计算机科学
COMPUTER SCIENCE

基于区块链的车联网信任管理机制研究

李凤云, 陈明明, 王林, 李朋, 鞠献银

引用本文

李凤云, 陈明明, 王林, 李朋, 鞠献银. 基于区块链的车联网信任管理机制研究[J]. 计算机科学, 2024, 51(4): 381-387.

LI Fengyun, CHEN Mingming, WANG Lin, LI Peng , JU Xianyin. Study on Trust Management Mechanism of Internet of Vehicles Based on Blockchain [J]. Computer Science, 2024, 51(4): 381-387.

相似文章推荐（请使用火狐或 IE 浏览器查看文章）

Similar articles recommended (Please use Firefox or IE to view the article)

基于同态加密的区块链混币方案

Blockchain Coin Mixing Scheme Based on Homomorphic Encryption

计算机科学, 2024, 51(3): 335-339. https://doi.org/10.11896/jsjkx.230100059

基于区块链的联邦蒸馏数据共享模型研究

Study on Blockchain Based Federated Distillation Data Sharing Model

计算机科学, 2024, 51(3): 39-47. https://doi.org/10.11896/jsjkx.230700186

许可链下的事务并行执行模型

Parallel Transaction Execution Models Under Permissioned Blockchains

计算机科学, 2024, 51(1): 124-132. https://doi.org/10.11896/jsjkx.230800201

CASESC:基于以太坊智能合约的云审计方案

CASESC:A Cloud Auditing Scheme Based on Ethereum Smart Contracts

计算机科学, 2023, 50(12): 368-376. https://doi.org/10.11896/jsjkx.221000185

一种安全高效的去中心化移动群智感知激励模型

Safe Efficient and Decentralized Model for Mobile Crowdsensing Incentive

计算机科学, 2023, 50(11A): 221000184-10. https://doi.org/10.11896/jsjkx.221000184

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.230900057

基于区块链的车联网信任管理机制研究

李凤云[1,2]　陈明明[2]　王　林[2]　李　朋[3]　鞠献银[3]
1 网络文化与数字传播北京市重点实验室　北京 110101
2 东北大学计算机科学与工程学院　沈阳 110819
3 沈阳城市学院智能与工程学院　沈阳 110112
(lifengyun@mail.neu.edu.cn)

摘　要　随着自动驾驶和智慧交通系统的发展,车联网技术发挥出了更加重要的作用。车联网是一个开放式的访问环境,这使得如何确保消息可靠、车辆可信等问题成为重大安全挑战。基于此,在已有基于区块链信任管理方案的基础上,重新设计车联网信任管理框架,以弥补现有解决方案存在的可扩展差、共识算法效率低等问题。框架主要由消息信任评估、车辆信任更新和信任区块的创建与共识3个模块组成。在消息信任评估模块中,为识别恶意节点的虚假消息,基于车辆实体的直接信任和邻居车辆的间接信任综合评估消息的可信度。在车辆信任更新模块,为有效抑制车辆的恶意行为,根据消息评估结果和车辆的历史行为对车辆信任进行调整。在区块创建与共识模块中,基于事件重要性和区块链的扩展能力,提出了基于重要性证明的优化共识算法。最后,通过仿真实验验证了框架的可用性,对比实验结果表明所提算法在可扩展性和鲁棒性方面均有显著的提升。

关键词:车联网;信任管理;区块链;共识算法
中图分类号　TP393

Study on Trust Management Mechanism of Internet of Vehicles Based on Blockchain

LI Fengyun[1],CHEN Mingming[2],WANG Lin[2],LI Peng[3] and JU Xianyin[3]
1 Beijing Key Laboratory of Internet Culture and Digital Dissemination Research,Beijing 110101,China
2 School of Computer Science and Engineering,Northeastern University,Shenyang 110819,China
3 School of Intelligent and Engineering,Shenyang City University,Shenyang 110112,China

Abstract　With the development of autonomous driving and intelligent transportation systems,vehicle networking technology is playing an increasingly important role. Due to the open access environment of the Internet of Vehicles,how to ensure the reliability of messages and the credibility of vehicles has become a major security challenge. Building upon existing blockchain-based trust management solutions,there is a need to redesign a trust management framework for vehicular networks to address scalability issues and the inefficiency of consensus algorithms in current solutions. The framework is primarily composed of three modules:message trust evaluation,vehicle trust update,and the creation and consensus of trust blocks. In the message trust evaluation module,to identify false messages from malicious nodes,the credibility of messages is comprehensively assessed based on the direct trust of vehicle entities and the indirect trust from neighboring vehicles. In the vehicle trust update module,to effectively curb malicious behavior,vehicle trust is adjusted based on message evaluation results and the historical behavior of vehicles. In the block creation and consensus module,an optimized consensus algorithm based on proof of importance is proposed,considering event significance and blockchain scalability. Finally,the usability of the framework is verified by simulation experiments,and the comparative experimental results show that the proposed algorithm achieves good results in scalability and robustness.

