车联网交互信息控制传输与安全共享方案

王樊[1]，代玥玥[1]，杨慧炅[2]，王秀华[1]，卢云龙[3]
（1. 华中科技大学网络空间安全学院，湖北 武汉 430074；2. 香港理工大学电子计算学系，香港 999077；
3. 北京交通大学电子信息工程学院，北京 100044）

摘　要：在车联网中应用联盟链实现道路交通观测信息管理，可以兼顾公有链的去中心化和私有链的高效特性，提升车辆间通信的透明度。然而，现有方案没有充分考虑恶意车辆和恶意路侧单元（RSU, road side unit）节点传播虚假信息的风险，可能导致城市交通瘫痪和事故。此外，海量车辆数据和重复事件报告传输增加了计算和通信开销，影响了系统的可行性与可扩展性。针对上述问题，提出了针对车联网场景中交互信息的控制传输与高效安全共享方案。首先，设计了基于角度差自变换区域码的信息传输控制策略，该策略通过设定车辆区域码距离的阈值限制信息的转发量，并采用 Bloom Filter 对信息进行过滤，减少冗余信息的传输。其次，建立了基于诚信分的管理机制以应对恶意节点传播虚假信息对系统的破坏。最后，提出了动态管理多主节点 Hotstuff（DMML-Hotstuff, dynamically manage multiple leader Hotstuff）共识算法，有效解决了单主节点性能瓶颈问题，并通过动态节点调整提高了系统吞吐量和拜占庭容忍度。仿真结果表明，所提方案相比现有方案减少了 23% 和 39% 的车辆信息传输量，并能实时评估诚信分，快速识别并隔离恶意节点。在共识算法方面，与 3 种主流拜占庭容错算法相比，吞吐量分别提高了 19%、52% 和 188%。

关键词：车联网；联盟链；共识算法；诚信分机制
中图分类号：TN929.08
文献标志码：A
doi：10.11959/j.issn.2096−3750.2025.00480

Vehicle networking interactive information control transmission and security sharing scheme

WANG Fan[1], DAI Yueyue[1], YANG Huijiong[2], WANG Xiuhua[1], LU Yunlong[3]
1. School of Cyber Science and Engineering, Huazhong University of Science and Technology, Wuhan 430074, China
2. Department of Computing, Hong Kong Polytechnic University, Hong Kong 999077, China
3. School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing 100044, China

Abstract: The application of alliance chain in vehicle networking to achieve road traffic observation information management can take into account the decentralization of public chain and the efficient characteristics of private chain, and improve the transparency of communication between vehicles. However, existing schemes do not adequately consider the risk of malicious vehicles and malicious road side unit (RSU) nodes spreading false information, which can lead to urban traffic paralysis and accidents. In addition, the transmission of massive vehicle data and repeated incident reports increases the computing and communication overhead, which affects the feasibility and scalability of the system. Aiming at the above problems, a control transmission and efficient and secure sharing scheme for interactive information in the vehicle-connected scene was proposed. Firstly, an information transmission control strategy based on angular difference self-transforming area code was designed. The amount of information forwarded was limited by setting the threshold of

收稿日期：2025−02−07；**修回日期：**2025−03−11
通信作者：代玥玥，yueyuedai@hust.edu.cn
基金项目：国家自然科学基金委员会青年科学基金资助项目（No. 62201219）；湖北省自然科学基金计划项目（No. 2025AFB572）
Foundation Items: National Natural Science Foundation Committee, Youth Science Fund Project (No. 62201219), Hubei Provincial Natural Science Foundation Program (No. 2025AFB572)

vehicle area code distance, and Bloom Filter was adopted to filter information to reduce the transmission of redundant information. Secondly, a management mechanism based on credit points was established to deal with the damage to the system caused by malicious nodes spreading false information. Finally, the DMML-Hotstuff (dynamically manage multiple leader Hotstuff) consensus algorithm was proposed, which effectively solved the performance bottleneck of single master node. The system throughput and Byzantine tolerance were improved by dynamic node adjustment. The simulation results show that the proposed scheme reduces the vehicle information transmission by 23% and 39% compared with the existing methods, and can evaluate the credit score in real time and quickly identify and isolate malicious nodes. In terms of consensus algorithms, the throughput is improved by 19%, 52% and 188%, respectively, compared to the three mainstream Byzantine fault-tolerant algorithms.

Key words: Internet of vehicle, alliance chain, consensus algorithm, reputation mechanism

0　引言

随着智能感知设备和内置传感器的广泛使用，车联网[1]正加速迈向高度智能化与自动化。通过实现车辆之间的高效通信与实时的道路交通信息共享，车联网不仅优化了交通流量、提升了驾驶安全性，也为智能交通系统提供了强大的数据支持和技术保障。

车联网通常采用传统的集中式服务器来管理车辆身份和道路交通数据等信息[2]，但这种架构存在显著的安全隐患。信息可能面临泄露或篡改的风险，不仅威胁用户隐私，还可能被不法分子利用实施恶意攻击（如伪造车辆身份或干扰交通系统）对交通安全构成严重威胁[3]。此外，集中式架构存在单点故障风险，一旦服务器遭受攻击或崩溃，整个系统的运行可能陷入瘫痪，严重影响车联网的稳定性和可靠性。

区块链作为一种分布式技术[4]，其去中心化的特性为改进车联网的集中式管理提供了完善方案[5-6]。然而，区块链和车联网的开放性特点使其仍面临着恶意车辆传播虚假道路交通观测信息的风险[7]。此外，车辆向路侧单元（RSU, road side unit）节点上传的海量交通数据使区块链面临共识效率低下的问题，而其中大量重复的交通事件报告则进一步浪费了宝贵的网络资源[8]。这些因素严重影响了车联网系统的安全性，并阻碍了交通信息在车联网中的高效共享与处理。

信誉管理，由于其可追溯性和多维性的特点，被认为是提高车联网中实体交互效率以及维护系统安全性和可靠性的一种有效方法。文献[9]提出了一种基于区块链的分布式信誉管理系统，可有效对抗举报活动中的攻击和自私行为。文献[10]建立了一种基于区块链的分布式信任管理机制来解决车辆命名数据网络（V-NDN, vehicular named data networking）中的恶意节点问题，该方案中车辆会根据车辆信誉值和消息本身的特征来判断接收消息的可信度。文献[11]提出了一种基于双层区块链的分布式信誉评估与管理模型，用于增强车辆自组网络的安全性。文献[12]提出了一种基于区块链的分布式信誉系统，该系统可确保参与者的隐私，为联网和自动驾驶汽车提供安全和弹性的信誉计算。文献[13]提出了一种基于区块链的去中心化信任管理系统，允许车辆直接广播共享信息。尽管区块链的抗篡改性很大程度上促进了车联网中信息安全共享的研究，但现有研究往往未充分考虑区块链在实时更新方面的需求以及车辆快速变换位置和海量信息传输对系统性能的影响[14-17]，也没有考虑恶意车辆或恶意RSU节点共享错误信息可能导致导航错误、紧急制动故障等问题。

由于车联网中存在海量的道路交通信息交互，网络拥塞成为潜在问题。目前，相关研究方案大致可分为两类。第一类是通过减少数据传输延迟和增加信道容量等手段来提升网络信道的质量。LACC[18]是一种通信拥塞控制协议，采用线性整数规划方法来选择车辆中的邻居，而非传统的贪婪算法。然而，LACC的设计主要针对短距离数据传输。Luo等[19]提出了一种结合5G和车联网的软件定义协同架构，并基于图论设计了数据共享算法，以提升数据共享性能。另一种方法是通过降低源节点的数据生成速率，从而减轻网络流量负担。Zhuang等[20]提出了一种拥堵自适应数据收集方案，该方案根据拥堵程度动态调整数据生成速率。此外，还分析了拥塞控制对数据精度的影响。Mohammed等[21]通过指数函数调整消息速率，设计去中心化拥塞管理系统，缓解车联网中的信道拥堵问题。然而，大多数改善网络通

道的方案效果有限，难以有效实现。同时，降低数据生成速率在保证交通数据准确性和覆盖范围方面也面临挑战。

区块链和联盟链的主要区别在于网络的去中心化程度和参与权限。区块链通常是公开且完全去中心化的，任何人都可以参与并验证交易。然而，在车联网这种数据量巨大、实时性要求高的应用场景中，区块链可能面临性能瓶颈，如交易吞吐量低和网络延迟高。相比之下，联盟链在确保一定程度去中心化的同时，可以灵活地控制节点权限和共识机制，从而有效提升系统性能，减少网络延迟，并更好地保护数据隐私。此外，联盟链的访问控制和节点认证机制使其能够有效防范恶意节点攻击，提供更高的安全性和系统稳定性。车联网中运用联盟链的原因在于，车联网涉及多个行业和企业的合作，参与方之间需要共享信息，但又必须保护敏感数据，如车辆位置、驾驶行为等。联盟链能够提供更强的隐私保护，同时确保各方之间的信任和数据共享，从而满足车联网对高效、安全的需求[22-24]。

