面向双层区块链的人车分离信任管理方案

张海波[1,2]，黄泓龙[2]，李方伟[1]，徐勇军[2]
（1. 公共大数据安全技术重庆市重点实验室，重庆 401420；2. 重庆邮电大学通信与信息工程学院，重庆 400065）

摘　要：针对车联网中车辆与驾驶员信任关系混乱导致的信任偏差问题，提出了一种基于双层区块链的人车分离信任管理方案，构建了由长期驾驶员信誉区块链和临时车辆信誉区块链组成的双层区块链架构，旨在降低系统存储负载并提升信任管理效率。首先，设计了基于模糊提取的双重密钥人车认证方法，以建立稳定的人车信任链接关系。其次，通过综合直接交互、间接交互和信息质量评价等多维度指标，全面评估了车辆信誉。此外，设计了自适应调整组规模实用拜占庭容错（AS-PBFT）共识算法，以优化共识规模和降低共识时间。最后，通过仿真实验验证结果表明，所提方案在恶意车辆识别率和区块链共识速率性能上优于现有方案。

关键词：车联网；区块链；信任管理；人车信任
中图分类号：TN92
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2024191

Trust management scheme for driver-vehicle separation on dual-layer blockchain

ZHANG Haibo[1,2], HUANG Honglong[2], LI Fangwei[1], XU Yongjun[2]
1. Chongqing Key Laboratory of Public Big Data Security Technology, Chongqing 401420, China
2. School of Communications and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

Abstract: Aiming at the trust bias caused by chaotic trust relationships between vehicles and drivers in the Internet of vehicles, a driver-vehicle separation trust management scheme based on dual-layer blockchain was proposed, a dual-layer blockchain architecture consisting of a permanent driver reputation blockchain and a temporary vehicle reputation blockchain was constructed, aiming to reduce system storage load and improve trust management efficiency. Firstly, a dual-key driver-vehicle authentication method based on fuzzy extraction was designed to establish a stable driver-vehicle trust link. Secondly, vehicle reputation was comprehensively evaluated using multidimensional indicators including direct interaction, indirect interaction, and information quality assessment. Additionally, the adaptive size-practical Byzantine fault tolerance (AS-PBFT) consensus algorithm was designed to optimize the consensus scale and reduce consensus time. Finally, through simulation experiments, it is shown that the proposed scheme outperforms existing schemes in terms of malicious vehicle identification rate and blockchain consensus speed.

Keywords: Internet of vehicles, blockchain, trust management, driver-vehicle trust

---

收稿日期：2024–07–04；修回日期：2024–10–29
通信作者：黄泓龙，s220132061@stu.cqupt.edu.cn
基金项目：国家重点研发计划基金资助项目（No.SQ2023YFB250002402）；国家自然科学基金资助项目（No.62371082，No.62271094）；公共大数据安全技术重庆市重点实验室开放基金资助项目（No.CQKL-QJ202300002）；重庆市留创计划创新类基金资助项目（No.cx2020059）
Foundation Items: The National Key Research and Development Program of China (No. SQ2023YFB250002402), The National Natural Science Foundation of China (No. 62371082, No. 62271094), The Foundation of Chongqing Key Laboratory of Public Big Data Security Technology (No. CQKL-QJ202300002), Chongqing Innovation and Entrepreneurship Program for the Returned Overseas Chinese Scholars (No.cx2020059)

0 引言

在过去的几十年里，通信[1]、云计算[2]和车载传感[3]等领域取得了长足的进步，改善了交通运营效率与驾驶员体验，也为下一代车联网（IoV, Internet of vehicles）铺平了道路。然而，随着越来越多联网汽车的出现，交通拥挤和事故频发给社会造成了巨大的损失。近年来，研究者提出了智能交通系统（ITS, intelligent transportation system），旨在建立安全高效的交通管理方案[4]。在ITS中，车辆之间存在大量的信息交换，车辆自组织网络（VANET, vehicular ad-hoc network）中的车辆之间进行交互，类似于人类的社会活动，车辆社交网（VSN, vehicular social network）也由此应运而生[5]。

VANET中的车辆具有高速移动特性，且车辆与其周围大多数相邻车辆之间的熟悉程度相对较低。相对陌生的环境使得在车辆之间共享信息的真实性和可靠性面临挑战，如果恶意用户趁机发布的错误交通信息没有被系统有效甄别[6]，可能会带来严重的后果，包括但不限于交通拥堵甚至严重的交通事故[7]。因此，构建一个能够确保交通安全的车联网信任管理系统显得尤为重要。Li等[8]提出了一种集中式的新型公告方案，通过评估消息的可靠性，使邻近车辆能够利用这些信息提高道路安全性和交通效率。Hu等[9]提出了一种可靠的基于信任的车队服务推荐方案，该方案中强大的中央服务器负责存储反馈数据、信誉列表等信息。然而，上述这些方案都依靠一个受信任的强大中心化实体，存在单点故障、可伸缩性差等问题，当节点数量膨胀时会对系统的承受能力带来挑战。

区块链作为近年来一种新兴的分布式账本存储技术，具有去中心化、一致性、防篡改和容错性等特点，在物联网等领域应用十分广泛[10]。Singh等[11]提出了一种基于智能合约的信任管理方案，由边缘的路侧单元（RSU, road side unit）共同协作维护车辆信任值，通过分片减少了区块链的工作负载，并使用智能合约搭建的开源平台验证了该方案的可行性。Zhang等[12]提出了基于评级制度的信誉计算机制以确保消息评价的合理性，并提出了工作量证明（PoW, proof of work）和权益证明（PoS, proof of stake）相结合的共识机制，确保声誉变化较大的车辆可以优先更新到区块链。Ahmad等[13]提出了一种新型的混合信任管理方案，该方案同时在传输层和应用层对节点本身信任度及数据的可信度进行评估，通过车辆接收的信息对车辆信任度进行建模和评估。Lee等[14]在区块链架构上做了改进，提出了一种基于区块链的两层信誉系统，减小了车辆的内存开销。区块链技术使得透明、分布式的安全信任管理系统的设计成为可能。此外，一些研究人员为了在车联网中更好地部署区块链，对区块链共识机制做了改进[15-19]。由此可见，区块链在VSN的信任管理方面发挥了很好的作用。

在当前IoV信任管理研究中，信任管理对象主要是车辆实体，车辆实体的信誉值即代表着驾驶车辆人员的信任情况。然而，在VSN中，驾驶员的正当或不正当行为会改变其在社交体系中的重要程度[20]，车与车的社交关系的本质是人与人之间的社交信任，因而VSN中驾驶员与车辆的信任角色需要重新规划。近年来，随着网约车和共享汽车等新模式经济快速发展[21]，大量网约车平台公司获得经营许可，汽车分时租赁企业也广泛开展经营，因此共享汽车成为未来城市交通中不可或缺的一部分。在共享交通中，车辆与驾驶员往往处于非1对1的状态[22]。VSN与共享交通的发展给IoV带来了一个新问题：历史行为诚实的车辆不一定表明当前驾驶员值得信任，以往仅仅考虑车辆信任度的IoV信任管理模式存在信任偏差。因此，现阶段迫切需要设计一个新的IoV信任管理方案，以重新考量驾驶员与车辆之间的信任关系，防止信任偏差导致的恶意车辆攻击。可以预料的是，由于新的方案会引入驾驶员信誉值等大量信息，提高了区块链的负载，从而会影响区块的出块效率，因此新的模型还需要解决这一问题。

根据上述讨论，针对在新一代ITS中车辆和驾驶员信任关系混乱导致的信任偏差问题，本文将车辆作为驾驶员信誉值更新的载体，充分利用区块链在分布式安全性能方面的优势，提出了一种人车分离的双层区块链信任管理方案。本文主要工作如下。