Keywords　Internet of Vehicles,Trust management,Blockchain,Consensus algorithm

1　引言

随着计算机技术的发展,车联网作为移动自组织网络的应用之一,在汽车工业中得到了广泛应用[1-2]。与传统的移动自组织网络不同,车联网具有高移动性和拓扑易变性,因此其更容易遭受内部和外部的攻击。这些攻击为设计安全的车联网带来了诸多问题,包括安全、隐私和信任[3]。由于整个车联网是一个开放式的访问环境,因此攻击者更容易通过修改、

到稿日期:2023-09-11　返修日期:2024-01-25
基金项目:国家重点研发计划(2022YFE0114200);网络文化与数字传播北京市重点实验室开放课题(2021021900051)
This work was supported by the National Key Research and Development Program of China(2022YFE0114200) and Open Research Fund from Beijing Key Laboratory of Internet Culture and Digital Dissemination Research(2021021900051).
通信作者:王林(smart_wl@163.com)

拦截、注入和删除消息等方式来进行攻击。例如，攻击者获取并改变用于引导道路上车辆的交通信息，并在网络内传播虚假消息，造成交通堵塞、交通事故等危害。为使车联网获得更广泛的应用，必须设计一种有效的方案来解决安全和信任问题，从而能够应对车联网所面临的各种威胁，以实现车联网的商业价值。

针对车联网中的信任问题，目前普遍采用信任管理机制作为解决方案。在已有的方案中，按其部署方式，可以分为集中式和分布式两类。但其存在单点故障、节点信任不一致且不易于维护等问题。近年来，由于区块链技术具有去中心化、安全透明等特点，在存储、跟踪、管理和交换数据时，区块链技术能够合理解决集中式、安全和信任等问题[4]。为保证车辆间交互的信息可信，Yuan 等[5]提出了基于区块链的信用体系，利用区块链记录、更新车辆的路由表，在所提的信誉机制下实现了车联网系统通信开销的大幅降低。Yang 等[6]利用区块链技术设计了一种车载网络信任管理方案，使用工作量证明(Proof of Work，POW)和权益证明算法(Proof of Stake，POS)，选出矿工节点并生成新的偏移量区块，存储车辆节点的信任值。在完成验证后，将新偏移量区块加入区块链中。在现有区块链方案中，共识算法大部分均为 POW 或 POS 的相关变体[7]。POW 虽然具有去中心化、安全性高等特点，但其能耗大，共识时间长。而 POS 虽耗能小，但容易产生马太效应，带来去中心化的问题。在车联网环境中，由于路边单元 RSU(Road Side Unit)算力一般较小，不足以执行 POW 算法，若提升算力，又会导致整个车联网部署成本提升。此外，由于 POW 设计的限制，全部节点都在进行算力竞赛，争相记账，同时全部节点又要进行验证区块以及确认达成一致的公链，出块速度较慢，这将影响车辆信任状态信息的传播，导致无法及时清除恶意车辆。

类似地，Lu 等[8]利用区块链设计了一种匿名声誉管理方案来处理车联网中的信任和隐私问题。虽然在该方案考虑了隐私、激励机制等因素，但基于推荐计算声誉的方式存在合谋攻击的风险，而且该方案不具备抵御能力。Hbaieb 等[9]设计了一种两层区块链架构。在该架构中，信任是通过声誉和位置坐标形成的，并采用本地区块链来满足车联网低延迟的要求。通过引入边缘节点来完成局部信任管理，而 RSU 节点负责建立通信系统的全局信任。Zhang 等[10]使用区块链和深度学习技术来管理车辆网络中的信任。每辆车都会对邻近车辆接收到的信息进行评估，并将识别出的不可信的车辆报告给附近的 RSU 节点。此外，Zou 等[11]为提高车联网的安全性，提出了区域联合学习的方法。该方法将车辆划分为多个区域以维护局部学习模型，并设计信誉机制以保证参与区域学习车辆的可信度。

现有方案大多只针对局部问题展开设计，未考虑完整的信任管理过程。区块链设计中所采用的共识算法效率低，导致可扩展性差[12-14]。针对上述基于区块链的信任管理方案中存在的问题，并以提升方案的可扩展性和鲁棒性为目的，本文展开以下研究工作：为提升检测虚假恶意消息的准确率及方案的扩展能力，重新构建基于区块链的信任管理框架。所提框架主要包含 3 个阶段：消息信任评估、车辆信任更新和信任区块的创建与共识。

2 本文工作

2.1 信任管理框架设计

为了避免集中式和分布式架构的缺陷，框架采用半分布的形式在车联网中进行部署[15]。半分布式网络是车联网中采用区域划分的网络结构，其有助于快速决策并有效维护区块链[16-18]。因此，本文采用具有区域划分的车联网分布式架构作为结构基础，根据地理单元将车联网系统划分为若干区域，且每个区域由若干个 RSU 组成。RSU 负责将区域内的事件数据通过区块链在其他区域内进行共享。每个车辆节点与区域内距离最近的 RSU 进行交互，让事件请求得到快速响应。

在上述车联网分布式架构的基础上，设计了如图 1 所示的信任管理框架。该框架包括车辆信息交互和车辆信任管理两个层次，分别由车辆和 RSU 两类实体构成。其中，车辆是车联网内的通信主体，每辆车配备 OBU 模块，并具备一定的数据存储和计算能力。此外，每辆车拥有一组信任参数，用于评估车辆实体的可信水平。而 RSU 是部署在道路两侧的基础设施，具备计算、存储和服务处理能力，能发挥边缘服务器的作用，主要用于维护和托管区块链，负责收集车辆汇总信息来评估安全消息的真实性，广播安全紧急通知，记录事件信息到区块链，更新车辆信任值等。