联盟链通过共识机制加速达成交通信息的一致性。目前存在多种共识算法，例如，工作量证明（PoW, proof of work）[25]，其要求参与者进行适当耗时且复杂的计算工作，通过解决一个数学难题（如寻找特定哈希值）来竞争新区块的生成权。权益证明（PoS, proof of stake）[25]则是根据参与者持有的代币数量来决定其参与共识的权重。意见证明（PoO, proof of opinion）[26]是一种基于用户意见或投票来达成共识的机制，网络节点可以通过表达对特定提案或数据的看法来参与共识过程。上述非拜占庭容错共识算法通常依赖于固定或可信的节点参与共识，而车联网中的节点具有高动态性和不确定性，节点之间的信任关系不稳定，很难建立长期可信的节点集，这种信任假设在车联网场景下不够现实。实用拜占庭容错（PBFT, practical Byzantine fault tolerance）[27]共识算法是一种面向分布式系统的容错算法，设计用于在存在恶意节点的情况下实现系统的一致性和可靠性。PBFT通过引入多个节点的参与和投票来达成共识，能够容忍最多$(N-1)/3$个恶意或故障节点（其中N是节点总数）。文献[28]提出的HotStuff算法通过将PBFT算法的平均通信复杂度从$O(n^2)$优化至$O(n)$，有效地解决了传统PBFT共识算法在系统规模扩大时遇到的性能降低问题。文献[29]中提到的CBFT是一种多主节点共识算法，每个主节点在其分配的分区内独立完成一个PBFT实例以提高系统的吞吐量和可扩展性。上述拜占庭容错算法在增强区块链网络的安全性、可扩展性和效率方面起着至关重要的作用[30]。车联网需要实时同步海量道路交通信息，而现有的拜占庭容错共识方案可能面临性能瓶颈，导致信息交互延迟较高。此外，这些方案往往忽视恶意节点的检测，未能及时消除破坏联盟链安全的恶意节点，因此上述拜占庭容错共识算法在车联网场景下效果欠佳。

针对以上问题，本文提出车联网交互信息控制传输与高效安全共享方案。本文具体贡献如下。

1) 针对车联网中大规模道路交通观测信息传输及冗余信息引发的网络拥塞问题，本文提出了一种高效的角度差自变换区域码信息传输控制策略。这一策略具有较强的针对性，能够有效管理信息流。首先，通过设定车辆区域码距离的阈值，有效限制信息的转发范围。同时，引入动态的地理和角度因素，使得信息传播的控制更加精确，避免了不必要的广播，从而有效缓解网络拥塞。其次，利用空间效率极高的Bloom Filter概率数据结构，快速判断元素是否属于某个集合，从而有效检测并过滤冗余交通信息，最大限度地减少车辆间冗余交通信息的传输。

2) 针对恶意节点传播虚假交通信息的问题，本文提出了一套覆盖车辆和RSU两类实体的诚信分管理机制，旨在保护车联网的可信环境。该系统通过分析参与实体的历史行为，能够动态评估并有效管理车辆节点的诚信状况，同时确保RSU在安全可控的范围内运行。对于传播虚假或误导信息的恶意节点，系统将采取惩罚或隔离措施，进一步维护车联网的可靠性与安全性。

3) 针对联盟链节点在处理海量交通信息时难以实现高效共识并存在性能瓶颈的问题，本文提出了动态管理多主节点HotStuff（DMML-HotStuff, dynamic management multiple leader HotStuff）共识算法。该算法设置多个主节点以流水线形式进行共识，解决传统共识算法单主节点性能瓶颈问题。对于恶意共识节点，本文通过诚信分高低动态调整共识节点集群，能够及时发现并剔除拜占庭节点，并将诚实节点加入共识集群中，以此增强联盟链的稳定性。此外，本文根据系统交易量的变化动态调整共识节点数量，以更适应系统吞吐量的需要。

1　系统模型

为解决车联网中恶意节点传播虚假交通信息及冗余信息导致的联盟链共识效率低下和网络拥塞问题，本文提出利用诚信分管理机制抑制恶意节点影响，采用基于角度差自变换区域码的信息传输控制策略降低传输量，并结合 Bloom Filter 减少冗余信息，最后通过设计 DMML-HotStuff 共识算法提升共识效率。系统模型如图 1 所示，本文研究构建的系统架构主要包含两类实体：车辆以及 RSU。两类实体均持有由证书授权（CA, certificate authority）机构颁发的证书，且所有实体间的交互均通过椭圆曲线 ElGamal 加密和签名技术[31]进行处理，以确保信息传输的机密性和完整性。

1) 车辆：参与车联网中的车辆是拥有先进计算和通信功能的智能移动节点。在本文研究的车联网模型中，车辆依据其功能划分，担任两种角色——信息提供车辆（IPV, information provide vehicle）和信息评分车辆（ISV, information scoring vehicle）。随着情境的变化，同一辆车可以同时充当两种角色。IPV 有责任积极地收集和汇报交通信息，ISV 便以其接收到的信息为基础，对信息可信度进行评分。

2) RSU：RSU 存储系统中海量信息以及维护诚信分系统的完整性，同时是联盟链中的共识节点。

当 IPV 采集到信息后利用 Bloom Filter 过滤冗余信息，然后借助先进的 第五代车联网（5G-V2X, 5th generation vehicle-to-everything）技术，并利用角度差自变换区域码信息传输控制策略向选定的 ISV 及 RSU 传递关键信息。ISV 在接收到信息后对其可信度进行评分，之后将评分结果发送给距离区域码最近的 RSU。若 RSU 收到来自 IPV 采集的信息，利用 Bloom Filter 过滤冗余信息，随后将处理后的信息安全地存储于本地，并将信息索引上传至联盟链，这样在降低联盟链存储负担的同时，也提升了信息检索的效率与安全性。若 RSU 接收到来自 ISV 的评分反馈，则将汇总处理这些评分，并将转换后的诚信分上传至联盟链。联盟链采用 DMML-HotStuff 共识算法，高效地对这些信息进行共识。当有车辆需要请求相关信息时，可以根据联盟链上的诚信分高低有选择性地向 RSU 请求获得。

2　系统设计

2.1　角度差自变换区域码信息传输控制方案

车联网中海量的道路交通信息传输对系统实时性的要求和性能瓶颈带来了严峻的挑战，现有的提升网络通信效率方案往往受限于实施难度，难以达到预期效果。因此本文提出一种角度差自变换区域码信息传输控制方案以高效地降低网络信息传输量。

首先，将一块地理位置划分成 m 个区域，其中第 k 个区域可以用 $\text{area}_k\,(k = 1, 2, 3, \cdots, m)$ 表示。每个区域有若干个车辆，假设该道路上一共有 n 辆小车，记为 $v_i\,(i = 1, 2, 3, \cdots, n)$。不同区域内的车辆或 RSU 会被赋予一串二进制编码，该编码代表着车辆或 RSU 的身份信息，每一个二进制串由区域码和