1) 建立了一个IoV场景下人车分离的信任管理架构，使用双层区块链分别对人和车的信任信息进行存储。设计了一种新型的人车认证方法，通过对人的生物特征和车的密钥进行验证，实现驾驶员到

车辆的信任转换过程。同时，新的双层区块链架构对车辆区域进行了分区管理，下层区块链节点定期向上层区块链节点上报信任信息后会清除历史信息，从而提升系统的运转效率，减轻系统的负载压力。

2) 提出了一种人车信誉值更新模型。在该模型中，通过综合车辆的直接交互评价、间接交互评价和信息质量评价对车辆当前行为做信誉评分。利用车辆信誉评分建立驾驶员近期信任表，在设定的时间节点，根据近期信任表对驾驶员信誉值进行更新。多方车辆行为评价保证了信任评价的可靠性，同时在驾驶员近期信任表中使用轮次代替了时间戳，有效地预防了恶意车辆的周期性攻击。

3) 针对车联网系统中节点的计算能力和存储能力有限的问题，提出了自适应调整组规模实用拜占庭容错（AS-PBFT, adaptive size-practical Byzantine fault tolerance）共识算法，该算法根据近期活跃度与信誉值排名对 IoV 车辆进行两轮筛选，由筛选后的车辆节点组成共识委员会，在由可信节点组成的共识委员会中随机选择领导节点，由领导节点率领共识委员完成此次共识。仿真实验结果表明，该共识算法提高了共识速率，降低了节点的存储压力。

1　系统模型

1.1　系统组成

本文所设计的系统主要由可信领导路侧单元（T-RSU, trusted leader RSU）、本地辅助路侧单元（L-RSU, local secondary RSU）、车辆和区块链组成，系统模型如图 1 所示。

1) T-RSU。可信实体，T-RSU 难以被击破，其计算能力强，在系统中还作为车辆注册信息的管理中心。

2) L-RSU。半可信实体，负责收集信誉值评价影响信息，计算本地车辆节点的当前信誉值，并定期更新驾驶员全局信誉值。L-RSU 将更新后的全局信誉值传递给上层区块链节点 T-RSU，以确保整个系统的信任关系能够及时地反映在区块链上。L-RSU 大量存在于本地车辆网络中，为本地车辆提供通信服务。

3) 车辆。车辆能够在下层区块链作为全节点维护区块链。一旦驾驶员登录车辆，该车辆将继承驾驶员的历史信誉值，并在所在区域内进行活动。

4) 区块链。因其具有去中心化、不可篡改和透明的特性，区块链在本文系统中作为信任和数据管理的核心基础设施，负责记录和维护驾驶员及车辆的历史信誉值，确保信息的完整性和可追溯性。而通过双层结构的设计，使区块链允许本地车辆在不同区域间进行无缝迁移和信任信息的即时更新。这种设计使得系统能够高效地管理复杂的信任关系，同时保持了对历史数据的完整记录和对当前活动的实时反映。

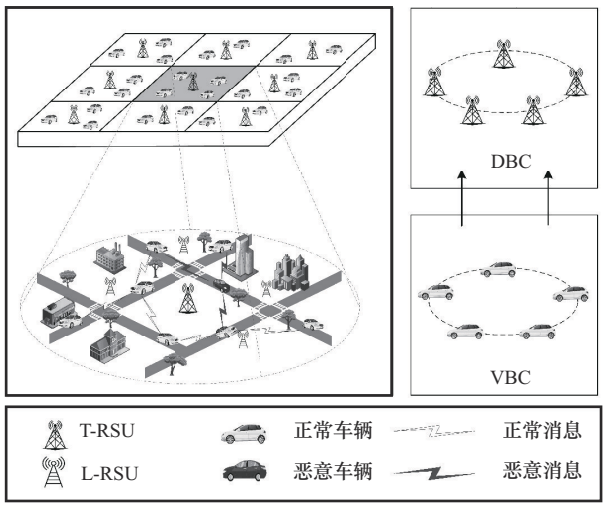


图 1　系统模型

1.2　双层区块链

本文系统的双层区块链分别负责对驾驶员和车辆的信誉值进行维护，上层区块链作为长期区块链管理驾驶员的信任情况，而下层区块链定期清零更新，管理某个分区当前行驶车辆的信任情况。

1) 驾驶员信任值区块链（DBC, driver trust value blockchain）。作为上层区块链，DBC 记录全局所有历史登记的驾驶员信息。该区块链由全局性能较好的 T-RSU 维护，由于历史信息量较大，为了降低维护其正常运作的成本和难度，DBC 会在系统设定的更新时间节点进行更新。

2) 车辆信任值区块链（VBC, vehicle trust value blockchain）。作为下层区块链，VBC 记录当前区域中的本地车辆信息。L-RSU 与本地车辆共同维护该区块链，VBC 规模小、更新频率快，采用本文提出的 AS-PBFT 算法作为 VBC 的共识算法。当车辆

进入一个新的区域后，会加入当前区域的VBC，前一个区域的交通信息不会影响车辆在新区域的活动。

1.3　人车密钥

在本文方案中，人与车作为2个独立的实体，需要采用不同的密钥信息以保证系统的安全性，因此加入系统时两者的密钥信息缺一不可，这两类密钥信息分别如下。

1) 驾驶员生物信息密钥。指纹、虹膜、面部特征等都属于生物信息的范畴，它们能够高度精准地验证生物个体身份。在注册过程中，驾驶员通过专用的生物采集器将这些生物信息录入系统，并由T-RSU进行安全存储。由于生物信息的个人独有性，这种密钥系统能够有效防止身份冒用和非法访问[23]，确保驾驶员信息的安全和隐私。

2) 车辆数字密钥。当驾驶员准备在某车辆上进行登录或启动时，除了身份验证外，还需要输入车辆数字密钥，以确认车辆的信息并验证驾驶员的合法性。通过车辆数字密钥系统，可以确保只有经过授权的人员才能操作车辆，从而大大增强了车辆的安全性[24]。同时，这一系统还能有效降低车辆被盗用的风险，为车主和驾驶员提供了更加可靠的保障。

1.4　对手模型

分布式的IoV信任管理框架为攻击者提供了渗透网络的机会，攻击者可以利用模型结构进行恶意行为，其主要目标在于拦截或改变数据，或是通过恶意行为破坏系统的信誉评定。这些攻击会损害信誉系统的可靠性，使识别模型和处理模型威胁更具挑战性。

本文方案的威胁主要来自以下2个方面。

1) 恶意车辆。传统的恶意车辆可能会持续性地进行恶意行为。为了隐藏身份，某些恶意车辆会周期性地切换诚实行为和恶意行为来避免系统检测。

2) 妥协RSU。本文方案假设只有安全性较低的L-RSU可能会被击破，这些L-RSU中的数据可能会遭到篡改，在这个L-RSU区域中的车辆服务会被拒绝。

2　方案设计

2.1　方案流程

如图2所示，本文设计的信任管理方案主要包括6个步骤：① 人车认证；② 数据共享；③ 信誉评价，主要包括信息质量评价、直接交互评价和间接交互评价；④ L-RSU辅助下基于AS-PBFT的VBC定期更新；⑤ 近期信任表更新和驾驶员状态评估；⑥ 驾驶员信誉计算和DBC更新。