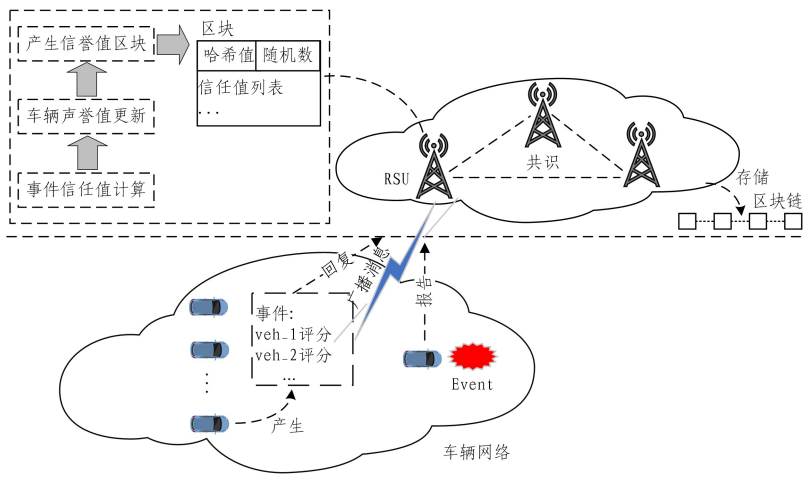


图 1 基于区块链的车联网信任管理框架图

Fig. 1 Blockchain based trust management framework of Internet of Vehicles

如图 2 所示，信任管理框架整体流程包括 3 个模块，分别为消息信任评估、车辆信任调整以及信任区块的创建与共识。消息信任评估用于验证车辆报告的安全紧急消息是否可信，它包含证据信息收集、合谋攻击检测和消息信任值计算 3 个步骤。车辆信任调整和信任区块的创建与共识是消息信任评估的后续处理过程。前者根据消息信任评估结果对参与事件的车辆给予奖励和惩罚；后者将车辆更新后的信任值以及相关事件信息打包成区块，达成共识后，将车辆信任值的信息在车联网内进行共享。

具体流程如图 2 所示。

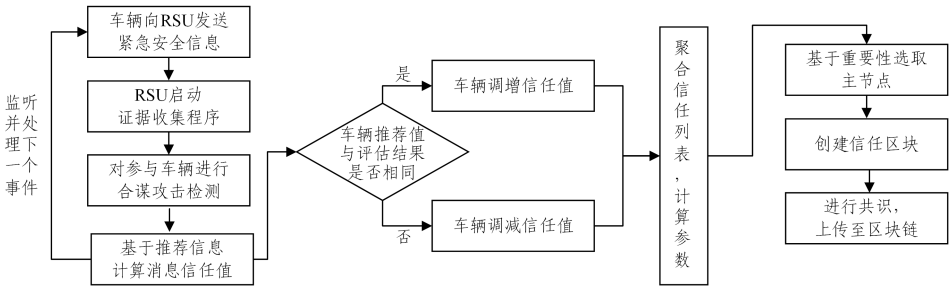


图 2　信任管理框架流程图

Fig. 2　Framework of trust management

2.2　信任管理模型内容

2.2.1　消息信任评估

消息信任评估是信任管理模型的核心内容，是检测恶意节点和虚假信息的关键步骤。根据车联网的特点，形成了适用于车联网环境的信任评估流程，如图 3 所示，具体步骤描述如下。

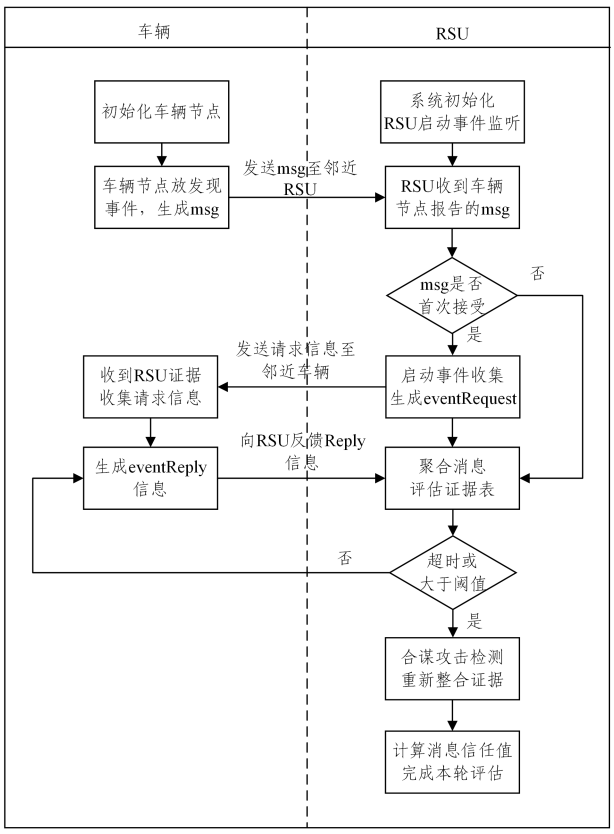


图 3　车联网信任评估流程

Fig. 3　Internet of Vehicles trust assessment process

(1)首先为存储车辆信任值的区块链创建创世纪块；然后初始化车辆节点，为每个节点分配唯一身份标识 vid 并初始化车辆信任值 TV_{vid}，其初始默认值为 0.5；随后，启动 RSU 监听程序，接收车辆报告的安全消息。

