

基于信任值的车联网分层共识优化协议

翟宝琴¹, 王健¹, 韩磊², 刘吉强¹, 何嘉豪¹, 刘天皓¹

(1. 北京交通大学智能交通数据安全与隐私保护技术北京市重点实验室, 北京 100044;

2. 北京计算机技术及应用研究所, 北京 100854)

摘要: 随着车联网、5G 和人工智能技术的快速发展, 智能交通成为交通技术发展趋势, 车联网作为车-车、车-路信息交互平台, 是智能交通信息共享和处理的基础。同时车联网安全备受关注, 特别是数据安全问题, 可能会造成用户隐私泄露。区块链技术的发展成为一种解决途径, 但在效率、安全性等方面仍面临新挑战。随着车辆节点、信息增多, 如何在车辆高速移动环境中高效完成信息共识也成为问题关键。针对上述问题, 提出基于区块链及信任值的自下而上双层 RSU (road side unit) 链共识协议。对比几种典型的共识结构并依据实际车联网场景、符合速度、容错率以及减少通信量需求, 选择自下而上双层共识结构。通过赋予每辆车信任值, 并基于节点参与程度、工作完成情况及消息价值度提出组领导节点选举算法, 以确保系统安全性。基于上述共识结构与算法工作, 完整描述协议具体流程, 分为区域划分、组领导节点选取、局部共识、领导主节点选取、全局共识、域内广播 6 个步骤。从安全性、通信复杂度、共识算法时延、容错率 4 个方面对实验进行分析。实验证明, 与其他方案对比, 本协议在可抵抗合谋攻击、女巫攻击等条件下, 可以有效降低通信复杂度, 缩短共识时延, 并在安全前提下提高容错率, 使更多节点参与信息共享, 满足车联网场景需求。

关键词: 共识分层; 车联网; 信任值; 区块链; 信息更新效率

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2021097

Hierarchical proxy consensus optimization for IoV based on blockchain and trust value

ZHAI Baoqin¹, WANG Jian¹, HAN Lei², LIU Jiqiang¹, HE Jiahao¹, LIU Tianhao¹

1. Beijing Key Laboratory of Security and Privacy in Intelligent Transportation, Beijing Jiaotong University, Beijing 100044, China

2. Beijing Institute of Computer Technology and Application, Beijing 100854, China

Abstract: With the rapid development of Internet of vehicles, 5G and artificial intelligence technologies, intelligent transportation has become the development trend of transportation technology. As a vehicle-vehicle and vehicle-road information interaction platform, the Internet of vehicles is the basic support platform for intelligent traffic

收稿日期: 2021-06-16; 修回日期: 2021-09-03

通信作者: 王健, wangjian@bjtu.edu.cn

基金项目: 国家重点研发计划 (2020YFB2103800)

Foundation Items: The National Key R&D Program of China (2020YFB2103800)

引用格式: 翟宝琴, 王健, 韩磊, 等. 基于信任值的车联网分层共识优化协议[J]. 网络与信息安全学报, 2022, 8(3): 142-153.

Citation Format: ZHAI B Q, WANG J, HAN L, et al. Hierarchical proxy consensus optimization for IoV based on blockchain and trust value[J]. Chinese Journal of Network and Information Security, 2022, 8(3): 142-153.

information sharing and processing. At the same time, the security of Internet of vehicles has attracted much attention, especially data security which may cause user privacy leakage. The blockchain technology has become a solution, but it still faces new challenges in efficiency, security and other aspects. With the increase of vehicle nodes and information, how to efficiently achieve information consensus in high-speed vehicle moving environment has become a key problem. Then a bottom-up RSU (road side unit) chain consensus protocol was proposed based on blockchain and trust value. Several typical consensus structures were compared, and bottom-up two-layer consensus structure was adopted according to the actual scenarios of the Internet of vehicles. Moreover, a group leader node election algorithm was proposed which is based on node participation, work completion and message value. The system security was ensured by assigning trust value to each vehicle. Following the consensus structure and algorithm work mentioned above, the specific process of the protocol was comprehensively described, which was divided into six steps: region division, group leader node selection, local consensus, leader primary node selection, global consensus, and intra-domain broadcast. Then the experiments were analyzed from four aspects: security, communication complexity, consensus algorithm delay and fault tolerance rate. Experiments showed that, compared with other schemes, the proposed protocol can effectively reduce communication complexity and shorten consensus delay under the condition of resisting conspiracy attack, witch attack and other attacks. On the premise of security, the protocol improves fault tolerance rate and enables more nodes to participate in information sharing to satisfy the requirements of Internet of vehicles scenarios.

