.

[2] YANG F C, WANG S G, LI J L, et al. An overview of Internet of vehicles[J]. China Communications, 2014, 11(10): 1-15.

[3] ZHANG K, NI J B, YANG K, et al. Security and privacy in smart city applications: challenges and solutions[J]. IEEE Communications Magazine, 2017, 55(1): 122-129.

[4] LI W J, SONG H B. ART: an attack-resistant trust management scheme for securing vehicular ad hoc networks[J]. IEEE Transactions on Intelligent Transportation Systems, 2016, 17(4): 960-969.

[5] LIU J J, ZHANG S B, SUN W, et al. In-vehicle network attacks and countermeasures: challenges and future directions[J]. IEEE Network, 2017, 31(5): 50-58.

[6] LIU X C, HUANG H P, XIAO F, et al. A blockchain-based trust management with conditional privacy-preserving announcement scheme for VANETs[J]. IEEE Internet of Things Journal, 2020, 7(5): 4101-4112.

[7] AZAD M A, BAG S, HAO F, et al. Decentralized self-enforcing trust management system for social Internet of things[J]. IEEE Internet of Things Journal, 2020, 7(4): 2690-2703.

[8] CHEN J M, LI T T, PANNEERSELVAM J. TMEC: a trust management based on evidence combination on attack-resistant and collaborative Internet of vehicles[J]. IEEE Access, 2018, 7: 148913-148922.

[9] LAI C Z, ZHANG K, CHENG N, et al. SIRC: a secure incentive scheme for reliable cooperative downloading in highway VANETs[J]. IEEE Transactions on Intelligent Transportation Systems, 2017, 18(6): 1559-1574.

[10] 杨哲. 面向车联网的安全机制与关键技术研究[D]. 北京: 北京邮电大学, 2019.
YANG Z. Research on security mechanism and key technologies for Internet of vehicles[D]. Beijing: Beijing University of Posts and Telecommunications, 2019.

[11] ENGOULOU R G, BELLAICHE M, HALABI T, et al. A decentralized reputation management system for securing the Internet of ve-

hicles[C]//Proceedings of 2019 International Conference on Computing, Networking and Communications. Piscataway: IEEE Press, 2019: 900-904.

[12] TANGADE S, MANVI S S, LORENZ P. Trust management scheme based on hybrid cryptography for secure communications in VANETs[J]. IEEE Transactions on Vehicular Technology, 2020, 69(5): 5232-5243.

[13] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[R]. 2008.

[14] LIU Z, XU Y, ZHANG C, et al. A blockchain-based trustworthy collaborative power trading scheme for 5G-enabled social Internet of vehicles[J]. Digital Communications and Networks, 2022, 8: 976-983.

[15] YANG Z, ZHENG K, YANG K, et al. A block chain-based reputation system for data credibility assessment in vehicular networks[C]//Proceedings of IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications. Piscataway: IEEE Press, 2018: 1-5.

[16] KANG J W, YU R, HUANG X M, et al. Blockchain for secure and efficient data sharing in vehicular edge computing and networks[J]. IEEE Internet of Things Journal, 2019, 6(3): 4660-4670.

[17] LU Z J, WANG Q, QU G, et al. BARS: a blockchain-based anonymous reputation system for trust management in VANETs[C]//Proceedings of 17th IEEE International Conference on Trust, Security and Privacy In Computing and Communications/ 12th IEEE International Conference on Big Data Science and Engineering. Piscataway: IEEE Press, 2018: 98-103.

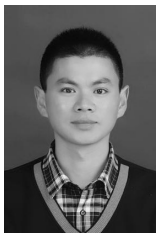
[18] YANG Z, YANG K, LEI L, et al. Blockchain-based decentralized trust management in vehicular networks[J]. IEEE Internet of Things Journal, 2019, 6(2): 1495-1505.

[19] ZHANG H B, LIU J J, ZHAO H L, et al. Blockchain-based trust management for Internet of vehicles[J]. IEEE Transactions on Emerging Topics in Computing, 2021, 9(3): 1397-1409.

[20] 江沛佩, 王骞, 陈艳姣, 等. 区块链网络安全保障: 攻击与防御[J]. 通信学报, 2021, 42(1): 151-162.
JIANG P P, WANG Q, CHEN Y J, et al. Securing guarantee of the blockchain network: attacks and countermeasures[J]. Journal on Communications, 2021, 42(1): 151-162.

[21] 何泾沙, 张琨, 薛瑞昕, 等. 基于贡献值和难度值的高可靠性区块链共识机制[J]. 计算机学报, 2021, 44(1): 162-176.
HE J S, ZHANG K, XUE R X, et al. A highly reliable consensus mechanism for blockchain based on contribution and difficulty values[J]. Chinese Journal of Computers, 2021, 44(1): 162-176.

[作者简介]



张海波（1979– ），男，重庆人，博士，重庆邮电大学副教授、硕士生导师，主要研究方向为车联网、区块链、安全认证等。

曹钰坤（1999– ），男，湖北宜昌人，重庆邮电大学硕士生，主要研究方向为车联网、区块链、信任管理。

刘开健（1981– ），女，重庆人，重庆邮电大学讲师，主要研究方向为区块链、信任管理等。

王汝言（1969– ），男，湖北浠水人，博士，重庆邮电大学教授、博士生导师，主要研究方向为泛在网络、多媒体信息处理等。