2.2　人车认证

在参与到信任管理系统前，需要对驾驶员身份和车辆信息进行认证。由于本文方案中驾驶员身份的特殊性与重要性，基于模糊提取器提出了一种基

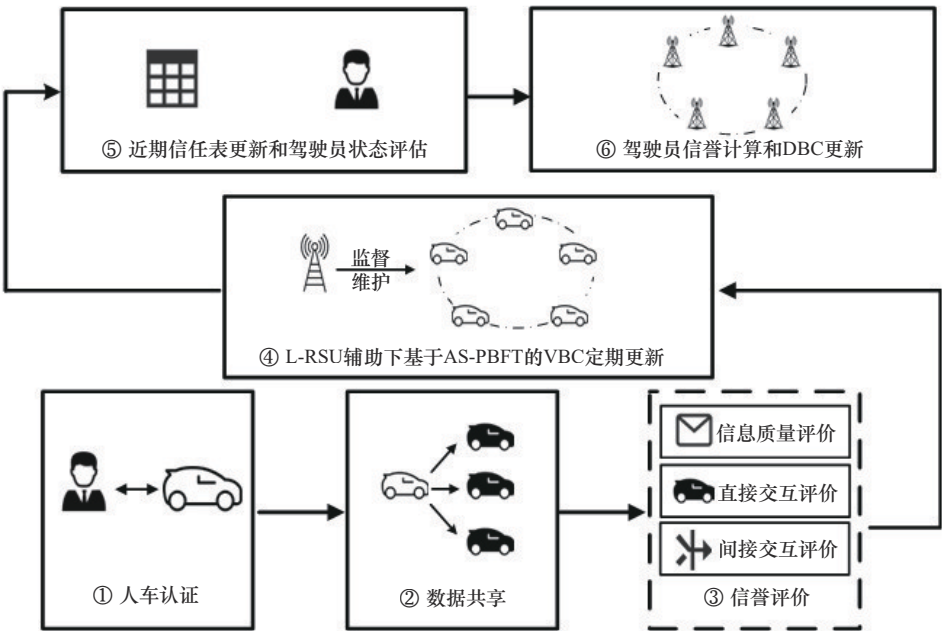


图2　系统流程

于密钥与生物特征的双重认证方案。

该方案定义了一个阶为q的循环群G、一条基点为P的椭圆曲线$E(F_p)$，一个安全且抗碰撞的单向哈希函数$H(\cdot)$，基于椭圆曲线加密算法随机选择私钥$\mathrm{Pri} \in Z_q^*$，并计算出其公钥$\mathrm{Pub} = \mathrm{Pri}P$。

当驾驶员登录到先前注册过的车辆时，系统会对其进行身份认证以确保身份信息准确。如图3所示，驾驶员认证流程包括以下步骤。

1) 驾驶员d_i将身份信息ID_{d_i}、生物特征ω'_{d_i}和车辆密码PW_{c_j}输入车辆c_j。

2) 车辆c_j向T-RSU$_{k_0}$发送驾驶员身份信息ID_{d_i}、车辆信息ID_{c_j}、认证请求Qurey_{d_i,c_j}和签名信息Signature以查询DBC数据。同时，选择一个随机数N_1计算随机密钥N_1P，并与当前时间戳T_1一并发送给L-RSU$_k$。

3) T-RSU$_{k_0}$查询驾驶员d_i的历史注册信息，确认条件无误后将注册信息$(\mathrm{CID}_{d_i,c_j}, K_{d_i,c_j}, P_{d_i})$以及当前时间戳$T_2$传递至L-RSU$_k$，注册信息的相关参数曾在人车注册时存入。具体地，人车动态身份密码$\mathrm{CID}_{d_i,c_j} = H(\mathrm{ID}_{d_i} \| \mathrm{ID}_{c_j} \| N_0)$，其中$N_0$为引入的随机数，双重密钥$K_{d_i,c_j} = H(R_{d_i}, \mathrm{PW}_{c_j})$，随机密钥$R_{d_i}$和辅助公共信息$P_{d_i}$由模糊提取器的随机密钥生成函数$\mathrm{Gen}(\omega_{d_i}) \rightarrow (R_{d_i}, P_{d_i})$产生，而$\omega_{d_i}$为驾驶员$d_i$在注册时采集的生物特征信息。

4) 当L-RSU$_k$收到来自T-RSU$_{k_0}$的确认信息后，选择一个随机数N_2计算随机密钥N_2P，将N_2P与确认信息$(\mathrm{CID}_{d_i,c_j}, P_{d_i}, T_2)$一并传递给车辆$c_j$。

5) 车辆c_j采用模糊提取技术中的恢复算法$\mathrm{Rep}(\omega'_{d_i}, P_d) \rightarrow R'_{d_i}$恢复出随机密钥$R'_{d_i}$，计算以验证驾驶员生物特征的哈希值密钥$K'_{d_i,c_j} = H(R'_{d_i} \| \mathrm{PW}_{c_j})$，并利用随机值$N_1$和$N_2$计算基于随机数产生的哈希值密钥$K_r = H(N_2N_1P \| N_2P \| N_1P)$，接着计算车辆$c_j$的认证密钥$\mathrm{Auth}_{c_j} = H(K'_{d_i,c_j} \| K_r \| T_1 \| T_2)$。类似地，在L-RSU$_k$中计算基于随机数产生的哈希值密钥$K_r = H(N_2N_1P \| N_2P \| N_1P)$和L-RSU$_k$的认证密钥$\mathrm{Auth}_{R_k} = H(K_{d_i,c_j} \| K_r \| T_1 \| T_2)$。

6) 验证$\mathrm{Auth}_{c_j} \stackrel{?}{=} \mathrm{Auth}_{R_k}$，确认认证结果。若相等则认证成功，回复车辆$c_j$的验证消息；否则认证失败，禁止车辆$c_j$加入系统。

2.3　车辆数据共享和信誉评价

2.3.1　数据共享

本文方案中，数据共享方式主要有普通服务请

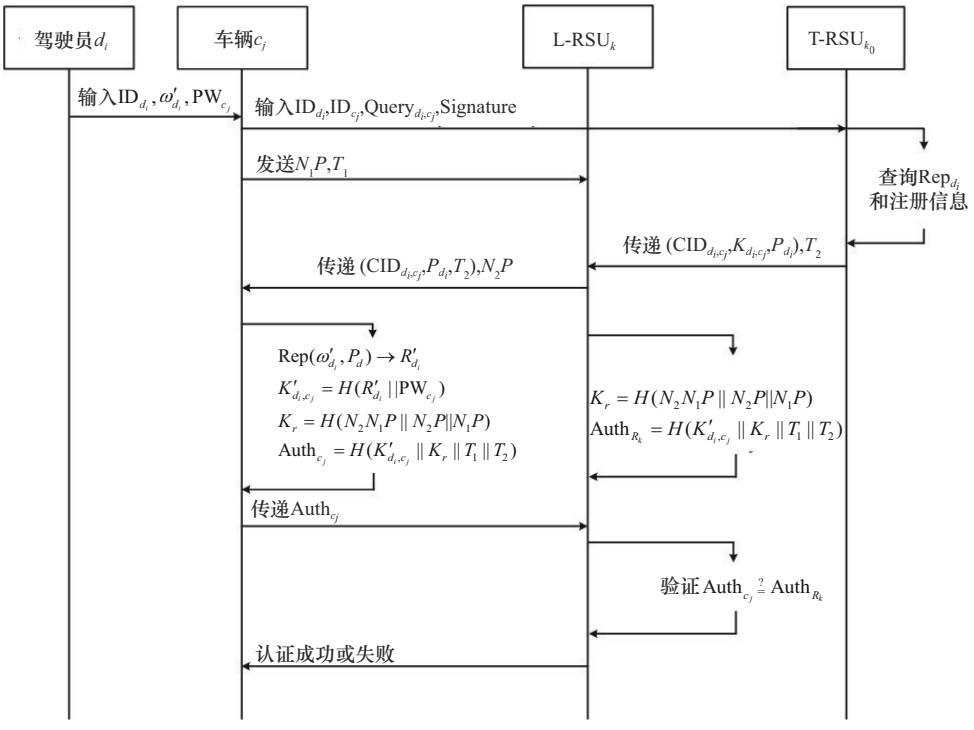


图3　驾驶员认证流程

求和交通事件通告两类。两类数据共享方式都涉及数据提供方c_j向数据接收方$c_{j'}$提供信息，$c_{j'}$再对c_j进行信息质量检查及信誉评价。高效的数据共享有利于增强驾驶员体验，促进驾驶员互动与社区感。两类数据共享方式具体步骤分别如下。