(2)车辆节点 v 发现事件 e 时，v 为事件 e 生成安全警告消息 msg，并将其发送给附近的 RSU。msg 的内容格式如下：

〈消息编号，消息类型，事件位置坐标，事件描述，报告者位置坐标，时间戳〉

(3)RSU 接收到 msg 后，立即验证该消息是否为首次接收。若为 RSU 首次接收，随后为 msg 创建对应的消息信任评估事件，并生成与事件相关的请求消息 $eventRequest$。完成上述操作后，RSU 向通信范围内的邻近车辆发送请求信息，并收集相关证据。$eventRequest$ 格式如下：

〈事件编号，msg，RSU ID，RSU 位置坐标〉

(4)其他车辆收到事件请求信息时，根据自身意愿决定是否参与事件验证。对于积极参与验证的车辆，会给予信任奖励来获取相应车联网服务。如果车辆参与事件验证，则生成相应事件反馈信息 $eventReply$。$eventReply$ 内容格式如下：

〈事件编号，反馈结果，车辆 ID，车辆位置坐标，时间戳〉

(5)当 RSU 收集到的反馈信息达到一定数目，或者事件收集程序超过设定的时间阈值，则终止证据收集。

(6)对参与消息评估的车辆集合进行合谋攻击检测。在检测后，将合谋车辆证据信息从反馈消息列表中清除，并重新整理事件证据列表。

(7)基于重新整理的事件证据列表计算消息的信任值，完成本轮信任评估。

当证据信息收集结束后，开始按照如下步骤依次计算，完成消息信任评估。根据证据收集得到的信息形成最终用于消息信任值计算需要的事件验证集合$\{IE, VE_1, VE_2, \cdots, VE_i\}$。其中，$IE$ 代表事件发起者的信息记录，VE_i 代表与事件 e 相关邻近车辆的信息集合。IE 和 VE 的信息内容形式分别如下：〈车辆 ID，事件位置，报告者位置，事件报告时间，车辆信任列表〉、〈车辆 ID，事件反馈值，报告者位置，车辆信任值〉。其中，$EL\langle x_e, y_e\rangle$ 为事件位置；$RL\langle x_{vid}, y_{vid}\rangle$ 为报告者位置；vid 表示车辆 ID；t_{init} 和 t_{end} 分别代表事件报告时间和证据收集结束时间，用于衡量当前 msg 的时效性；车辆信任值和车辆信任列表从区块链中获取。

首先，基于事件发起者 IE 计算消息的直接信任值，计算过程如式(1)所示：

$$dt=\omega+e^{-\lambda(d+t+l)} \tag{1}$$

其中，dt 表示车辆节点关于事件 e 的直接信任值；d,t,l 分别表示报告者位置与事件位置间的有效距离、消息时效性以及事件发起者的信任水平，它们是 dt 计算的参考因素。具体计算过程如下：

$$d=\frac{\sqrt{(x_{\text{vid}}-x_e)^2+(y_{\text{vid}}-y)^2}}{dist} \tag{2}$$

$$t=\frac{t_{\text{end}}-t_{\text{init}}}{T} \tag{3}$$

$$l=1-(TV-\delta\cdot TV_{\text{chnum}}) \tag{4}$$

式(2)中，有效距离基于欧几里得公式计算，$dist$ 表示 RSU 的通信半径。式(3)中，T 表示当前时段完成事件评估的平均处理时长，根据网络状态动态调节其阈值。在式(4)中，TV 表示车辆节点的当前信任值；TV_{chnum} 代表车辆信任增减变化次数；δ 表示车辆信任值的调减系数。

然后，基于邻近车辆的推荐信息集合 VE_i 计算消息的间接信任值。根据车辆的反馈结果 0 或 1 分成两个集合：Set_A 和 Set_{NA}。分别计算每条反馈结果的可信度：

$$ec_i=\begin{cases}\theta_1\cdot e^{-\lambda d}+\theta_2\cdot l, & TV\geqslant 0.5\\ 0, & TV<0.5\end{cases} \tag{5}$$

RSU 获得事件推荐证据的可信度集合 $EC=\{ec_1,ec_2,\cdots,ec_i\}$。然后在 EC 的基础上，使用贝叶斯推理计算消息的间接信任值 it：

$$it=\frac{p(e)\cdot\prod\limits_{i\in Set_A}p(ec_i/e)}{p(e)\cdot\prod\limits_{i\in Set_A}p(ec_i/e)+p(\bar{e})\cdot\prod_{i\in Set_A}p(ec_i/\bar{e})} \tag{6}$$

其中，$p(e)$表示事件 e 发生的先验概率，是根据以往经验分析设定的概率，而对立事件的 $p(\bar{e})=1-p(e)$。$p(ec_i/e)$表示认为事件 e 发生的条件概率，其值为属于 Set_A 集合中的 ec_i；相反，$p(ec_i/\bar{e})$的值为属于 Set_{NA}集合中的 ec_i。

最后，采用加权聚合的方式计算最终的消息信任值。

$$mt=\alpha\cdot \mathrm{d}t+\beta\cdot i \tag{7}$$

2.2.2 车辆信任调整

消息信任评估结束后，根据其评估结果给予参与事件验证的车辆适当的信任奖励或惩罚，这是信任激励机制中的关键步骤。根据“建立信任比毁坏信任更难”这一原则，本文采用“慢奖励快惩罚”的思想来设计车辆信任调整策略：提升信任需要经过长期的诚实行为可以通过发布较多真实消息来获取奖励；降低信任值只需经过几次恶意行为便可将其信任值调整至 0.5 以下，并且对于重新积累信任后再次作恶的车辆，其信任值降到恶意水平的速度会更快。