Keywords: consensus optimization, internet of vehicles, trust value, blockchain, efficiency of information updating

0 引言

融合物联网、人工智能等技术的智能交通技术为交通管理、自动驾驶、物流服务等提供了有力支撑。智能交通应用通过车联网^[1]可以实现车辆间和车路间通信,支持车辆及时获取环境信息,以提供各种智能交通服务。

与此同时,车联网面临诸多安全问题。且随着车联网节点增多,信息存储增加,车联网存在单点信息负载、信息安全、信息更新效率等问题^[2]。区块链^[3]具有透明性、匿名性、分布式等特点受到广泛关注,特别在交通领域,利用区块链技术可构建一个安全可靠的交通系统,解决数据存储、隐私安全、数据篡改和身份验证等问题^[4-5]。同时可结合信任机制、智能合约、机器学习等第三方技术进一步解决安全等问题。Chen^[6]等利用信任管理构建双层区块链进行数据共享,确保数据传输安全并提出相关激励措施鼓励节点间信息共享,同样 Yang^[7]等为车辆赋予信任值,并以此判断信息虚假情况且利用节点信任值激励车辆表现良好;可在传输存储数据时,保证数据安全的前提下,通过智能合约^[8-9]、机器学习,合理分配共享数据。

引入区块链解决系统安全性问题时,系统需要消耗大量计算开销、数据存储等满足数据共享服务。其中对于数据存储更新问题,当全网信息同步更新时,随着车联网节点增多,车辆速度变化快,当数据共享网络信息同步速度不匹配车辆节点移动速度时,时延问题可能会造成不同区域信息不一致、车辆得到无意义旧数据等问题。

综合上述车联网中安全性与信息更新等问题,本文主要工作如下。

1) 提出基于区块链与信任值的 RSU 分层代理框架,在网络结构分组的基础上,将区块链应用于车联网中,解决单点信息存储及安全等问题。

2) 提出基于信任值的 RSU 链分层代理信任共识优化,在信任值的基础上通过选举组领导节点,并在领导间进行全网信息同步更新,提升信息更新效率,减少系统时延,满足车辆节点获取最新信息的需求。

3) 从通信复杂度、算法时延、容错率和安全性等方面进行实验分析,验证本文提出方案的正确性。

本文对比了 4 种共识结构后挑选出最符合场景需求的共识结构——自下而上的共识结构,并提出分层共识中领导节点选取算法,保证系统安

全性, 实验证明所提方案在通信复杂度、时延、容错率及安全方面均表现良好。

1 相关技术研究现状

车联网作为互通网络, 可通过感知层收集、上传各类交通数据来服务于数据共享。为进一步加强车辆间合作共享道路信息, 提升交通效率, 研究者采用集群方式增强沟通^[9-10], 并设计相应安全协议。但交通道路中车辆数目、交通数据增加, 将造成存储压力、数据安全等问题。将区块链技术应用在车联网中^[6-8], 可解决隐私安全问题^[11], 缓解存储压力等, 同时也可利用共识等机制安全完成信息共识。

在引入区块链技术的基础上, 为进一步提升系统可靠性及效率, 研究者将区块链进行分层操作, 在分层方面, 主要有网络结构分层及共识分层。Singh 等^[12]基于区块链构建多级网络模型用于安全监控, 确保身份信息安全, 增强系统可靠性, 但增加了系统管理开销。Rashid 等^[13]提出基于区块链技术的多层安全网络模型, 利用遗传算法、粒子群优化算法等, 将网络划分为 K 个集群, 并选举出群领导组成公有链同步信息, 但在具体物联网场景下随着网络规模增大, 公有链进行共识则会造成一定网络时延。Hou 等^[14]构建多层区块链, 将用户根据一定安全级别进行分组, 将不同层级的数据存储至相应层级的链中, 从而实现安全的数据访问控制。同样, 为保证数据安全、可追溯, Aujla 等^[15]和丁庆洋等^[16]针对车联网和市场产品将区块链分层, 减少系统时延开销。但是目前研究大多数针对网络结构分层, 为进一步减少时延, 可以在结构分层的基础上进行共识优化。