1) 普通服务请求。数据请求车辆$c_{j'}$向附近VBC节点L-RSU$_k$发送服务请求，L-RSU$_k$向VBC中的所有车辆节点广播服务请求消息meg_{req}。

数据提供车辆c_j向L-RSU$_k$发送共享数据，L-RSU$_k$需要检查车辆c_j当前驾驶员的信誉值Rep_{d_i}是否大于Rep_{thr}，符合要求则将其共享数据上传到VBC。

车辆$c_{j'}$与其他对数据感兴趣的车辆可以从VBC下载相关数据，并对其信息质量进行评价。

2) 交通事件通告。当交通路况通告车辆c_j发现交通事件（如追尾事故、道路拥堵）时，它会将该信息meg_{Tra}广播给L-RSU$_k$以及其他车辆，以达到事故预警、拥堵控制的目的。

L-RSU$_k$信息接收者车辆$c_{j'}$在获取到交通通告信息meg_{Tra}后，根据事件等级做出不同响应，当交通应急事件等级较高时，L-RSU$_k$会发出警报，交通运输部门收到警报后，会做出派警、关闭路段等应急措施，以避免交通事故。当交通应急事件等级较低时，L-RSU$_k$会将交通应急事件等级做记录，附近车辆自行对事件进行处理，如调整行车路线等，并在一定时间后对车辆c_j进行信誉评价。

例如，当高速公路出现某起追尾事故时，c_{witness}作为首批目击者，应立即将该交通事故信息$\text{mes}_{\text{newtra}}$广播给当地路侧单元$\text{L-RSU}_{\text{near}}$以及附近其他车辆。$\text{L-RSU}_{\text{near}}$会发出警报，相关部门立即关闭附近高速路段，附近其他车辆在收到警告后会小心通过相关路段，以避免二次交通事故。

2.3.2 信息质量评价

在IoV中，通信距离、消息事件差等因素会对信息质量产生影响。本文方案为了对消息本身可信度进行考量，过滤掉不真实或误导性的车辆消息，引入了信息质量评价机制。信息质量评价值$\text{Info}Q_{(j'j,t)}$会影响车辆的信誉评价。

$$\text{Info}Q_{(j'j,t)}=\frac{\text{rel}(\text{Dist}+\text{TL})}{2} \tag{1}$$

$$\text{Dist}=\frac{d_m-d}{d_m} \tag{2}$$

$$\text{TL}=\eta(t-t_0)^{-\varepsilon} \tag{3}$$

其中，rel表示消息相关指数，Dist表示距离系数，TL表示时间新鲜度、信息请求时间t_0与接收时间t相关，d_m表示VBC区域直径，d表示数据接收车辆$c_{j'}$与数据发送车辆c_j之间的距离。

2.3.3 直接交互评价

服务请求车辆$c_{j'}$与信息提供车辆c_j的直接交互信任值基于其之前的直接共享交互历史信任值。车辆的信息直接交互评价遵循基于beta分布的信誉函数。

$$T_{(j'j,t)}^{\text{direct}}=\frac{\text{pos}}{\text{pos}+\text{neg}} \tag{4}$$

其中，$T_{(j'j,t)}^{\text{direct}}$表示车辆$c_{j'}$对车辆$c_j$的直接交互信誉值，pos和neg分别表示车辆$c_{j'}$与车辆$c_j$的正面和负面的交互次数。而在车辆$c_j$所发送的所有历史消息中，只有通过VBC共识并记录在当前VBC上的消息才会被记录为正面消息，否则会被认定为负面交互。

2.3.4 间接交互评价

车联网环境中依靠单车进行直接交互评价无法对车辆交互进行准确评价，需要引入间接交互评价作为对车辆整体行为信任评估的补充。具体来说，通过邻居信任表和邻居历史信任对间接信任值进行衡量。

$$T_{(j'j,t)}^{\text{indirect}}=\sum_{k=1}^{M}\text{Info}S_{(k,t)}T_{(k,t)}^{r}\text{TR}_{(k,t)} \tag{5}$$

$$\text{Info}S_{(k,t)}=\frac{1}{8}\left(\sum_{a=1}^{2}(1-m_a)+\sum_{b=3}^{5}(2-m_b)\right) \tag{6}$$

$$\text{TR}_{(k,t)}=\frac{\text{Rep}_k^{\text{old}}}{\sum_{n=1}^{M}\text{Rep}_n^{\text{old}}} \tag{7}$$

其中，$T_{(k,t)}^{r}\in\{0,1\}$，表示M个中介车辆的推荐评级，$\text{Info}S_{(k,t)}$表示第k个邻居的个人信息评价值，$\text{TR}_{(k,t)}$表示历史信任权重，m_a、m_b的取值会影响个人信息评价值，如表1所示。

值得注意的是，RDD_m为驾驶员最近驾驶该车辆的行驶路程，其能够体现驾驶员与车辆的匹配程度。

表1　　驾驶员个人信息评价值

指标	类别区间	评分
居住地(m_1)	本地	0
	非本地	1
车牌地(m_2)	本地	0
	非本地	1
车况评级(m_3)	I级	0
	II级	1
	III级	2
RDD_m(m_4)	[0,30〉km	0
	[30,50〉km	1
	>50 km	2
车距(m_5)	[0,100〉km	0
	[100,1 000〉km	1
	>1 000 km	2

2.3.5　车辆信誉计算

由车辆$c_{j'}$请求数据，车辆c_j提供数据的本次车辆交互过程完成后，L-RSU$_k$需要计算本次行为后车辆c_j的车辆信誉值$\mathrm{Cre}_{(j,t)}$。当信息质量评价、直接交互评价和间接交互评价都完成之后，需要对影响车辆信誉值的多因素进行综合评分。

$$\mathrm{Cre}_{(j,t)} = \alpha_1 \mathrm{Info}Q_{(j',j,t)} + \alpha_2 T^{\mathrm{indirect}}_{(j',j,t)} + \alpha_3 T^{\mathrm{direct}}_{(j',j,t)} \quad (8)$$

其中，$\alpha_1 + \alpha_2 + \alpha_3 = 1$。车辆新信誉值由RSU$_k$计算，并在近期信任表中更新。

2.3.6　基于AS-PBFT的VBC更新

为了提升共识效率，本文提出了一种适用于IoV场景下的AS-PBFT共识算法。如图4所示，在每次共识开始之前，需要确定共识委员会成员，VBC中该区域内的所有车辆节点被分类为领导节点、辅助节点和候选节点。

首先，信誉值低于阈值$\mathrm{Cre}_{\mathrm{thr}}$的低信任节点会被排除在选择范围外。然后，节点活跃等级较低，即sleep > 0的非活跃节点也将被排除在外。如果此时的节点规模仍然较大，共识节点组中的节点则会根据信誉值高低进行排序，由信誉值排名在前σ的节点组成最终的共识委员会。最后，从共识委员会所有节点中随机选取一个节点作为领导节点，作为AS-PBFT共识算法的主节点参与之后的共识。领导节点由某高信誉值节点担任，可以保证其可信度。领导节点在节点组中随机产生，避免了恶意方买通最高信任节点从而操控共识过程，提高了作恶方成本。