(1)计算车辆信任调整基数

信任调整基数是车辆信任奖励或惩罚的基准，分别用 $TBase_{\text{inc}}$ 和 $TBase_{\text{dec}}$ 表示，车辆被加入恶意名单中的次数用 num_{mv} 表示。其公式如下：

$$TBase_{\text{inc}}=TBase_{\text{init}}\cdot 2^{-num_{mv}} \tag{8}$$

$$TBase_{\text{dec}}=TBase_{\text{init}}\cdot 2^{num_{mv}-1} \tag{9}$$

其中，$TBase_{\text{init}}$的初始值为 0.01，并且 $TBase_{\text{inc}}$ 和 $TBase_{\text{dec}}$ 的值随着 num_{mv} 的次数的变化而变化。当车辆始终保持诚实行为时，其奖励、惩罚额度均为 0.01。随着 num_{mv} 次数的增加，其奖励、惩罚额度呈指数变化。

(2)计算车辆奖惩系数

车辆奖惩因子是车辆信任调整的系数杠杆，分别用 φ_{inc} 和 φ_{dec} 表示。公式如下：

$$\varphi_{\text{inc}}=\mu^{+} \tag{10}$$

$$\varphi_{\text{dec}}=2^{\mu^{-}}-1 \tag{11}$$

其中，车辆发送真实或虚假消息的次数，分别用 μ^{+} 和 μ^{-} 表示。φ_{inc}呈线性变化，φ_{dec}呈指数变化。在系数杠杆的设计中应用“慢奖励快惩罚”的思想。μ^{+} 和 μ^{-} 只在车辆信任一直处于可信范围内进行累加，当车辆的信任水平低于 0.5 时，将其加入恶意列表，同时将 μ^{+} 和 μ^{-} 置为 0。

(3)更新车辆信任值

当车辆反馈值与 msg 的评估结果不同时：

$$TV_{\text{update}}=TV_{\text{cur}}-TBase_{\text{dec}}\cdot\varphi_{\text{dec}} \tag{12}$$

当车辆反馈值与 msg 的评估结果相同时：

$$TV_{\text{update}}=TV_{\text{cur}}+TBase_{\text{inc}}\cdot\varphi_{\text{inc}} \tag{13}$$

其中，TV_{cur} 表示车辆当前信任值，与区块链中的 TV_{vid} 相对应。

2.2.3 信任区块创建与共识

当对参与消息评估的车辆进行信任值调整后，RSU 要及时将更新后的车辆信任值和相关事件信息打包成区块上传至区块链中，便于其他区域的 RSU 在后续消息信任评估中使用。本文所上传的区块结构如图 4 所示。

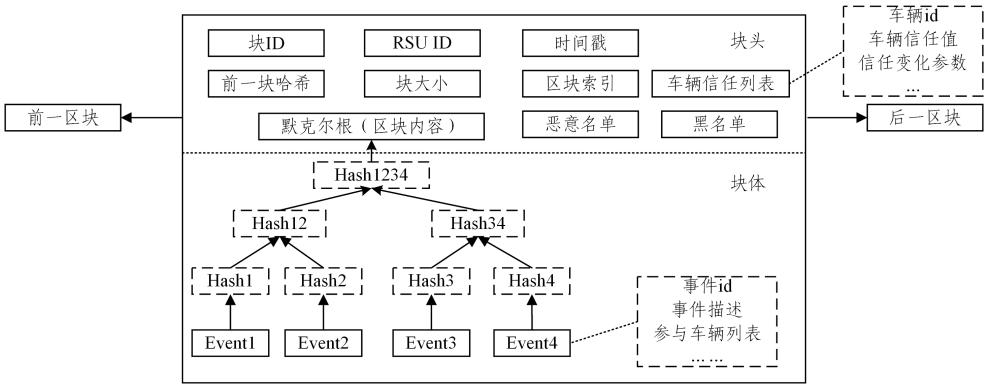


图 4 信任区块示意图

Fig. 4 Trust block diagram

区块结构主要包括块头和块体两部分。在块头中，除了前一区块的主要信息，包括哈希、区块 ID、RSU ID、块大小、

时间戳等传统块头元素，还引入了车辆信任列表、区块索引、恶意名单和黑名单等元素。

车辆信任列表是根据块体中的事件信息聚合而成，并放置在块头中，以便获取车辆信任值及信任变化参数。车辆信任列表的结构内容由如下参数组成：V_{id} 是车辆节点的唯一身份标识，可帮助快速检索车辆信任记录；TV_{cur} 表示车辆节点当前的信任值，是进行消息信任评估的重要参数；TV_{min} 表示车辆信任值连续变化区间的最小值；TV_{max} 表示车辆信任值连续变化区间的最大值；TV_{change} 示车辆信任变化度；TV_{chnum} 表示信任增减变化指数；$TV_{flucnum}$ 表示信任波动指数。其中，TV_{change}，TV_{chnum} 和 $TV_{flucnum}$ 是用于检测合谋攻击的相关参数。

块体中主要记录与消息信任评估相关的事件信息，保存车辆信任调整的依据，为其他 RSU 验证区块提供详细记录。块体中记录事件信息的参数包括事件编号 E_{id}、事件描述 E_{desc}、事件发起车辆 E_{intveh}、参与验证车辆的列表 $E_{vallist}$、事件评估结果 E_{eval}，以及车辆信任调整列表 TV_{update}。