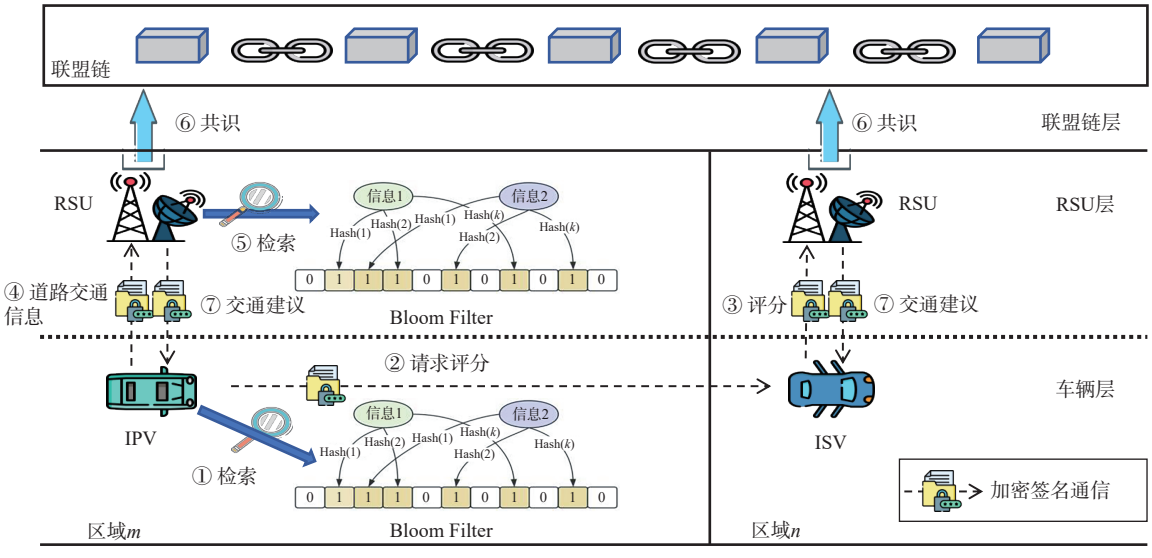


图 1　系统模型

车辆码（或RSU码）组成。

在系统初始化阶段，每辆车和RSU都有一张所有车辆编码表和RSU编码表，在每一个编码尾部都有一个是否活跃标志位。若有小车新进入该区域，小车会向该区域的中央RSU请求初始化参数，中央RSU将响应小车初始角度α和车辆编码。车辆区域码是不断更新的，角度差自变换区域码如图2所示，若车辆v_i在区域area_1中，经过一段时间后到达区域area_2，在此时间段v_i行驶的距离是s_0，v_i每隔一定时间会向道路中央RSU发送消息，以计算此时车辆与RSU的距离，v_i分别在area_1和area_2计算出的距离是s_1和s_2，利用式(1)和式(2)计算出角度差β

$$\cos\beta = \frac{s_1^2 + s_2^2 - s_0^2}{2 \times s_1 \times s_2} \tag{1}$$

$$\beta = \arccos(\cos\beta) \tag{2}$$

随后，按照式(3)计算出车辆最新角度α'

$$\alpha' = (\alpha + \omega \times \beta + 360) \bmod 360 \tag{3}$$

其中，ω是车辆行驶方向，当车辆上的方向感知器判定方向为顺时针时$\omega = 1$，为逆时针时$\omega = -1$。区域码$\text{code}_{\text{area}}$将按照式(4)进行更新

$$\text{code}_{\text{area}} = \left\lfloor \frac{\alpha' \times m}{360} \right\rfloor \tag{4}$$

当车辆更新完区域码后，会在编码表中搜索距离区域码最近且活跃的RSU共识节点RSU_a，并向其请求车辆编码列表$\text{list}_{\text{code}}$和Bloom Filter，同时接收到车辆请求的RSU会更新车辆编码列表并向其他RSU广播更新后的列表。车辆编码列表存储了实时车辆编码信息，便于IPV查找ISV以共享信息。Bloom Filter存储了现有信息的hash映射位，车辆可以高效地判断自己收集的信息是否已经被其他车辆上传至RSU。由于车辆密集且移动轨迹相似，不同IPV有可能重复上传相同信息，从而不可避免地增加网络通信的负载和系统运行的开销。因此当IPV采集到信息后，首先会在Bloom Filter中检索是否已存在相同信息（通过不同hash函数映射后对应位均为1），若存在，则会将其删除后再打包其他信息上传至RSU_a。当RSU接收到来自IPV的信息后，会将该信息在本地Bloom Filter中检索。如果检测到信息重复，该信息不会被打包存储，反之，该信息会被打包存储至RSU本地，并将信息索引（包含对此信息的评价结果）上传至协调节点进行共识，当有车辆需要请求相关信息时，可以根据联盟链上的评价结果有选择性地向RSU请求获得。具体而言，Bloom Filter的假正率（将本不存在于集合中的元素判定为已存在于集合中）决定了过滤的准确性，假设Bloom Filter使用q位长度的二进制比特位（$q \in Q$, Q为所有二进制位的集合）和k个独立的hash函数，那么插入u个元素（$u \in U$, U为所有插入位的集合）后对应位仍为0的概率如式(5)所示

$$P_0(u) = (1 - \frac{1}{q})^{ku} \tag{5}$$

因此对应位被设置为1的概率如式(6)所示

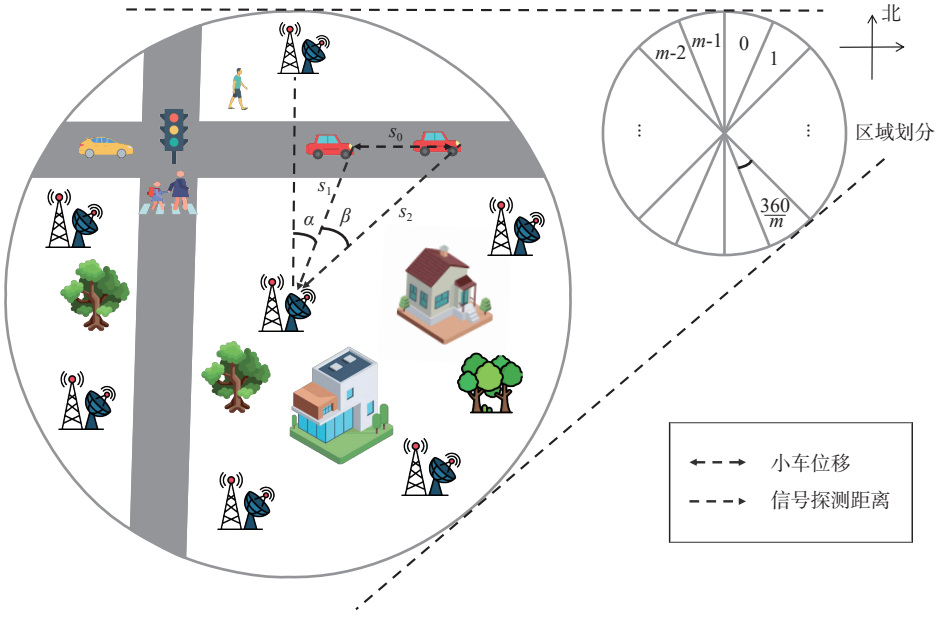


图2　角度差自变换区域码

$$P_1(u)=(1-(1-\frac{1}{q})^{ku})^k \tag{6}$$

当$U \ll Q$时，假正率如式(7)所示

$$\begin{aligned}P^+&=(1-\frac{|U|}{|Q|})P_1(u)=\\&(1-\frac{|U|}{|Q|})(1-(1-\frac{1}{q})^{ku})^k\approx(1-e^{\frac{-ku}{q}})^k\end{aligned} \tag{7}$$

由于车联网中不同的车辆和RSU都有一份Bloom Filter且伴有Bloom Filter的传输共享，系统整体误判率如式(8)所示

$$\begin{aligned}&E(\overline{P^+})=\prod_{i=1}^{n}(E((1-\frac{|U|}{|Q|})(P_1(u)-\delta_1)^k+\\&\sum_{i=1}^{k}\binom{k}{i}\delta_0{}^i(P_1(u)-\delta_0)^{k-i}))=\\&\prod_{i=1}^{n}(E((P_1(u)-\delta_1)^k-\frac{|U|}{|Q|}(P_1(u)-\delta_0)^k))=\\&\prod_{i=1}^{n}(E((P_1(u)+\delta_0-\delta_1)^k-\\&\frac{|U|}{|Q|}(P_1(u)-\delta_1)^k))\approx(p^+)^n\end{aligned} \tag{8}$$

其中，δ_0和δ_1分别代表传输时比特位从1变为0和从0变为1的概率，一般δ_0和δ_1的值非常小，因此在本文中不加以考虑。从式(8)可以得到，系统整体误判率极低，从而有效保证了信息过滤的准确性。其次，IPV将采集到的信息发送给多个ISV进行评分，然而，信息共享的过程若不加以控制，会给网络通信带来很大负荷。为了有效降低这一载荷并提升信息共享效率，本文采用的策略是：IPV只会把收集到的信息发送给区域码距离在阈值内的ISV，车辆之间区域码距离如式(9)所示

$$d(i,j)=\mathrm{code}_{\mathrm{area}}^{v_i}\oplus\mathrm{code}_{\mathrm{area}}^{v_j}\bmod m \tag{9}$$

其中，$\mathrm{code}_{\mathrm{area}}^{v_i}$和$\mathrm{code}_{\mathrm{area}}^{v_j}$分别表示$v_i$和$v_j$的区域码。这样不仅显著减少了整个车联网中信息传输的次数和距离，还意味着由于地理位置的接近，这些信息更能直接反映出相关区域的真实和即时交通情况。因此，相对于那些远距离的接收者，信息的时效性和可信度更高。