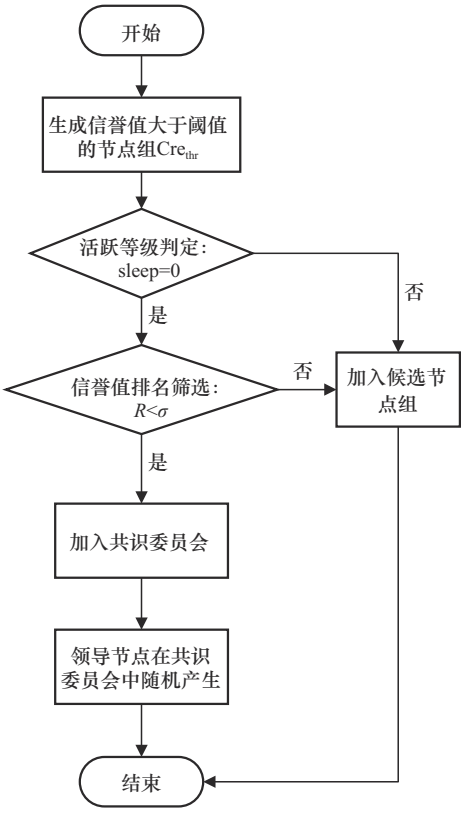


图4　共识委员会选择

相较于PBFT，由于其对共识规模的控制，AS-PBFT在共识时延需求小、交易频率大的大型网络中也能够有较好的表现。而在信任管理的车辆网络中，信誉值成为优良的过滤节点条件，使得在这样的车辆网络中部署AS-PBFT是可行的。具体的AS-PBFT共识流程如图5所示，其中详细地阐述了节点之间的消息传递过程，具体过程如下。

1) 当VBC需要产生新的区块时，在该区域内的L-RSU会根据VBC中在线车辆的信誉值与活跃情况确定共识委员会，并随机选定领导节点。其共识委员会规模R必须满足PBFT的恶意节点容错准则（$R > 3f + 1$）。L-RSU需要在共识开始前通告共识委员会中的各节点参与共识，各节点等待共识开始。

2) L-RSU向领导节点传递请求消息，领导节点对消息进行确认。

3) 领导节点向辅助节点发送预准备消息，各辅助节点验证成功后进入准备阶段。

4) 每个辅助节点向共识委员会中其他所有节

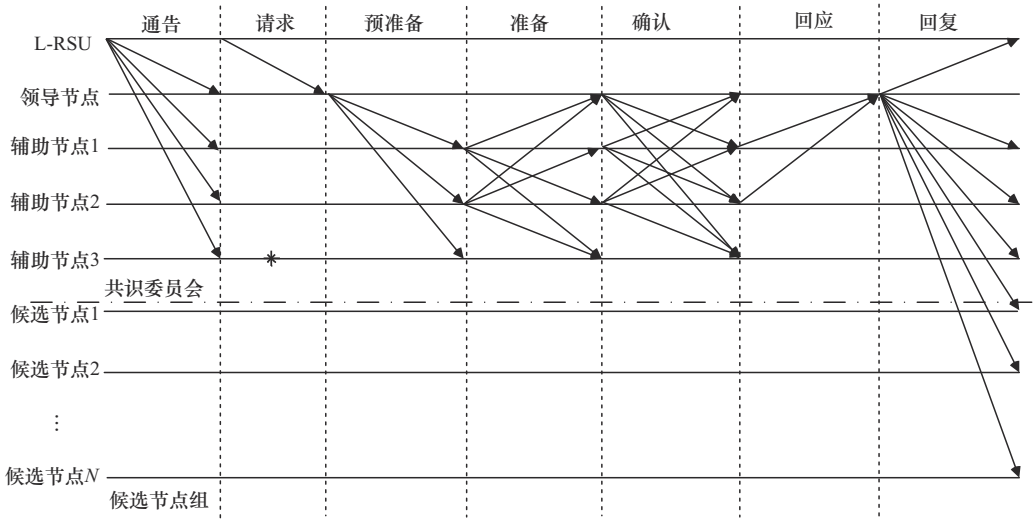


图5　AS-PBFT共识流程

点发送准备消息，如果消息得到验证，辅助节点将进入确认阶段。

5) 所有成功验证消息的辅助节点将回应消息传递给领导节点，以达成共识。

6) 当领导节点获得超过$3f+1$个确认消息后，则共识达成，领导节点需要将确认结果发送给VBC中的其他所有车辆节点，包括L-RSU。

2.4　驾驶员状态评估和信誉更新

2.4.1　人车匹配度

人车匹配度通过设置人车匹配度参数，分析驾驶员与车辆的匹配度。匹配度越高，则当前车辆更能体现出驾驶员的信任情况，驾驶员积累信誉也越快。

$$M_{(d_i,c_j)}=\frac{\mathrm{RDD}_m}{\mathrm{RDD}_{\mathrm{all}}} \tag{9}$$

其中，$M_{(d_i,c_j)}$表示在最近一段时间驾驶员d_i驾驶车辆c_j行驶距离RDD_m占驾驶员d_i驾驶所有车辆行驶距离$\mathrm{RDD}_{\mathrm{all}}$的比例。

2.4.2　活跃判定

本文方案设计了活跃判定策略，确保系统中的活跃驾驶员更有机会提升信誉值，并降低非活跃用户的影响。当上次更新时间间隔过久时，会将相关车辆标记为非活跃成员，车辆需要完成$\frac{N}{5}$信誉累计行为才能解除，其中N是近期信任表中的最大序数。

2.4.3　近期信任表

通过建立近期信任表，存储驾驶员最近的信誉历史，以便更快速、准确地更新驾驶员的信誉值，如表2所示，其代表着驾驶员d_i最近N次信誉累积情况。驾驶员具体信誉更新表达式为

$$\mathrm{PR}_{d_i}=\min\left(\frac{\sum_{n=1}^{N}\eta M_{(d_i,c_{j_n})}\mathrm{Cre}_{(j_n,t_n)}}{N},\mathrm{PR}_{\max}\right) \tag{10}$$

$$\eta=\begin{cases}\mathrm{e}^{-\lambda n}, & d_i\text{为活跃成员}\\ 0\ , & d_i\text{为非活跃成员}\end{cases} \tag{11}$$

其中，η表示信任衰减函数，历史轮次数越大的车辆信誉值占比应该越小，$\mathrm{PR}_{\max}$表示预设值设置的驾驶员信誉最大值。近期信任表可以避免恶意车辆的周期性攻击。

表2　　**驾驶员近期信任情况**

轮次	驾驶车辆	车辆信誉	匹配度	记录时间
1	c_{j_1}	$\mathrm{Cre}_{(j_1,t_1)}$	$M_{(d_i,c_{j_1})}$	t_1
2	c_{j_2}	$\mathrm{Cre}_{(j_2,t_2)}$	$M_{(d_i,c_{j_2})}$	t_2
⋮	⋮	⋮	⋮	⋮
N	c_{j_N}	$\mathrm{Cre}_{(j_N,t_N)}$	$M_{(d_i,c_{j_N})}$	t_N

2.4.4　DBC更新

L-RSU会持续收集共识信息，对驾驶员信誉值、人车匹配度等进行更新。当到达系统设置的DBC更新节点时，L-RSU将更新后的驾驶员信誉值、人车匹配度发送给T-RSU，然后删除本地信息，等待下阶段的信息存储。

值得注意的是，由于DBC链中的节点数量不多，且每个T-RSU节点信任度较高，因此链中每个节点轮流担任挖矿节点更新DBC。

3　安全性分析

3.1　恶意车辆攻击

1) 未注册用户攻击。指的是某些未在VBC中注册的驾驶员想要通过已注册车辆在DBC中进行恶意行为的攻击手段。当驾驶员首次注册时，人车注册信息 $\mathrm{Reg}_{d_i,c_j}=\{\mathrm{CID}_{d_i,c_j},N_0,P_{d_i},K_{d_i,c_j}\}$ 会被保存到DBC中，当未注册驾驶员 d_i' 想要驾驶车辆 c_j 并进入系统时，T-RSU会对 $\mathrm{ID}_{d_i'}$ 和 ID_{c_j} 进行认证，$\mathrm{CID}_{d_i',c_j}=H(\mathrm{ID}_{d_i'}\|\mathrm{ID}_{c_j}\|N_0)\neq H(\mathrm{ID}_{d_i}\|\mathrm{ID}_{c_j}\|N_0)$。因此当未注册驾驶员 d_i' 在未注册情况下直接进行认证时则会遭到T-RSU拒绝，进而无法与系统中的车辆进行信息交换。