在针对共识优化的研究中, 为进一步保证共识算法安全性、伸缩性, 符合不同场景需求, 将需解决问题及解决方案总结, 如表 1 所示。

针对共识问题的探讨主要分为两部分, 即系统性能与安全性。在性能方面, 有研究者关注到共识顺序^[10], 传统拜占庭协议要求正确节点达成一致, 但忽略具体达成协议的顺序, 研究者赋予节点信任值, 依据信任值对顺序进行探究; 在针对共识中带宽与存储的要求, PoS (proof of stake)

的多重签名算法 Pixel^[17]可大幅度减少开销; 为进一步降低共识复杂度, 研究者对共识结构做出优化, 利用聚类算法^[18]将节点进行分组并选出组领导节点, 组内共识后, 领导节点进行共识。利用相同思路, 可将双层共识结构推广至多层, Li 等^[19]在提出双层协议后, 探究其可伸缩性。在提升系统性能的同时, 仍需确保安全性, 由于异步协议相较于同步协议更能保证系统安全性, 如在抵抗 DDoS 攻击时具有更强的鲁棒性, 因此 Duan 等^[20]进一步提出异步共识协议, 并在吞吐量、时延方面做优化; 推广后做出分析。在上述方案中仍需考虑具体场景的结构问题。

表 1 共识优化解决方案
Table1 Solution of consensus optimization

解决问题	解决方案
扩容、可伸缩性	Bitcoin-NG、双层共识 ^[19] 、conflux
分片技术	ELASTICO ^[21]
异步性	Honeybadger ^[22] 、BEAT ^[20]
结构优化	K-PBFT ^[18] 、双层共识 ^[19]
开销	针对 PoS 的多重签名算法 Pixel ^[17]

本文主要解决车联网场景中高效共识问题, 随着车辆节点增多, 如何在车辆高速移动环境下完成信息共识, 即车辆在区域间移动时可保证数据同步更新且一致成为关键。其中共识结构优化可减少全局共识时延, 提升信息共识效率。针对共识结构分层, 当前解决方案主要有: 双层结构^[19] (可拓展至多层)、聚类结构^[18]、树形结构^[23]等, 为进一步筛选出适应本场景的结构, 本文对具体结构进行了分析比较。

2 基于信任值的 RSU 链分层代理共识优化协议

本节首先介绍系统模型, 在对比传统结构后, 为本场景选择最适合结构, 并介绍了分层中组领导节点选取算法, 最后给出了分层协议流程。

2.1 基于区块链的车联网系统模型

由于协议主要研究车联网共享信息时同步更新效率, 因此该车联网系统主要由两部分组成, 即路边单元 (RSU, road side unit), 以及装备车载单元 (OBU, on-board unit)。系统模型如图 1

所示, 车辆可从授权信任中心注册并获取初始信任值, 在信息共享过程中, 基站可根据车辆表现情况进行信任值更新, 为确保车辆进入下一个区域前, 基站维护的车辆信任表得到及时更新, 基站链需快速安全地实现信息共识。

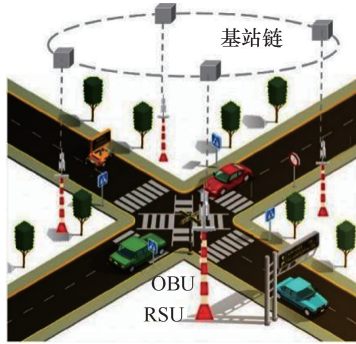


图1 系统模型
Figure 1 Model of system

本文主要研究信息同步问题, 因此将围绕如下主体进行研究。

OBU: 在车联网中代表车辆, 是分享交通信息的主体, 车辆每次采取就近原则与距离最近的RSU通信。

RSU: 在系统设计中, 在关键路口处会放置RSU, 用来收集车辆发送来的关于此路口的交通信息, 并且所有的RSU组成基站链, 用来同步RSU维护的车辆信任列表, 在区块链技术的基础上, 同步车辆信任值列表。这些基站都拥有相同的计算力。

信任管理: 在车联网中车辆共享交通信息时, 为确保共享信息过程中车辆的隐私安全性, 可为每辆车颁发假名保证通信匿名, 并为每辆车设置信任值, 辅助判断交通信息的正确性。本文考虑车辆信任值保存在RSU链中利用区块链去中心化、可追溯性等特点做网络统一管理, 与其他方案不同的是, 本文系统模型的车辆不知道本身信任值, 信任值只存于RSU链中, 可继续服务于辅助交通信息判断等。由于本文以共识结构优化为主, 因此以RSU链为主要介绍对象, 对其中的全网共识统一信任信息做出研究。