2.2　车辆诚信分模型

诚信分管理有助于车辆高效地判断信息来源的可靠性，对此，本文创建了一套车辆诚信分管理机制。车辆诚信分模型如图3所示。车辆v_i和车辆v_j之间发送消息格式如式(10)所示

$$\begin{aligned}&\mathrm{msg}(v_i\rightarrow v_j)=\\&E_{\mathrm{sk}_{v_i}}\{\mathrm{serial},\mathrm{type},\mathrm{event},\mathrm{IPVcode},\mathrm{ISVcode},t\}\end{aligned} \tag{10}$$

其中，$E_{\mathrm{sk}_{v_i}}$代表v_i的私钥，serial代表发送消息的序列号，type代表消息类型（发送或者回复），event代表事件，IPVcode代表信息提供车辆编码，ISVcode代表信息评判车辆编码，t代表时间戳。当v_j完成对v_i的评价之后，v_j将对v_i的评价结果发送给RSU，消息格式如式(11)所示

$$\begin{aligned}&\mathrm{msg}(v_j\rightarrow\mathrm{RSU})=E_{\mathrm{sk}_{v_j}}\{\mathrm{serial},\mathrm{type},\mathrm{event},\\&\mathrm{result},\mathrm{IPVcode},\mathrm{ISVcode},t\}\end{aligned} \tag{11}$$

其中，$E_{\mathrm{sk}_{v_j}}$代表v_j的私钥，result代表ISV给IPV的评价结果。ISV评判IPV提供的信息得分如式(12)和式(13)所示

$$S=I+e^{-\lambda(d+t)} \tag{12}$$

$$t=t_{\mathrm{end}}-t_{\mathrm{start}} \tag{13}$$

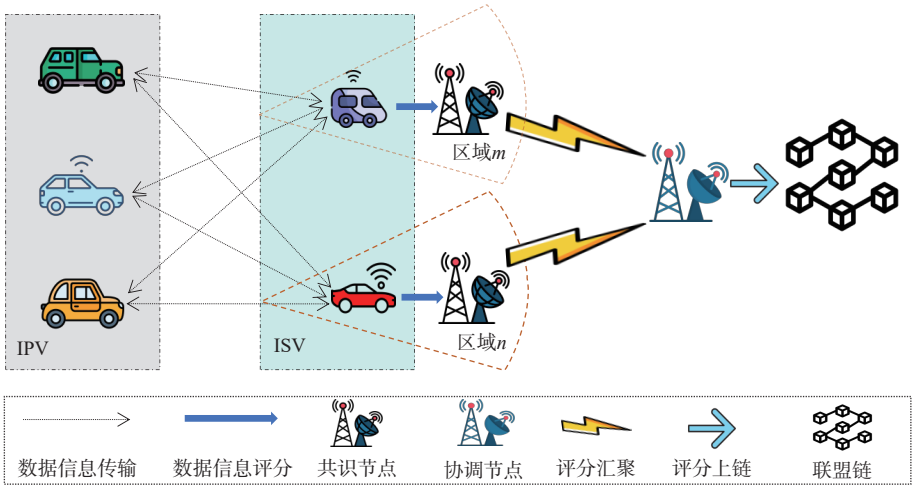


图3　车辆诚信分模型

其中，S是单个ISV评分情况，I是诚信分初始值，λ是诚信分变化率，d是IPV和ISV之间的区域编码距离，t表示提供消息的实时性，t_{start}表示事件起始时间，t_{end}表示事件信息提供时间。当信息评判车辆v_j针对该事件收到信息集合$E=\{e_1,e_2,e_3,\cdots,e_l\}$，$l$是收集到的信息数量，每个IPV仅能提供一份信息且每条信息的提供是相互独立的，ISV根据式(8)和式(9)生成S集合$\{S_1,S_2,S_3,\cdots,S_l\}$，然后根据贝叶斯公式算出$v_i(i=1,2,3,\cdots,l)$报告事件的聚合可信度，如式(14)所示，最后根据式(15)生成最终的ISV评分结果

$$p(e|e_1,e_2,\cdots,e_l)=\frac{p(e_1|e)\times p(e_2|e)\times\cdots\times p(e_l|e)\times p(e)}{p(e_1,e_2,\cdots,e_l)}=\frac{p(e)\times\prod_{i=1}^{l}p\ (e_i|e)}{\prod_{i=1}^{l}p\ (e_i)}\Rightarrow p(e|E)=\frac{p(e)\times\prod_{i=1}^{l}p\ (e_i|e)}{p(e)\times\prod_{i=1}^{l}p\ (e_i|e)+p(\bar{e})\times\prod_{i=1}^{l}p\ (e_i|\bar{e})} \tag{14}$$

$$R=\begin{cases}1, & p(e|E)\geqslant \text{threshold}\\ -1, & p(e|E)<\text{threshold}\end{cases} \tag{15}$$

其中，$\bar{e}$是事件e的互补事件，如果$p(e|E)$超过一定阈值，则ISV判定IPV所发送消息为真实消息，否则判定为虚假消息。车辆v_i将信息发送给ISV集合，所以IPV对于事件e会收到多个来自不同ISV的评价，ISV会将评价发送给距离区域码最近的RSU共识节点，然后RSU共识节点将评价汇聚到协调节点，协调节点对IPV的最终平均得分如式(16)所示，在评分之后会将评分结果发送给主节点进行共识，最终上传到联盟链

$$G=\frac{\sum_{j=1}^{w}C_j\times R_{j\to i}}{w} \tag{16}$$

其中，w代表v_i对事件e收到来自ISV评价数量，C_j代表v_j的诚信分，$R_{j\to i}$代表v_j对v_i的评价。平均得分会影响v_i的诚信分变化，为了控制诚信分变化的幅度以使系统更加稳定，采用了式(17)的处理方式

$$C_i'=\begin{cases}C_i+G^{\rho}, & G>0\\ C_i+G^{\sigma}, & G\leqslant 0\end{cases} \tag{17}$$

其中，$\rho\in(0,1)$，$\sigma\in(1,+\infty)$，当车辆诚信分增加时，呈现先快后慢的趋势，相反，当车辆诚信分减少，呈现先慢后快的趋势。若是参与车联网的车辆不积极参与信息的收集及共享，那么RSU会每隔一小时检查与自己区域编码距离为d的车辆的诚信分变化次数，若变化次数为0，那么

$$C_i'=C_i\times(1-\varepsilon)^{\mu} \tag{18}$$

其中，$\mu\in(0,1)$，μ是RSU监测到IPV懒惰的次数。

2.3　DMML-HotStuff共识算法

尽管HotStuff共识算法能够提高协议的可扩展性和性能，但由于只有一个主节点，很容易出现性能瓶颈问题。本文提出的DMML-HotStuff共识算法，利用多主节点呈流水线式产生区块以突破性能瓶颈，同时通过动态节点调整机制进一步提高联盟链的吞吐量。虽然协调多主节点共识会增加每轮运算的复杂度，但是多主节点间的并行共识在整体上大幅度降低了联盟链出块时间。

假定一共有$N(3F+h+1)$个RSU节点，其中拜占庭节点数量不超过F个，将所有RSU节点划分为协调节点、主节点、跟随节点、候补共识节点4类节点，h是候补共识节点数量。协调节点负责收集和分发IPV发送来的信息以及共识节点集合的选择，主节点负责运算产生区块，跟随节点参与联盟链共识机制中的记账过程，候补共识节点暂时不参与共识运算，如果有需要更替或增加共识节点时，协调节点会选择候补共识节点加入到共识节点中。共识算法从第$r=0$轮开始，每一轮都会按照诚信分高低排序选出下一轮的共识节点集合Z_r和协调节点，并代替上一轮的共识节点集合Z_{r-1}和协调节点，协调节点从Z_r中选出y个主节点运算产生区块。该过程由一个协调节点在每一轮视图中自动完成，共识节点集合中的节点可以扮演多重角色，主节点也可以同时是协调节点，在本文中，协调节点是一个诚信分最高的共识节点。当共识节点被上一轮协调节点选举为协调节点后，会向所有共识节点发送协调节点变更消息Nchange，当主节点收到该消息后，会对消息进行签名，当协调节点收集到$N-F-h$个共识节点的同意票后就会创建view$_r$。DMML-HotStuff共识算法如图4所示，当进入第r轮视图后，协调节点会收集来自共识节点发送的信息，然后协调节点将现有信息划分为y个不重合的分区，为每个分区分配一个未被选取过的序列号，将这些序列号分配给y个主节点，同时按照序列号的大小排序给每个主节点分配一个索引号index$\in(0,1,2,3,\cdots,y)$，协调节点会将这些信息按照索引分配给各个主节点，如果存在上一轮视图中未完成共识的信息，那么优先分配遗留信息给主节点。主节点会呈流水线式处理这些分区，每个主节点会