2) 诽谤攻击。指恶意车辆在对其他车辆进行评价时故意评价较低得分，这会使车辆评分有失偏颇，本文方案中的诽谤攻击主要来自间接评价。假如有一组评价 $\mathrm{Eva}=\{\mathrm{Eva}_1,\mathrm{Eva}_2,\cdots,\mathrm{Eva}_n\}$，其中 Eva_i 表示第 i 个车辆对目标车辆的评价，L-RSU会计算这些评价的中位数作为大众评价 $\overline{\mathrm{Eva}}=\frac{1}{n}\sum_{i=1}^{n}\mathrm{Eva}_i$。当收集某个车辆 c_j 的间接评价 Eva_j 时，如果 $|\mathrm{Eva}_j-\overline{\mathrm{Eva}}|>\varepsilon_0$，则该条间接评价失效。L-RSU还会扣除诽谤者 c_j 的信誉值作为惩罚，而过低的信誉值会限制恶意车辆在系统中的活动。

3) 周期性开关攻击。恶意车辆为了避免被系统检测，会在保持正常行为一段时间后再进行周期性的恶意攻击。在系统中驾驶员信誉值更新的模块中，近期信任表的设置使恶意车辆通过等待时间降低上次恶意行为影响的做法失效。这是因为在近期信任表中，驾驶员信誉值的更新与时间新鲜度无关，只与 N 轮的更新轮次有关，驾驶员只有通过多次的诚实交互行为才能维持高信誉状态，这样的保护措施使得系统免受周期性攻击。

4) 黑洞攻击。当恶意车辆接收到消息后，保留或丢弃这些消息不传递给其他车辆。本文方案用二进制变量 $T_k=\{1(\text{传递消息}),0(\text{吞并消息})\}$ 表示车辆 c_k 的消息传递状态，假设车辆 c_k 在时间段 t 内的消息传递成功率为

$$T_i(t)=\frac{\sum_{k=1}^{N_i(t)}T_i^{(k)}}{N} \tag{12}$$

如果 $T_i(t)\leqslant\varepsilon_1$，即车辆消息在时间段 t 内传递成功率过低，那么这些黑洞车辆即一直拒绝消息传递的车辆，系统将其判定为可疑车辆，这些可疑车辆无法快速累计信誉值，且被限制参与系统活动。

3.2　妥协RSU攻击

本文方案中，L-RSU大量存在于系统中，往往是性能较一般的设备，其存在被恶意攻击的可能性，因此以下主要讨论的是半可信实体L-RSU受攻击的情况。

1) 数据篡改。被入侵的RSU往往想要篡改数据，如驾驶员信誉值、事务信息等，以达到恶意用户目的。在传统集中式系统中，被篡改的数据难以被发现，但在基于区块链的本文方案中，当某个 $\mathrm{L\text{-}RSU}_{a_0}$ 被攻陷后，想要篡改系统中的某些历史数据，其需要更改VBC链上数据。$G_{\mathrm{VBC}_a}=\{\mathrm{L\text{-}RSU}_{a_0},\cdots,\mathrm{L\text{-}RSU}_{a_p},c_{a_0},\cdots,c_{a_q}\}$ 为该区域 VBC_a 的所有节点，除非攻击者同时掌控超过 $\frac{p+q}{2}$ 个节点以上，否则多数正常节点在发现原区块链与被更改区块链存在差别后，会拒绝恶意RSU篡改数据的行为，苛刻的条件和高昂的成本会使攻击者望而却步。

2) 服务拒绝。当RSU被入侵后，入侵者可能通过拒绝服务的方式使L-RSU无法正常工作，从而影响车辆的通信和信誉值更新服务。T-RSU作为能力强大的可信实体，当附近L-RSU出现异常后，T-RSU会向同区域的其他L-RSU发送警告信息，暂时将受攻击L-RSU排除在系统运作外。

4　性能评估

4.1　仿真设置

为了对本文方案所提信誉评估算法的性能以及共识机制性能进行评估，本节在处理器为Intel（R）Core（TM）i5-11500、RAM为16 GB的Windows 10环境下进行仿真实验。仿真参数如表3所示。本文方案采用VEINS框架，该框架提供了一个强大的工具，在基于真实地图的街道场景中模拟车辆和通信设备的行为。仿真场景如图6所示，选取了重庆渝北某地段的OpenStreetMap地图，模拟了该地区存在5个L-RSU下的200辆车在一个DBC更新周期下的信誉积累过程。

表3　　仿真参数

参数	取值
仿真时间/s	300
车辆数量/辆	200
RSU数量/个	5
事故车辆/个	4
事故持续时间/s	10
仿真区域大小	2 000 m×3 000 m
消息传递范围/m	500
信号发射功率/mW	20
数据传输速率/(Mbit·s^{-1})	6
车辆天线高度/m	1.895
α_1	0.3
α_2	0.3
α_3	0.4
PR_{thr}	0.4
PR_{max}	1
λ	0.1
N	15
σ	20

图6　仿真场景

具体而言，本文方案利用SUMO软件将OpenStreetMap地图转换为OSM网格文件，利用Python模拟了所有车辆的路径流，使用Polyconvert工具将网络文件和OSM网格文件生成包含建筑物、绿地等地形特征的多边形文件。使用OMNET++模拟车辆之间的通信以及L-RSU计算车辆信誉的过程。针对AS-PBFT的性能检验，利用Docker容器和Fabric v0.6模拟多个节点的共识仿真过程。

图7为车辆发生事故后的消息传播场景，车辆节点20、节点40、节点60和节点80分别在仿真开始的15 s、30 s、45 s和60 s时发生事故，且每次的事故会持续10 s。事故会引发当事车辆以及附近目击车辆进行大量消息传递，进而更新车辆信誉情况。

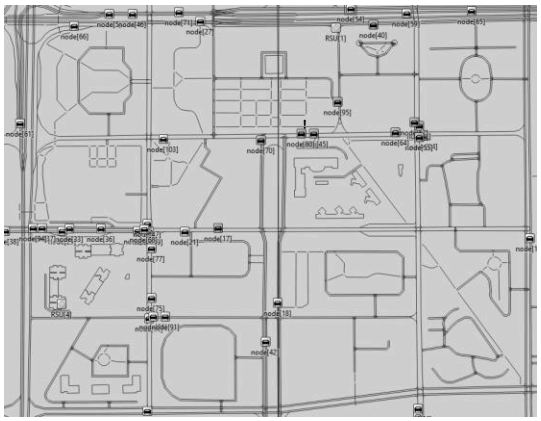


图7　车辆发生事故后的消息传播场景

4.2　驾驶员参数对信誉值积累影响

本文方案中引入了匹配度、活跃度等参数对驾驶员行为进行度量，这些参数为理解驾驶员行为对信誉值积累的影响提供了重要的量化指标。

人车匹配度matching用于衡量驾驶员在驾驶特定车辆时，该车的可信任程度。针对驾驶员做出正向行为积累信誉值的情况，本文方案通过改变matching大小，观察驾驶员信誉上涨速度，考察matching对信誉积累的影响。从图8中可以看到，当轮次为0时，各驾驶员的信誉值都是0.50。但是随着信誉的累积，当轮次为10时，matching=0.75的车辆驾驶员分别比matching=0.50与matching=0.25的车辆驾驶员的信誉值高出约15.9%和34.8%。因此，拥有更高matching的车辆拥有更高的可靠度，其驾驶员更容易累积信誉值，这表明系统中人车匹配度对信誉值积累有重要影响。