2.2 分层共识结构对比

在当前共识结构中, 所有节点为一组共同参与PBFT算法; 也有采用分层类型、树形结构等来优化共识协议, 以适应各种场景达到高效需求。

在车联网协议中, 需考虑如下指标。

(1) 速度

由于车辆移动速度快, 在到达下一个基站, 车主有可能上传交通信息, 因此时延为重要参考因素。

(2) 网络容错率

在车联网交通数据共享协议中, 在保证安全的前提下, 使更多节点参与。

(3) 通信复杂度

随着通信复杂度的增加, 时延成正比增加。

本文将从上述3个方面展开与其他方法中所提模型进行对比, 从而为本场景提出最佳共识结构。

(1) 两层PBFT共识协议

两层共识协议分为自下而上和自上而下两种共识结构。

1) 自下而上的两层协议共识结构, 如图2所示。

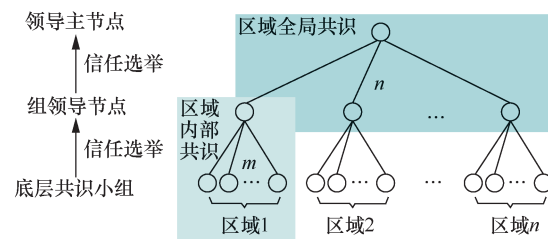


图2 自下而上两层协议共识结构
Figure 2 The structure of bottom-up two-layer consensus protocol

首先进行区域划分, 在确定组领导节点后, 所有组领导节点在组成第二层即领导层。采取此种方式共识, 需先在组内进行共识, 当组领导节点在第一轮共识确认阶段收到了超过2/3的节点消息时, 向领导主节点发出请求, 领导主节点将请求排序后广播进行第二轮共识。在第二轮共识中, 组领导节点在确认阶段收到2/3节点消息时, 即可回复与广播至组内。

2) 自上而下的两层共识结构, 有学者提出自上而下共识协议^[19], 具体应用在本场景中, 其结构如图3所示。

对于自上而下共识来说, 与本文分层(自下而上)一样首先要进行区域划分, 并且在区域划分时, 要考虑通信复杂度问题。从理论上分析, 采取自上而下共识时, 基站首先将更新信息打包, 向领导主节点发出申请, 在领导层共识完成后, 各个组领导节点仍需将更新信息广播至域内进行

第二次共识, 假设有 m 组, 则共需要进行 $m+1$ 次共识操作。但是在自下而上协议中, 考虑到可信度问题, 即组领导节点在域内共识完成后需交给领导主节点进行第二次共识, 在领导层共识中, 当其他域组领导节点接收到 $2f+1$ 个确认信息后, 可直接向域内广播, 不再进行共识, 即本文提出的自下而上的协议只需要两次共识, 因此在通信复杂度方面优于前者。