考虑到传统共识算法存在的弊端，本文结合车联网特点、信任管理内容需求等因素，设计了新的共识算法 POI-SPBFT。根据 SPBFT 的设计思想，将 RSU 节点分为两类：候选 RSU 和共识 RSU。其中，共识 RSU 负责进行区块共识；候选 RSU 将共识后的区块加入区块链中。而在选取主节点创建区块时，候选 RSU 和共识 RSU 均参与竞争。POI-SPBFT 算法具体步骤描述如下：

(1)系统首先在每个区域内选取一定数目的候选 RSU 和共识 RSU，完成初始化操作。

(2)系统运行时，RSU 节点基于事件的重要性程度来竞争记账权。

$$hash(block_h) \leqslant \text{arget} \cdot (Block_{imp} + \tau) \tag{14}$$

$$Block_{imp} = \sum_i Event_{imp} \tag{15}$$

其中，$target$ 表示求解问题的基础难度；$Block_{imp}$ 表示区块的重要度，是调节求解问题难度的系数。将多个消息评估事件产生的信息聚合后存储在同一区块，$Block_{imp}$ 也因此由若干个 $Event_{imp}$ 累加而成。事件重要度 $Event_{imp}$ 根据是否包含合谋车辆、恶意名单车辆数目以及信任变化度等因素综合计算，其计算方式如下：

$$Event_{imp} = a \cdot contain_cv + b \cdot num_mv + c \cdot tcm \tag{16}$$

其中，$contain_cv$ 表示当前区块中是否包含合谋车辆，取值 0 或 1；num_mv 表示当前区块数据中恶意车辆数目；tcm 表示需调整车辆信任的变化度，即区块中所有车辆的 $TBase_{inc}$ 或 $TBase_{dec}$ 总和。

RSU 基于消息评估事件所产生信任影响来计算当前区块重要度，并根据区块重要度来调节随机数难度，率先求解答案的 RSU 获得记账权。

(3)主节点将区块广播给所有共识 RSU。若共识 RSU 中不存在拜占庭节点，则执行优化的 SPBFT 算法：共识 RSU 收到区块后进行验证，但不在共识 RSU 之间相互广播；共识 RSU 验证后直接将结果反馈给主节点；主节点收到所有共识 RSU 的反馈并且反馈结果一致，则达成共识。若反馈结果不一致，则表示共识 RSU 中存在拜占庭节点，执行完整的 PBFT 算法逻辑：共识 RSU 收到区块时，与其他 RSU 进行相互广播，并在收到所有其他共识 RSU 节点发送的区块后，进行验证并反馈结果给主节点。主节点收到 2/3 的确认结果，即达成共识。

(4)达成共识后，主节点和共识节点将区块上传至区块链中，并把共识结果广播给其他候选 RSU。此外，还要清除共识 RSU 中的拜占庭节点，并从候选 RSU 中选取新的共识 RSU。每个 RSU 会拥有一个信任积分，当成功创建一个真实的区块，其信任积分加 1。在新一轮的共识 RSU 选举中，选取信任积分较高的候选 RSU。

3 实验验证

实验在处理频率为 2.90GHz 的 Intel i7 处理器以及 16GB 内存环境下进行，算法以及仿真实验采用 C++、GO 语言等实现。使用交通模拟包 SUMO 和离散事件模拟器 NS3 作为实验平台搭建的仿真工具。利用 OpenStreetMap 工具导出 OSM 地图文件，应用 SUMO 工具包对 OSM 地图进行处理，依次生成路网文件 net.xml、地图纹理文件 poly.xml，以及车辆随机移动的路由文件 rou.xml，并创建配置文件，将相关路径和路由等数据导入 NS3 模拟器中。利用 NS3 网络模拟器仿真车联网中车辆与车辆和 RSU 之间交互的过程，来收集随机事件生成的数据。最后，将车辆生成的事件数据导入 GO 语言搭建的区块链系统中，进行消息评估、信任调整以及完成区块创建、共识到上链的过程，并进行结果分析。仿真实验参数如表 1 所列，运行效果如图 5 所示。

表 1 实验仿真参数

Table 1 Experimental simulation parameters

实验参数	取值范围
仿真区域	1 km×1 km
仿真时间/s	2 000
车辆节点数目	300～500
车辆移动速度/(m/s)	15
恶意车辆占比/%	10～30
哈希函数	SHA256

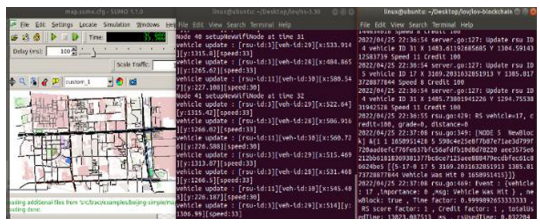


图 5 实验仿真效果图

Fig. 5 Experimental simulation effect

3.1 消息信任评估有效性

为评估消息信任评估的有效性，使用精确率作为评估指标。精确率指检测出真正虚假消息数量与检测出不可信消息数量的比值，用来衡量随着仿真环境中恶意车辆占比增多时，消息信任评估方法的有效性。在本组实验中，车辆总数为 500，恶意车辆数目占比在 10%～30%内变化。为减少误差，每组实验执行多次，结果取均值，实验结果如图 6 所示。随着恶意车辆数目的增加，消息评估的准确率呈下降趋势。从整体上看，在针对单点恶意攻击时，消息信任评估算法是有效的。此外，相比同类的采用综合信任评估方案中，对于间接