类似地，活跃度参数则反映了驾驶员在一段时间内参与系统的活跃度，活跃度高的驾驶员往往表现出更加积极的驾驶行为，可能更加注重安全和遵守规则，从而对信誉值的积累产生积极影响。通过

活跃度参数的引入，能够分析驾驶员行为的频率和稳定性，进一步理解其对信誉值的影响机制，为优化驾驶员行为提供数据支持。

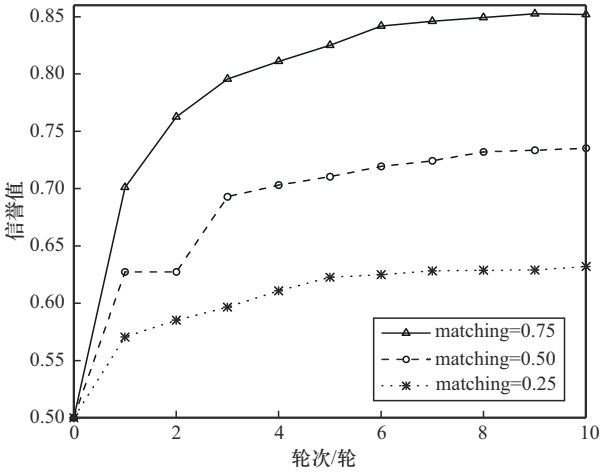


图8　人车匹配度对信誉值影响

本文方案将驾驶员的活跃度 sleepy 分为 3 级，sleepy 越小表示驾驶员的活跃度越高。由图 9 可以看到，sleepy=1 和 sleepy=2 的两位驾驶员通过同样的 10 次正向累积信誉值，在轮次为 10 时，其累积的信誉值分别比保持活跃度 sleepy=0 的驾驶员信誉值低 10.2% 和 26.1%，这是因其活跃度较低付出的代价。

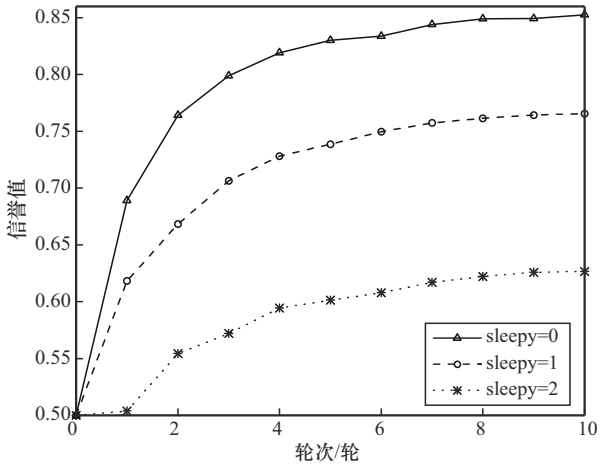


图9　活跃度对信誉值影响

4.3　恶意车辆识别性能分析

为了对系统恶意车辆识别性能进行分析，本文方案对 3 种模型在不同阈值下的恶意车辆检测率进行分析。除了本文方案外，对系统架构同为双层区块链的文献[14]与文献[25]进行了性能对比。文献[14]通过统计区块链货币的使用情况来衡量车辆信誉情况，但这种单一的评判标准无法得到准确的信誉值计算，而文献[25]采用了多因素信誉评价，但并未考虑车辆的历史信誉情况。在实验设置中，阈值越低，对恶意车辆的低信誉条件越苛刻，因此识别率也相对较低。如图 10 所示，在所有阈值区间内，本文方案的识别性能都明显优于其他 2 种方案，当阈值为 0.4 时，本文方案的恶意车辆识别率已经达到了 91.7%，高出其他 2 种方案 14.78% 和 39.53%，对恶意车辆进行了有效的识别，满足了一般的识别需求。当阈值为 0.45 时，本文方案的恶意车辆识别率已经达到 100%，但太高的阈值可能会导致诚实车辆被错误甄别。因此，本文方案的阈值设置为 0.4。

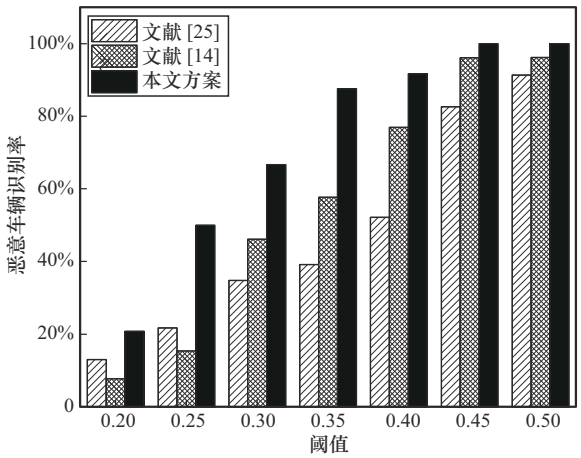


图10　恶意车辆识别性能对比

4.4　抗周期性攻击性能分析

为了分析本文方案的抗周期性攻击性能，本节对不同行为下驾驶员的信誉值变化进行了仿真。图 11 中展示了驾驶员信誉值在不同行为下的变化情况。这里针对系统的抗周期性攻击性能进行了分析，3 条线分别代表了驾驶员在正常行为、恶意行为及周期性攻击的情况下其信誉值的变化情况。本文方案没有采取大多数信任模型中的时间因子以减轻以往的恶意行为对信誉计算的影响，取而代之的是通过引入驾驶员近期信任表的方式更新驾驶员信誉。近期信任表中用更新轮次参数取代了时间参数，这意味着恶意驾驶员并不能通过拉长时间周期来减轻过去恶意行为的影响。因此，系统中的车辆必须保持自己的诚实交互行为才能使自己保持在一个高信誉状态。

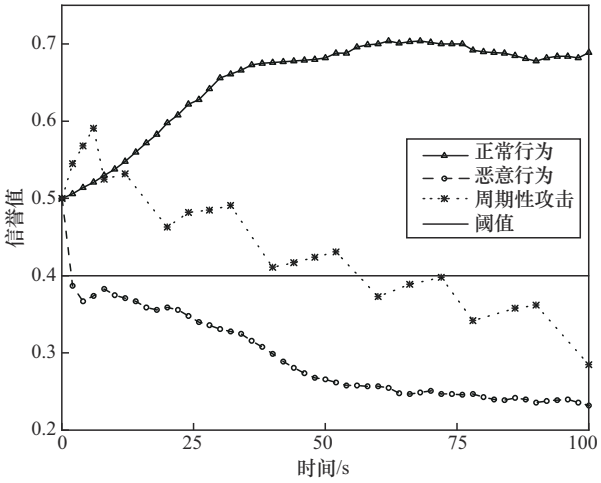


图11　驾驶员信誉值在不同行为下的变化情况

4.5　共识机制性能分析

为了对共识机制的性能进行分析，本文在同样的环境下对AS-PBFT与PBFT进行了性能比较。图12为VBC中运用PBFT与AS-PBFT的共识时间对比。节点数量被设置为4到80，目的是检验共识算法受规模影响的程度。受益于AS-PBFT中对低信誉值节点的两次过滤，这使得其共识规模始终保持在一个合理的范围，因此AS-PBFT的共识时间始终保持在较低的值，如图12所示，随着节点数量的增多，AS-PBFT算法的共识时间维持在5 s左右。相比之下，传统的PBFT在节点数量增大时，其共识时间会剧烈上升。因此，AS-PBFT在大规模节点环境下的共识性能明显优于PBFT。