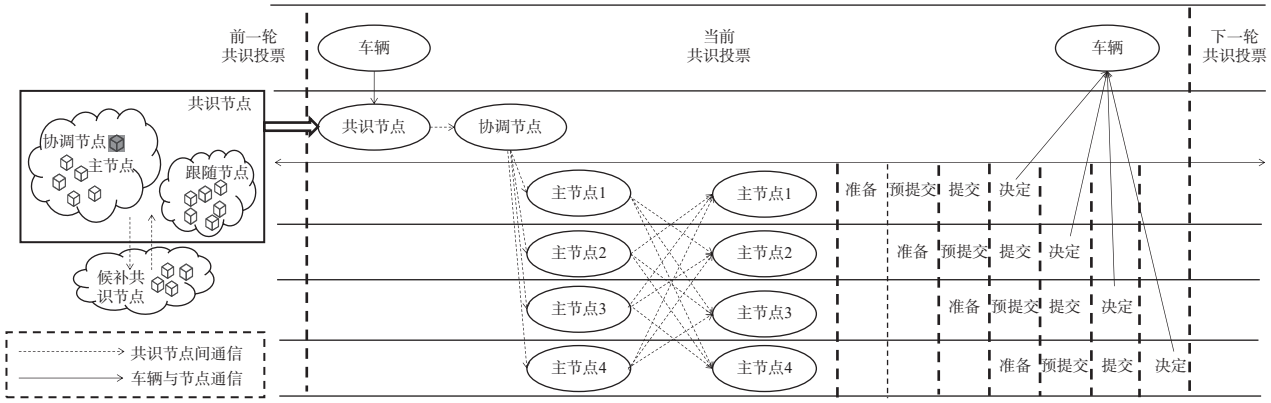


图4　DMML-HotStuff共识算法

向其他主节点广播4轮消息，分别是准备阶段、预提交阶段、提交阶段和决定阶段，在每个阶段中，主节点收到$\lceil(2\times|Z_r|)/3\rceil$（$|Z_r|$是共识节点数量）个共识节点的同意票后，会使用门限签名[32]技术将这些投票生成一个签名，在进入下一个阶段后，每个主节点会先检查上一阶段的签名，然后再进行本阶段的投票，当完成4个阶段的投票后，主节点就可以将区块添加到联盟链中。在不同主节点间进行流水线运算时，索引号小的主节点必须收到索引号减一的主节点上一阶段的投票消息后，才能进行本主节点本阶段的投票，索引号为0的主节点除外。

由于每一轮view选举出的主节点数量是不固定的，本文方案是首先给定一个初始值，然后协调节点会监控每一轮的信息上传量，如果上传量大于阈值，就相应增加共识主节点和减少共识跟随节点以加快共识速度，如果上传量小于阈值，就相应减少共识主节点和增加共识跟随节点以提高安全性，下一个视图中主节点数量按照式(19)进行变更

$$|M_{r+1}|=\left\lceil\frac{|M_r|\times D_{r-1}}{D_r}\right\rceil \tag{19}$$

相应地，下一个视图中跟随节点数量按照式(20)进行变更

$$|F_{r+1}|=|F_r|\times\left(1+\frac{|\mathrm{M}_r|\times\left(1-\dfrac{D_{r-1}}{D_r}\right)}{1-M_r}\right) \tag{20}$$

其中，D_r是本轮信息量，D_{r-1}是上一轮信息量，$|M_r|$是本视图中主节点集合M_r中主节点数量，$|F_r|$是本视图中跟随节点集合F_r中节点数量。

此外，本文采用基于诚信分的选择机制来确定共识节点集合，并决定由哪个节点担任主节点和协调节点。在每轮共识结束后，基于节点是否成功与其他节点协作达成共识和有效产生区块，系统会相应调整其诚信得分。如果共识节点集合正确产生区块，共识节点$\mathrm{RSU}_\phi(\phi=1,2,3,\cdots,|Z_r|)$诚信分变更如式(21)所示

$$T_r^\phi=T_{r-1}^\phi+V\left(\frac{\sum c_{\text{true}}}{e^{T_{r-1}^\phi}}+a\times\frac{\sum T_x}{|Z_r|}\right) \tag{21}$$

其中，c_{true}代表成功参与共识并出块的次数，V是判断共识节点是否成功参与本次共识的系数，当共识节点成功参与共识$V=1$，反之$V=0$，$\sum T_x/|Z_r|$代表所有共识节点的诚信分均值。a是节点诚信分调节因子，当共识节点是主节点时$a=-0.4$，当是普通共识节点时$a=0$，其作用是避免共识节点出现中心化节点问题，当共识节点成为主节点并成功出块后，其诚信分会被降低，不会出现同一主节点诚信分不断增长且长期保持最高的状态，其他共识跟随节点只要持续成功参与共识，就有机会成为主节点。如果共识节点集合未成功出块，按照式(22)更改诚信分

$$T_r^\phi=\begin{cases}T_{r-1}^\phi\times c_{\text{fail}} & c_{\text{fail}}=1,\\ T_{r-1}^\phi-c_{\text{fail}}\times\dfrac{\sum T_x}{|Z_r|}, & c_{\text{fail}}>1\end{cases} \tag{22}$$

其中，c_{fail}代表没有成功参与共识的次数。为了区分技术问题和恶意节点行为，本文系统采取了一种宽容机制。该机制允许每个共识节点有一次未能成功参与共识的机会而不损失其诚信分。然而，如果一个节点反复未能成功参与共识，系统会对相关共识节点的诚信分进行大幅度扣减。一旦一个共识节点的诚信分下降到一定临界点，它会被判定为不适合继续作为共识节点，这时协调节点将介入处理，协调节点从备选共识节点的池中，挑选诚信分较高、性能稳定的节点来代替那些诚信分过低的共识

节点，并将剔除的RSU节点编码活跃位置为0，新加入的RSU节点活跃位置为1，然后向所有车辆和RSU广播更新后的表。

3　安全性分析

3.1　恶意车辆攻击

1) 本文提出的方案可以有效解决恶意车辆故意传播虚假道路交通信息的问题，从而避免交通流受阻与灾难性交通事故的发生。本文提出的信息验证机制是车辆提供的信息会受到系统中多个其他车辆的验证和评估。如果一个车辆不断被评为不可信，其诚信分会经历一个逐渐加速的下降过程。这种下降是先缓慢而后迅速，形成了一种过滤恶意车辆信息的自然“防御机制”。一旦诚信分跌至某一临界点，恶意车辆发布的信息将不再被系统和其他信息需求者所采用。

2) 本文提出的方案可以有效解决恶意车辆故意给出偏离实情评价的问题，从而确保诚实车辆的权威性不被削弱。本文的设计是一旦诚实车辆收集到一份信息，它将把这份信息分发给几个被选中的评判车辆。每个信息的最终评分并不是由单一车辆决定，而是由多个评判车辆的意见经过加权汇总得出。此外，评判车辆的选择在每一轮评分过程中都会发生改变。这意味着即使在某一轮评分中，诚实车辆的诚信分因为被恶意扣分而下降，但只需要不停地提供真实信息，其诚信分就能逐渐回升到正常水平。

3) 本文提出的方案可以有效解决懒惰车辆的存在导致系统在全局优化上输入信息不足的问题，从而确保系统决策效果达到最佳。RSU共识节点会以每小时为周期进行审查，审查过去一小时内各行驶车辆是否进行信息的收集与分享。如果发现有车辆在这一时间段内没有积极参与信息的收集与分享，那么被认定为“懒惰”的车辆将受到相应处罚。RSU共识节点将自动扣除这些懒惰车辆的诚信分，诚信分过低的车辆将面临使用车联网服务的限制，甚至被禁止使用某些关键功能。