信任值的计算，本文虽同样基于其他车辆反馈信息进行计算，但不同的是，本文考虑了每辆反馈车辆的可信度，所考虑的场景更符合实际。因此，在恶意车辆较多的场景中，提供虚假的反馈信息来计算间接信任值时，本文方案更合理，准确性更高。

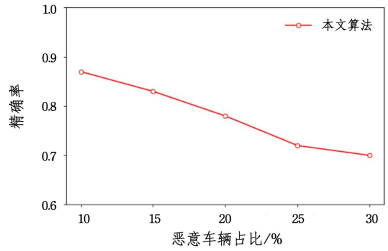


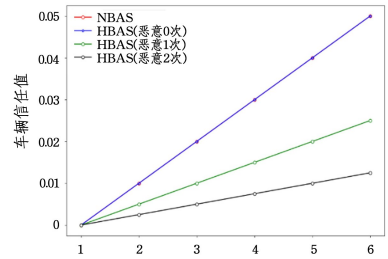
图 6 消息评估准确率随恶意车辆占比的变化情况

Fig. 6 Accuracy of message evaluation changes with proportion of malicious vehicles

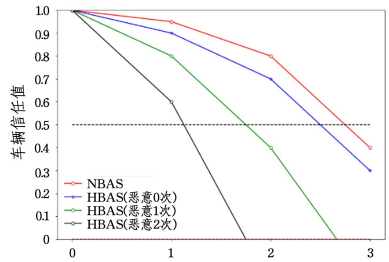
3.2 车辆信任变化情况

为了有效抑制恶意车辆，使恶意车辆的信任水平快速下降，本文在信任管理框架中引入车辆信任调整策略，来抑制车辆的恶意行为。分别设置如下对比实验：连续发送虚假消息、连续发送真实消息、间断发送虚假与真实消息对信任值变化的影响。本文策略表示为 HBAS(History-based Adjustment Strategy)，并且采用基于邻居辅助策略(Neighborhood-based Assist Strategy，NBAS)作为对比实验[19]。

由图 7(a)所示，本文策略在没有被评为恶意车辆时与基于邻居辅助车辆的信任变化情况相同。但是，随着被评为恶意车辆次数的增多，车辆信任值的增幅呈倍数递减。图 7(b)说明车辆被判定为恶意节点的次数越多，承担的代价越大。因为信任值调整策略中考虑了车辆通过积累信任进行多次作恶的可能。此外，与 NBAS 算法相比，本文策略考虑了车辆被评为恶意车辆的历史次数。被评为恶意车辆的次数越多，信任值恢复越慢，再次作恶时惩罚力度也更大，从而最大化降低了恶意车辆频繁作恶的可能性。



(a)连续发送真实消息次数



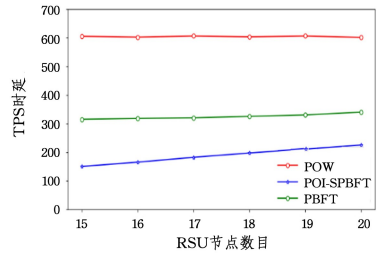
(b)连续发送虚假消息次数

图 7 连续发送真实、虚假消息对车辆信任值的影响

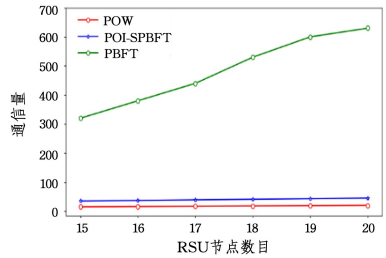
Fig. 7 Influence of continuous sending of true or false messages on vehicle trust value

3.3 共识算法对比

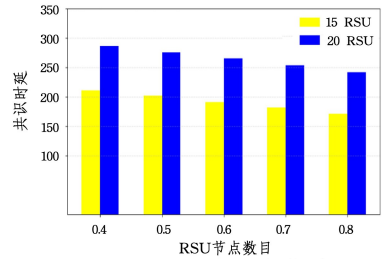
为了对比本文 PoI-SPBFT 算法的改进性能，分别在 TPS 时延、交易通信量、共识时延等方面进行分析，实验结果如图 8 所示。



(a)不同算法下 RSU 数目对 TPS 的影响



(b)不同算法下 RSU 数目对通信量的影响



(c)不同重要性对共识时延的影响

图 8 TPS 时延、通信量、共识时延对比图

Fig. 8 Comparison of TPS delay, traffic and consensus delay

TPS 时延指车联网环境中 RSU 生成一个区块所需的毫秒数，如图 8(a)所示，本文算法的 TPS 时延明显低于 POW，使得系统在单位时间内吞吐量增大，可扩展能力增强。交易通信量指车联网中共识 RSU 节点之间达成共识的通信次数，如图 8(b)所示。本文算法采用 SPBFT 方案，在不存在拜占庭节点的情况下，减少了共识节点数量，从而减少了通信次数。共识时延指车联网中共识 RSU 完成一次共识的时间消耗[20]，如图 8(c)所示。POI 参数变化对共识时延的影响体现在参数值越大，共识时延越小，从而保证了重要性的事件区块可以优先上传到区块链。

相比 POW 算法及其他同类算法，本文用区块重要程度这一系数来调节解题难度，不仅提升了选择记账节点效率，也兼顾了车辆信任评估的应用场景。区块重要程度越高，说明恶意车辆信息更重要，这类区块优先上链，也降低了恶意车辆信息因延时传播再次作恶的风险。此外，在区块共识环节采用 SPBFT 机制，相比 POW 采用算力验证，提升了共识效率；相比 PBFT，提升了共识速度。因此，PoI-SPBFT 算法不仅考虑了信任管理场景中重要信息优先上链的合理性，也降低了计算难度，从而降低了算力消耗。