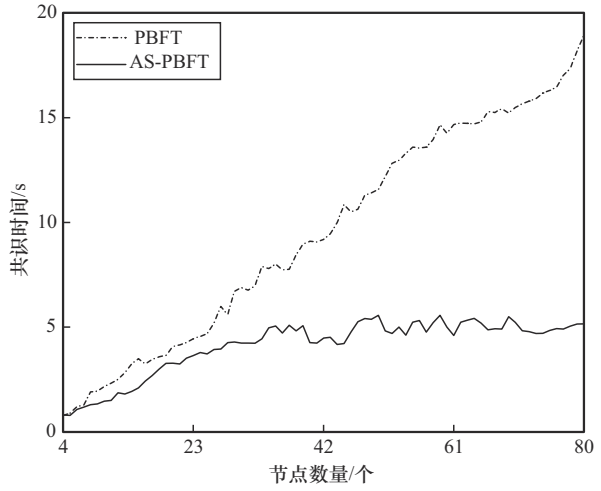


图12　共识时间对比

5　结束语

本文方案以人车分离的信任管理系统为核心，围绕着身份认证、数据共享和信誉评价、安全性分析与仿真验证等展开了设计和探讨。采用基于密钥与生物特征的双重认证机制，确保驾驶员身份及车辆信息的准确性和安全性；设计了包含信息质量评价机制、直接交互评价和间接交互评价的多层次信誉评价模型，保障数据的可靠性和驾驶员的信誉存储和更新；通过对驾驶员行为参数的量化分析，建立了驾驶员行为对信誉值的影响机制；考虑了可能的恶意车辆攻击和妥协RSU攻击，并提出了相应的防御策略和安全措施；最后通过仿真和实验数据验证了系统的有效性。

总体而言，本文方案在智能交通系统中建立了一个完善的信任管理体系，实现了对驾驶员身份认证、数据共享与信誉评价的全面管理和控制，为智能交通系统的安全运行和信誉建设提供了有效的技术支持和保障。然而，更多的规则约束与更繁杂的信息交换可能会使节点的参与积极性不高。因此，在未来的研究中，模型将引入激励机制以提高节点的合作性。

参考文献：

[1] HE R S, SCHNEIDER C, AI B, et al. Propagation channels of 5G millimeter-wave vehicle-to-vehicle communications: recent advances and future challenges[J]. IEEE Vehicular Technology Magazine, 2020, 15(1): 16-26.

[2] SHARMA S, MOHAN S. Cloud-based secured VANET with advanced resource management and IoV applications[C]//Connected Vehicles in the Internet of Things. Berlin: Springer, 2020: 309-325.

[3] YEONG D J, VELASCO-HERNANDEZ G, BARRY J, et al. Sensor and sensor fusion technology in autonomous vehicles: a review[J]. Sensors, 2021, 21(6): 2140.

[4] SUMALEE A, HO H W. Smarter and more connected: future intelligent transportation system[J]. IATSS Research, 2018, 42(2): 67-71.

[5] VEGNI A M, LOSCRÍ V. A survey on vehicular social networks[J]. IEEE Communications Surveys & Tutorials, 2015, 17(4): 2397-2419.

[6] WU W F, LI R F, XIE G Q, et al. A survey of intrusion detection for in-vehicle networks[J]. IEEE Transactions on Intelligent Transportation Systems, 2020, 21(3): 919-933.

[7] SUN Z B, LIU R Z, HU H T, et al. Cyberattacks on connected automated vehicles: a traffic impact analysis[J]. IET Intelligent Transport Systems, 2023, 17(2): 295-311.

[8] LI Q, MALIP A, MARTIN K M, et al. A reputation-based announcement scheme for VANETs[J]. IEEE Transactions on Vehicular Technology, 2012, 61(9): 4095-4108.

[9] HU H, LU R X, ZHANG Z H, et al. REPLACE: a reliable trust-based platoon service recommendation scheme in VANET[J]. IEEE Transactions on Vehicular Technology, 2017, 66(2): 1786-1797.

[10] HUO R, ZENG S Q, WANG Z H, et al. A comprehensive survey on blockchain in industrial Internet of things: motivations, research progresses, and future challenges[J]. IEEE Communications Surveys & Tutorials, 2022, 24(1): 88-122.

[11] SINGH P K, SINGH R, NANDI S K, et al. Blockchain-based adaptive trust management in Internet of vehicles using smart contract[J]. IEEE Transactions on Intelligent Transportation Systems, 2021, 22(6): 3616-3630.

[12] 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.

[13] AHMAD F, KURUGOLLU F, KERRACHE C A, et al. NOTRINO: a novel hybrid trust management scheme for Internet-of-vehicles[J]. IEEE Transactions on Vehicular Technology, 2021, 70(9): 9244-9257.

[14] 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(2): 1209-1223.

[15] DIALLO E H, DIB O, AGHA K A. An improved PBFT-based consensus for securing traffic messages in VANETs[C]//Proceedings of the 2021 12th International Conference on Information and Communication Systems (ICICS). Piscataway: IEEE Press, 2021: 126-133.

[16] LIU Z, LIWANG M H, HOSSEINALIPOUR S, et al. RFID: towards low latency and reliable DAG task scheduling over dynamic vehicular clouds[J]. IEEE Transactions on Vehicular Technology, 2023, 72(9): 12139-12153.

[17] SUO D J, MO B C, ZHAO J H, et al. Proof of travel for trust-based data validation in V2I communication[J]. IEEE Internet of Things Journal, 2023, 10(11): 9565-9584.

[18] CHEN X, XUE G L, YU R Z, et al. A vehicular trust blockchain framework with scalable Byzantine consensus[J]. IEEE Transactions on Mobile Computing, 2024, 23(5): 4440-4452.

[19] TU S S, YU H Y, BADSHAH A, et al. Secure Internet of vehicles (IoV) with decentralized consensus blockchain mechanism[J]. IEEE Transactions on Vehicular Technology, 2023, 72(9): 11227-11236.

[20] LV C C, CHEONG C, CAO Y, et al. Leveraging geographic information and social indicators for misbehavior detection in VANETs[J]. IEEE Transactions on Consumer Electronics, 2024, 70(1): 4411-4424.

[21] 付子旺, 刘峰, 齐佳音. 基于区块链技术的共享经济的研究：以共享汽车业务为例[C]//中国自动化大会(CAC2020)论文集. [出版地不详:出版者不详], 2020: 16-23.
FU Z W, LIU F, QI J Y. Research on sharing economy based on block chain technology: take car sharing business as an example[C]//The Chinese Congress of Automation(CAC2020). [S.l.: s.n.], 2020: 16-23.

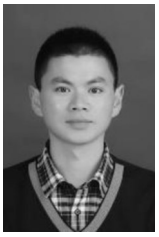
[22] LIAO F C, MOLIN E, TIMMERMANS H, et al. Carsharing: the impact of system characteristics on its potential to replace private car trips and reduce car ownership[J]. Transportation, 2020, 47(2): 935-970.

[23] SARKAR A, SINGH B K. A review on performance, security and various biometric template protection schemes for biometric authentication systems[J]. Multimedia Tools and Applications, 2020, 79(37): 27721-27776.

[24] 张文波, 黄文华, 冯景瑜. 基于无证书签密的车联社会网络安全通信机制[J]. 通信学报, 2021, 42(7): 128-136.
ZHANG W B, HUANG W H, FENG J Y. Secure communication mechanism for VSN based on certificateless signcryption[J]. Journal on Communications, 2021, 42(7): 128-136.

[25] RUAN W B, LIU J, CHEN Y F, et al. A double-layer blockchain based trust management model for secure Internet of vehicles[J]. Sensors, 2023, 23(10): 4699.

[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。

黄泓龙（2000– ），男，重庆人，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。

李方伟（1960– ），男，重庆人，博士，公共大数据安全技术重庆市重点实验室教授，主要研究方向为下一代无线通信系统的关键技术、移动通信安全、时间反演等。

徐勇军（1986– ），男，湖北赤壁人，博士，重庆邮电大学教授、博士生导师，主要研究方向为反向散射通信、智能反射表面、通感一体化等。