3.2　恶意RSU节点攻击

本文提出的方案解决了恶意RSU节点不公正地扣除诚实车辆诚信分的问题。在此系统中，车辆诚信分是由已经获得最高诚信分的RSU协调节点来计算和更新的，其评分结果被认为是最可靠的。即便有恶意节点试图通过给出不公的评分来影响诚实车辆的诚信分，但由于协调节点是动态更新的，一个恶意评分只是一时的，只要诚实车辆持续上传质量可靠的信息，它们的诚信分将在不久的时间内得到恢复。此外，懒惰RSU共识节点即便闲置不参与共识过程，也无法逃避系统的自我纠错机制。每一次共识过程都伴随着共识节点诚信分的变动，如果恶意节点的行为企图妨碍系统的正常运行，它们的诚信分将受到惩罚，一旦恶意节点的诚信分降至特定阈值以下，系统将自动将其从共识节点群中排除，并且引入备用的高诚信节点以保持共识过程的完整性。假设一共有$N(N \geqslant 3)$个共识节点，其中有$F(F \geqslant 0)$个拜占庭节点，另外还有$h(h \geqslant 0)$个候补节点，则系统允许的拜占庭节点数量范围如式(23)和式(24)所示

$$N - F + h \geqslant 2F + 1 \tag{23}$$

$$N - 1 \geqslant F \tag{24}$$

其中，式(23)表示诚信节点和诚信候补节点数量之和要大于等于$2F + 1$才能保证共识节点正常进行共识，式(24)表示只有协调共识节点不允许为拜占庭节点，因为在除了协调节点外，其他共识节点均为拜占庭节点的情况下，协调节点需要缓存现有的信誉分，在系统将这些拜占庭节点替换为诚实节点后，能够将宕机时段内信誉分变化上传至联盟链。联合上述两式可以得到式(25)

$$\begin{cases} F \leqslant N - 1, & h \geqslant 2N - 2 \\ F \leqslant \dfrac{N + h - 1}{3}, & 0 \leqslant h < 2N - 2 \end{cases} \tag{25}$$

在此考虑端点情况，若是诚信候补节点足够多，则系统能够允许的拜占庭节点比例为$(N-1)/3N$，若是没有诚信候补节点，则系统能够允许的拜占庭节点比例为$(N-1)/3N$。传统拜占庭容错共识算法最多能够允许的拜占庭节点比例为$(N-1)/3N$，因此本文的DMML-HotStuff共识算法能够允许的拜占庭节点比例要优于传统拜占庭容错共识算法。

4　仿真结果与分析

4.1　仿真设置

本文实验的环境是采用Apple M2芯片、8 GB内存、macOS操作系统的计算机，采用GO语言编写共识算法，使用veins5.2、OMNeT5.6.2、sumo1.8.0进行车辆网仿真。仿真实验初始化了2 000辆车和50个RSU，并将随机选取的一幅道路图划分为了32个部分，每个部分无重叠，给每辆车进行32位二

进制编码，其中区域码部分占8位，车辆码占24位，RSU编码中区域码占8位，其他24位代表着每一个RSU独特的身份码。本文将每一轮仿真实验时间设置成300 s，车辆间发送信息的区域码阈值设置为5，车辆报告事件的聚合可信度阈值设置为0.9[33]，影响共识节点数量变更的信息上传量阈值设置为0.8[34]，车辆和RSU的初始诚信分设置成10，同时设置30%的恶意车辆。由式(7)可知，Bloom Filter可能存在一定的假正率P^+，在此本文设置P^+能容忍的阈值是0.01，即假正率不超过1%。为了设置最佳效果，本文实验按照式(26)设置Bloom Filter参数

$$\lim_{q\to+\infty} P^+ = \lim_{q\to+\infty} \left(1-\left(1-\frac{1}{q}\right)^{ku}\right)^k \approx \left(1-e^{\frac{-ku}{q}}\right)^k \tag{26}$$

设函数

$$f(k) = \left(1-e^{\frac{-ku}{q}}\right)^k \tag{27}$$

令$x = e^{\frac{-u}{q}}$，取其对数并对k求导可以得到

$$\frac{f'(k)}{f(k)} = \ln\left(1-x^{-k}\right) + k\times\frac{x^{-k}\ln x}{1-x^{-k}} \tag{28}$$

当$f'(k)=0$时γ得到最小值，此时有

$$1-x^{-k} = x^{-k} \Rightarrow x^{-k} = \frac{1}{2} \Rightarrow e^{\frac{-ku}{q}} = \frac{1}{2} \tag{29}$$

将式(29)代入式(26)可以得到

$$\ln P^+ = \ln 2\frac{q}{u}\times(-\ln 2) = -\frac{q}{u}(\ln 2)^2 \tag{30}$$

根据式(30)可以得到

$$q = -\frac{u\ln\gamma}{(\ln 2)^2} \tag{31}$$

$$k = \frac{q(\ln 2)}{u} \tag{32}$$

其中，q是Bloom Filter位数组大小，本文实验中设置为16 MB，u代表插入过滤器的元素个数，k是hash函数数量。本文将每一轮仿真实验中u设置为10 000 000，根据u得到过滤器位数组和hash函数数量。

4.2　仿真分析

4.2.1　信息传输量比较

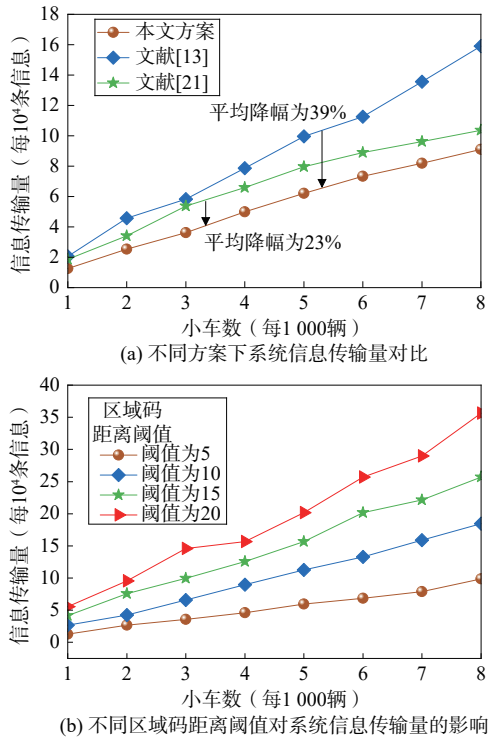
系统信息传输量对比如图5所示，本文实验比较了系统在不同情况下的信息传输量，其中图5(a)展示了在不同方案下系统信息传输量对比结果，图5(b)则分析了不同区域码距离阈值对系统信息传输量的影响。

图5(a)展示了在本文方案与文献[13]和文献[21]两种车辆信息共享方案在信息传输量方面的对比。从图5(a)中可知，相较于前两种方法，本文通过基于角度差自变换区域码的信息传输控制策略，显著减少了道路交通信息传输量，从而有效减轻了网络负载。随着车辆数的增加，本文方案较文献[13]的优势愈发明显，这是因为文献[13]仅考虑了车辆信誉管理机制，而忽视了对信息量的控制。当车辆数少于5 000时，本文方案相较于文献[21]展现出逐渐增加的优势。然而，当车辆数超过5 000时，这种优势开始降低。这是因为随着车辆数的增加，车辆密度也随之提高。在车辆密度较高的情况下，文献[21]提出的方案相较车辆密度低时能表现出更好的性能。为计算本文方案在信息传输量上的优化幅度，采用式(33)进行量化

$$\tau = \frac{\sum_{1}^{\kappa}\left(\xi_{\text{this}}-\xi_{\text{other}}\right)\Big/\xi_{\text{other}}}{\kappa} \tag{33}$$

其中，κ表示在不同车辆数条件下比较次数，ξ_{this}表示本文方案信息传输量，ξ_{other}表示另外两种方案之一的信息传输量。根据图5(a)中数据可以得出本文方案相比文献[21]和文献[13]方案信息传输量分别减少了23%和39%。

图5(b)展示了当区域码距离阈值分别设置为5、10、15和20时，对系统信息传输量的影响。从图5(b)中可以看出，随着距离阈值的增加，通信量也呈递增趋势，原因在于更大的阈值意味着每辆车在信息



(a) 不同方案下系统信息传输量对比

(b) 不同区域码距离阈值对系统信息传输量的影响

图5　系统信息传输量对比

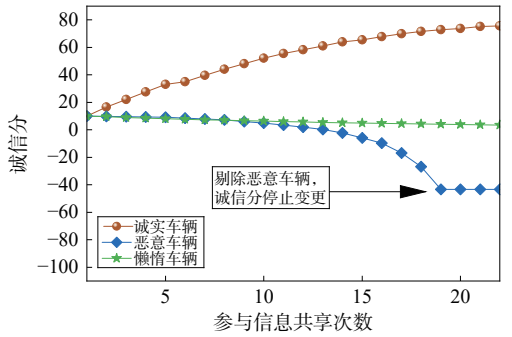
转发时涵盖对象的扩展，转发信息需发送给更多车辆。然而，值得注意的是，本文在设置阈值时不能简单追求低值。通常情况下，较低的阈值确实可以减少信息传输量，因为这样限制了每条信息被转发的车辆数。但是，若区域码阈值过低，将导致对IPV信息的评估不足，从而削弱了整个网络中信息的可信度。因此，在接下来的实验中，本文将区域码阈值设置为10，以在保证信息评估量充足的前提下尽量减少网络信息传输量。