结束语 本文针对基于区块链的信任管理框架在增强

可扩展性和鲁棒性等问题上展开研究，通过设计新的框架和算法来弥补现有方案中的缺陷。为增强扩展性，使区块链技术更适用于车联网中的信任管理方案，重新设计了基于区块链的信任管理框架，并提出了 POI-SPBFT 共识算法。最后，对本方案进行仿真测试，验证了框架的整体可用性。在未来的工作中，需要针对该框架在降低共识时延、增加区块链节点、降低资源消耗等方面进行改进。

参 考 文 献

[1] HU C, FAN W, ZENG E, et al. Digital twin-assisted real-time traffic data prediction method for 5G-enabled Internet of vehicles[J]. IEEE Transactions on Industrial Informatics, 2022, 18: 2811-2819.

[2] WANG C, CHEN C, PEI Q, et al. An information centric in-network caching scheme for 5G-enabled Internet of connected vehicles[J]. IEEE Transactions on Mobile Computing, 2023, 22: 3137-3150.

[3] GE X, HAN Q L, WU Q, et al. Resilient and safe platooning control of connected automated vehicles against intermittent denial-of-service attacks[J]. IEEE/CAA Journal of Automatica Sinica, 2023, 10: 1234-1251.

[4] ZHENG X, LI M, CHEN Y, et al. Blockchain-based secure computation offloading in vehicular networks[J]. IEEE Transactions on Intelligent Transportation Systems, 2021, 22: 4073-4087.

[5] YUAN M, XU Y, ZHANG C, et al. TRUCON: Blockchain-based trusted data sharing with congestion control in Internet of Vehicles[J]. IEEE Transactions on Intelligent Transportation Systems, 2023, 24: 3489-3500.

[6] YANG Z, YANG K, LEI L, et al. Blockchain- based decentralized trust management in vehicular networks[J]. IEEE Internet of Things Journal, 2018, 6(2): 1495-1505.

[7] XIE M, LIU J, CHEN S, et al. A survey on blockchain consensus mechanism: research overview, current advances and future directions[J]. International Journal of Intelligent Computing and Cybernetics, 2023, 16(2): 314-340.

[8] LU Z, WANG Q, QU G, et al. BARS: a Blockchain-based anonymous reputation system for trustmanagement in VANETs[C]// IEEE International Conference on Big Data Science and Engineering. 2018: 98-103.

[9] HBAIEB A, AYED S, CHAARI L. Blockchain-based trust management approach for IoV[C]// Proceeding of the 35th International Conference on Advanced Information Networking and Applications. 2021: 483-493.

[10] ZHANG C, LI W, LUO Y, et al. AIT: an AI-enabled trust management system for vehicular net-works using blockchain technology[J]. IEEE Internet of Things Journal, 2020, 8(5): 3157-3169.

[11] ZOU Y, SHEN F, YAN F, et al. Reputation-based regional federated learning for knowledge trading in blockchain-enhanced IoV[C]// IEEE Wireless Communications and Networking Conference. 2021: 1-6.

[12] LI X, LIU J, OBAIDAT M, et al. An unlinkable authenticated key agreement with collusion resistant for VANETs[J]. IEEE Transactions on Vehicular Technology, 2021, 70(8): 7992-8006.

[13] FENG J, LIU N, CAO J, et al. Securing traffic-related messages exchange against inside-and-outside collusive attack in vehicular networks[J]. IEEE Internet of Things Journal, 2019, 6(6): 9979-9992.

[14] CHEN X, DING J, LU Z Y. A decentralizedtrust management system for intelligent transportation environments[J]. IEEE Transactions on Intelligent Transportation Systems, 2022, 23: 558-571.

[15] LI B H, LIANG R C, ZHOU W, et al. LBS meets blockchain: an efficient method with security preserving trust in SAGIN[J]. IEEE Internet of Things Journal, 2022, 9: 5932-5942.

[16] LEE S, SEO S H. Design of a two layered blockchain-based reputation system in vehicular networks[J]. IEEE Transactions on Vehicular Technology, 2022, 71: 1209-1223.

[17] WANG Y, CHEN P, WU B, et al. A trustable architecture over blockchain to facilitate maritime administration for MASS systems[J]. Reliability Engineering & System Safety, 2022, 219: 20.

[18] CHOWDHURY M J M, USMAN M, FERDOUS M S, et al. A cross-layer trust-based consensus protocol for peer-to-peer energy trading using fuzzy logic[J]. IEEE Internet of Things Journal, 2022, 9: 14779-14789.

[19] HASROUNY H, SAMHAT A E, BASSIL C, et al. Trust model for secure group leader-based communications in VANET[J]. Wireless Networks, 2019, 25(8): 4639-4661.

[20] XU J J, ZHAO Y L, CHEN H Y, et al. ABC-GSPBFT: PBFT with grouping score mechanism and optimized consensus process for flight operation data-sharing q[J]. Information Sciences, 2023, 624: 110-127.

LI Fengyun, born in 1981, Ph.D, associate professor, is a member of CCF (No. 47373M). Her main research interests include Internet of vehicles, federated learning and data privacy presserving.

WANG Lin, born in 1996, postgraduate. His main research interests include blockchain and trust management.

（责任编辑：何杨）