4.2.2　诚信分变化

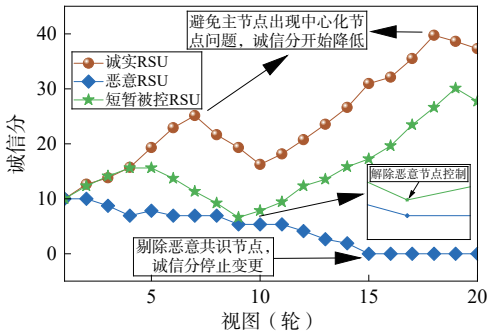
及时发现恶意实体对维护系统稳定性至关重要，因此本文实验测试了系统辨别不同类型实体的能力。系统中不同实体诚信分变化对比如图6所示，其中图6(a)展示了不同类型车辆诚信分变化趋势，图6(b)展示了不同RSU诚信分变化趋势。

在图6(a)中，诚实车辆通过不断且积极地参与到信息的分享与交换中，以可靠的行为建立了良好的信用记录，因此其诚信分增长趋势明显，如前文所述，为了控制诚信分变化幅度以使系统更加稳定，其诚信分呈现出一个“先快后慢”的增长模式。对比之下懒惰车辆由于缺乏对网络信息贡献的行为，其诚信分持续匀速下降。恶意车辆的诚信分呈现出“先慢后快”的下降趋势，这意味着，虽然一开始诚信分的减少不是特别明显，但一旦被系统识别出有持续的恶劣行为，诚信分下降速率将迅速增加，表现出一种惩罚性质的下降动态，当信誉分下降到一定值后，系统将不再允许该恶意车辆参与信息共享。

在图6(b)中，诚实RSU在还未获得主节点地位时，通过连续且正确地参与共识过程，其诚信分累积上升。然而，一旦这些RSU成为主节点，并始终正确参与共识，它们的诚信分反而开始减少，这一机制防止了任何一个RSU长期占据主导地位，保持了网络的权力分布均衡性和安全性。诚信分减到一定阈值后，这些RSU将转换为跟随节点，此时，它们的诚信分再次开始增加，给予它们再次成为主节点的可能性。恶意RSU由于其不良行为，诚信分会持续下降，当诚信分降至0时，将被移除出共识节点集群，并替换新的RSU到集群中。短暂被控RSU在正确参与共识时，其诚信分会缓慢上升。但是，一旦它被控制，并开始执行异常行为，诚信分会快速下降。尽管如此，当这种控制被解除，随着RSU恢复正常行为，它的诚信分也会逐渐回升至正常水平。



(a) 不同类型车辆诚信分变化趋势



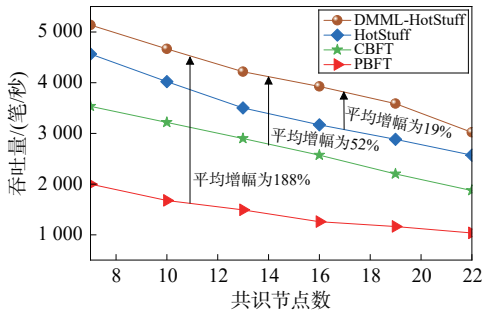
(b) 不同RSU诚信分变化趋势

图6　诚信分变化对比

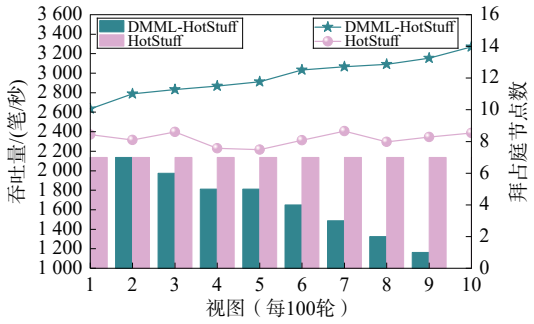
4.2.3　算法吞吐量比较

由于拜占庭容错共识算法相较于非拜占庭容错共识算法有着更好的容错能力和更高效的共识机制，拜占庭容错算法在车联网这种复杂多变、对安全和实时性要求高的场景下更具适用性。在不同条件下共识算法的吞吐量对比如图7所示，其中图7(a)展示了在没有拜占庭节点攻击的前提下DMML-HotStuff共识算法与另外3种拜占庭容错共识算法（PBFT[27]、HotStuff[28]以及CBFT[29]）的吞吐量对比情况，图7(b)展示了在存在拜占庭节点前提下DMML-HotStuff共识算法与传统HotStuff共识算法的吞吐量对比情况。

从图7(a)中可以看出，DMML-HotStuff共识算法在吞吐量方面表现出显著优势，相较于参照的3种算法，它能够在单位时间内处理更多的交易请求。随着参与共识的节点数量增加，吞吐量呈现出逐渐下降的趋势。这是因为更多的节点参与共识意味着必须处理更多的消息交换，以达到网络中所有节点的一致状态。4种算法复杂度对比见表1，PBFT和CBFT算法通信复杂度是$O(n^2)$，然而，当视图连续转换时（如在不稳定的网络环境中，或在面对攻击时），通信复杂度会急剧升高到$O(n^4)$，另外，HotStuff算法和DMML-HotStuff算法具有较低的通



(a) 无拜占庭节点攻击时不同算法吞吐量对比



(b) 存在拜占庭节点时不同算法吞吐量对比

图7　吞吐量对比

表1　　4种算法复杂度对比

算法	通信复杂度	连续切换视图通信复杂度
PBFT	$O(n^2)$	$O(n^4)$
CBFT	$O(n^2)$	$O(n^4)$
HotStuff	$O(n)$	$O(n^2)$
DMML-HotStuff	$O(n)$	$O(n)$

信复杂度$O(n)$，在处理大量信息传输时更为有效。但是HotStuff算法在连续变换视图时，通信复杂度也会上升到$O(n^2)$，与此不同，DMML-HotStuff算法在共识阶段就已经考虑下一轮主节点的选举，这样可以避免在主节点失败时出现共识中断的问题。此外，本文采用了多主节点的策略，这使得共识过程可以呈流水线的方式进行，即使在主节点连续故障导致频繁切换视图的极端情况下，其通信复杂度也能维持在$O(n)$。为了计算DMML-HotStuff共识算法相比另外3种共识算法吞吐量的提升效果，其提升率可通过式(34)计算

$$\varsigma = \frac{\sum_{1}^{\varpi}(H_{\text{this}} - H_{\text{other}})/H_{\text{other}}}{\varpi} \tag{34}$$

其中，ϖ表示在不同共识节点数条件下比较次数，H_{this}表示DMML-HotStuff吞吐量，H_{other}表示另外3种共识算法之一的吞吐量。根据图7(a)中数据，可以得出DMML-HotStuff共识算法对比HotStuff、CBFT、PBFT 3种共识算法，吞吐量在无拜占庭节点条件下分别提高了19%、52%、188%。

在图7(b)对应的实验中，共设置了22个共识节点，其中包含7个拜占庭节点。实验结果显示，通过采用共识节点交替机制，DMML-HotStuff共识算法能够随着视图的不断更迭，逐步减少拜占庭节点的影响，最终将其数量减少至0。该策略有效降低了视图切换过程中产生的开销，从而显著提升了系统的吞吐量，使其在不断优化中保持稳定增长。

5　结束语

本文针对车联网中现有方案未能有效解决的冗余交通信息传输、恶意车辆和恶意RSU节点传播虚假信息以及共识算法性能瓶颈问题，提出了一种车联网交互信息控制与高效安全共享方案。首先，设计了一种角度差自变换区域码信息传输控制策略，通过设定车辆区域码之间的距离阈值，有效限制信息转发，同时利用Bloom Filter减少冗余信息传输，从而缓解网络拥塞。其次，建立了一套诚信分管理机制，涵盖车辆和RSU两个层面，以增强系统的安全防护能力。最后，提出了动态管理DMML-HotStuff共识算法，解决传统共识算法中单主节点性能瓶颈问题，同时，通过动态节点调整方案，有效提升了联盟链系统的整体吞吐量。实验结果证实了本文所提方案的优越性，相较于现有的两种车辆交互信息处理方法，该方案分别减少了23%和39%的信息传输量，并具备实时动态评估车辆和RSU诚信度的能力，能够快速识别和隔离恶意节点。此外，联盟链系统的吞吐量相比现有3种拜占庭容错共识算法分别提升了19%、52%和188%。在未来的工作中，将进一步用联邦学习检测拜占庭节点以提高系统的稳定性。

参考文献：

[1] 赵川斌, 高飞飞. 通信感知算力一体化在车联网中的应用探讨[J]. 移动通信, 2024, 48(3): 1-7.
ZHAO C B, GAO F F. Exploring the application of integrated sensing, communication, and computing in vehicle-to-everything[J]. Mobile Communications, 2024, 48(3): 1-7.

[2] 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.

[3] ABBES S, REKHIS S. A blockchain-based solution for reputation management in IoV[C]//Proceedings of the 2021 International

Wireless Communications and Mobile Computing (IWCMC). Piscataway: IEEE Press, 2021: 1129-1134.

[4] 高镇, 崔琪楣, 张雪菲, 等. 区块链在物联网系统中的应用探讨[J]. 物联网学报, 2020, 4(2): 10-17.
GAO Z, CUI Q M, ZHANG X F, et al. Discussions about application of blockchain in IoT systems[J]. Chinese Journal on Internet of Things, 2020, 4(2): 10-17.

[5] FENG C S, LIU B, YU K P, et al. Blockchain-empowered decentralized horizontal federated learning for 5G-enabled UAVs[J]. IEEE Transactions on Industrial Informatics, 2022, 18(5): 3582-3592.

[6] ZHANG C, XU Y, HU Y P, et al. A blockchain-based multi-cloud storage data auditing scheme to locate faults[J]. IEEE Transactions on Cloud Computing, 2022, 10(4): 2252-2263.

[7] DUAN S J, LYU F, REN J, et al. Multitype highway mobility analytics for efficient learning model design: a case of station traffic prediction[J]. IEEE Transactions on Intelligent Transportation Systems, 2022, 23(10): 19484-19496.

[8] LOBATO W, MENDES P, ROSÁRIO D, et al. Redundancy mitigation mechanism for collective perception in connected and autonomous vehicles[J]. Future Internet, 2023, 15(2): 41.

[9] XU Y W, YU E Z, SONG Y X, et al. $\mathcal{R}$-tracing: consortium blockchain-based vehicle reputation management for resistance to malicious attacks and selfish behaviors[J]. IEEE Transactions on Vehicular Technology, 2023, 72(6): 7095-7110.

[10] LIU Z, YU M J, LI R. Blockchain-based trust management mechanism in V-NDN[C]//Proceedings of the 2023 26th International Conference on Computer Supported Cooperative Work in Design (CSCWD). Piscataway: IEEE Press, 2023: 1433-1438.

[11] HOU B C, XIN Y, ZHU H L, et al. VANET secure reputation evaluation & management model based on double layer blockchain[J]. Applied Sciences, 2023, 13(9): 5733.

[12] MAHMOUD H, AZAD M A, ARSHAD J, et al. A framework for decentralized, real-time reputation aggregation in IoV[J]. IEEE Internet of Things Magazine, 2023, 6(2): 44-48.

[13] 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.

[14] 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.

[15] YIN B, WU Y L, HU T S, et al. An efficient collaboration and incentive mechanism for Internet of vehicles (IoV) with secured information exchange based on blockchains[J]. IEEE Internet of Things Journal, 2020, 7(3): 1582-1593.

[16] YU L, DENG J, BROOKS R R, et al. Automobile ECU design to avoid data tampering[C]//Proceedings of the 10th Annual Cyber and Information Security Research Conference. New York: ACM Press, 2015: 1-4.

[17] LI M S, GAO J, ZHAO L, et al. Adaptive computing scheduling for edge-assisted autonomous driving[J]. IEEE Transactions on Vehicular Technology, 2021, 70(6): 5318-5331.

[18] SANGAIAH A K, RAMAMOORTHI J S, RODRIGUES J J P C, et al. LACCVoV: linear adaptive congestion control with optimization of data dissemination model in vehicle-to-vehicle communication[J]. IEEE Transactions on Intelligent Transportation Systems, 2021, 22(8): 5319-5328.

[19] LUO G Y, ZHOU H B, CHENG N, et al. Software-defined cooperative data sharing in edge computing assisted 5G-VANET[J]. IEEE Transactions on Mobile Computing, 2021, 20(3): 1212-1229.

[20] ZHUANG Y, YU L, SHEN H Y, et al. Data collection with accuracy-aware congestion control in sensor networks[J]. IEEE Transactions on Mobile Computing, 2019, 18(5): 1068-1082.

[21] MOHAMMED N, KADHIM R A. Congestion control in VANETs based on message rate adaptation by the exponential function[C]//Proceedings of the 2022 5th International Seminar on Research of Information Technology and Intelligent Systems (ISRITI). Piscataway: IEEE Press, 2023: 24-28.

[22] AL-JAROODI J, MOHAMED N. Blockchain in industries: a survey[J]. IEEE Access, 2019, 7: 36500-36515.

[23] 谭朋柳, 万里旭冉. 一种具有主从区块的区块链架构[J]. 物联网学报, 2021, 5(2): 116-124.
TAN P L, WAN L X R. A blockchain architecture with master-slave blockchain[J]. Chinese Journal on Internet of Things, 2021, 5(2): 116-124.

[24] AMIRI M J, AGRAWAL D, EL ABBADI A. Permissioned blockchains: properties, techniques and applications[C]//Proceedings of the 2021 International Conference on Management of Data. New York: ACM Press, 2021: 2813-2820.

[25] OUYANG Z Q, SHAO J, ZENG Y F. PoW and PoS and related applications[C]//Proceedings of the 2021 International Conference on Electronic Information Engineering and Computer Science (EIECS). Piscataway: IEEE Press, 2021: 59-62.

[26] GARG R, ARORA N, UPPAL S, et al. Proof of opinion (PoO): a new consensus algorithm for decentralized blockchain networks[C]//Proceedings of the 2023 4th International Conference for Emerging Technology (INCET). Piscataway: IEEE Press, 2023: 1-6.

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

[28] YIN M F, MALKHI D, REITER M K, et al. HotStuff: BFT consensus with linearity and responsiveness[C]//Proceedings of the 2019 ACM Symposium on Principles of Distributed Computing. New York: ACM Press, 2019: 347-356.

[29] GAI F Y, FARAHBAKHSH A, NIU J Y, et al. Dissecting the performance of chained-BFT[C]//Proceedings of the 2021 IEEE 41st International Conference on Distributed Computing Systems (ICDCS). Piscataway: IEEE Press, 2021: 595-606.

[30] ZHANG X J, ZHONG W Y, YANG C, et al. BFT consensus algorithms[C]//Proceedings of the 2023 IEEE 10th International Conference on Cyber Security and Cloud Computing (CSCloud)/2023

IEEE 9th International Conference on Edge Computing and Scalable Cloud (EdgeCom). Piscataway: IEEE Press, 2023: 434-439.

[31] 赵中原, 高旺, 蒋璐瑶, 等. 基于椭圆曲线ELGamal的隐私保护分布式优化算法[J]. 自动化学报, 2025, 51(1): 210-220.
ZHAO Z Y, GAO W, JIANG L Y, et al. Privacy-preserving distributed optimization algorithm based on elliptic curve ELGamal[J]. Acta Automatica Sinica, 2025, 51(1): 210-220.

[32] 荆继武, 张世聪, 王平建. 门限密码技术及其标准化进展[J]. 密码学报(中英文), 2024, 11(1): 227-254.
JING J W, ZHANG S C, WANG P J. Threshold cryptography technology and standardization process[J]. Journal of Cryptologic Research, 2024, 11(1): 227-254.

[33] SUN X Y, DAI J, LIU P, et al. Using Bayesian networks for probabilistic identification of zero-day attack paths[J]. IEEE Transactions on Information Forensics and Security, 2018, 13(10): 2506-2521.

[34] 路宇轩, 孔兰菊, 张宝晨, 等. MC-RHotStuff: 面向多链基于信誉的HotStuff共识机制[J]. 计算机研究与发展, 2024, 61(6): 1559-1572.
LU Y X, KONG L J, ZHANG B C, et al. MC-RHotStuff: multi-chain oriented HotStuff consensus mechanism based on reputation[J]. Journal of Computer Research and Development, 2024, 61(6): 1559-1572.

[作者简介]

王樊（1999– ），男，华中科技大学网络空间安全学院硕士生，主要研究方向为区块链、车联网。

代玥玥（1990– ），女，华中科技大学网络空间安全学院副教授，主要研究方向为数字孪生、边缘智能、区块链、联邦学习。

杨慧炅（1999– ），女，香港理工大学电子计算学系硕士生，主要研究方向为区块链安全、车联网。

王秀华（1989– ），女，华中科技大学网络空间安全学院副研究员，主要研究方向为区块链安全、人工智能安全。

卢云龙（1991– ），男，北京交通大学电子信息工程学院教授，主要研究方向为宽带移动通信系统与专用移动通信、人工智能、新一代电子信息技术。