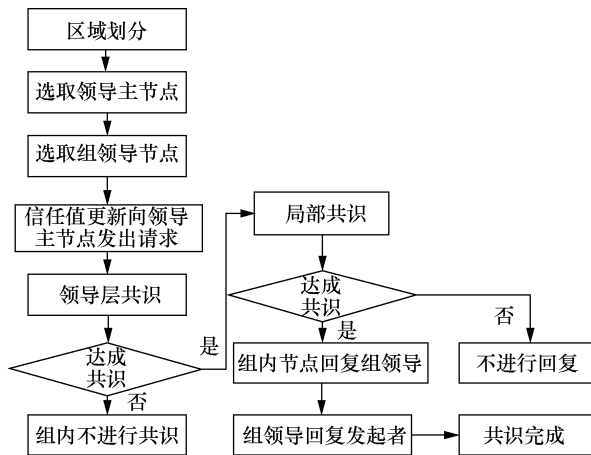


图 3 自上而下两层共识协议结构

Figure 3 The structure of top-down two-layer consensus protocol

(2) 基于树形网络拓扑结构 PBFT 共识算法

树形共识协议^[23]结构如图 4 所示, 在树形共识协议中, 只有最底层子网运行完整的 PBFT 协议, 高层子网在共识时, 将准备阶段与确认阶段结合。树形结构的提出可以降低通信复杂度。但是在树形结构中, 可靠性成为关键问题, 并仍然存在下述问题。首先, 树形结构确认, 树形结构建立在全网的基础上, 依据信任值进行统一划分, 但在实际车联网场景中, 按照区域 (地理位置) 划分更符合实际场景需求。其次, 参数确定, 在构建网络时, 假设每个子网中有 k 个节点, 则树形结构为满 $k-1$ 叉树, 文献[23]给出通信复杂度公式, 但对于层数确定和子网内节点数目的确定, 以达到最小通信量, 文中没有给出解决方案。最后, 动态调整问题, 在车联网场景下, 基站是确定因素, 但车辆是不可预测性因素, 因此基站可信度一直处于动态变化中, 如果采用树形结构, 则每完成一次共识, 需要重新评估各个基站信任值, 进行动态调整。

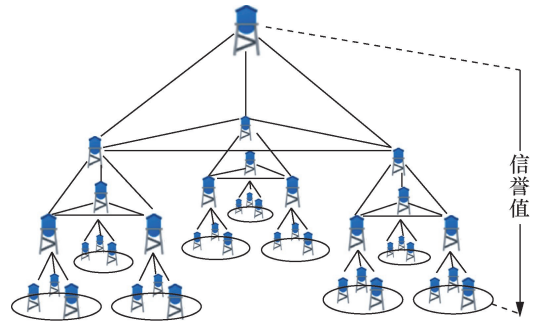


图 4 树形共识协议结构

Figure 4 Tree consensus protocol structure

(3) 基于聚类算法的 K-PBFT 共识机制

在聚类算法 K-medoids 的基础上, 与 PBFT 相结合形成 K-PBFT 机制^[18], 其思想为: 首先将社会公信度较高的节点作为集群中心点, 并且中心节点改动概率较小, 其余节点则根据聚类中心, 采用相似度 (距离等) 算法, 找到所属中心, 完成聚类工作; 其次, 在聚类完成后, 节点首先向各个集群中心点提出申请, 在组内完成共识后, 在主节点层进行第二次共识操作, 当主节点层达成共识后, 主节点广播至集群内。聚类共识协议结构如图 5 所示。

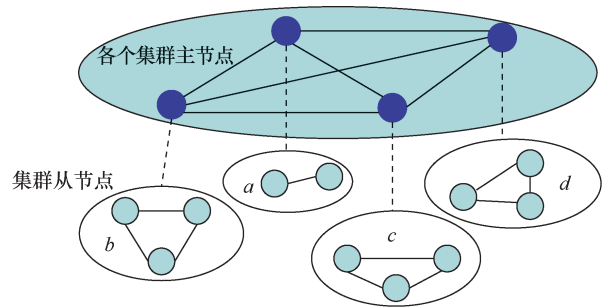


图 5 聚类共识协议结构

Figure 5 Clustering consensus protocol structure

在具体车联网场景下, 按照聚类思想可以将距离较近的基站聚为一类。其优点为在两层共识结构的基础上, 可以加一层监管机构, 使得每一次信任值得到监督, 但存在中心节点更换问题与聚类参数确定问题。原始方案中可以根据相似度进行聚类, 但在车联网中, 基站之间在地理位置、完成度方面可能存在差异, 在计算能力方面相当, 并且可信度还与周围车辆有关, 因此在相似度方面, 距离因素占主导地位, 即聚类退化为按照区域划分。

不同共识协议结构性能对比如表2所示。

表2 不同共识协议结构性能对比
Table 2 Comparison of structure and performance of different consensus protocols

共识结构	通信复杂度	容错率
自下而上共识(本文方案)	$C = 2n^2 + 2m^2 - 2n - m + mn$	下层: $n/3$ 上层: $m/3$
自上而下共识 ^[19]	$C = (m+1)^2 + m(n+1)^2$	下层: $n/2$ 上层: $m/3$
树形结构 ^[23]	$C = s'2k^2 + (s-s')(k^2 + 2k - 1)$	$n/3$
单层共识	$C = 2n(n-1)$	$n/3$
K-PBFT ^[18]	$C = 2n^2 + 2m^2 - 2n - 3m + mn$	下层: $n/3$ 上层: $m/3$

其中, m 代表组数, n 代表组内节点个数, s' 代表最底层子网树, s 代表总子网数, k 为子网中节点个数。不同共识协议结构优缺点对比如表3所示。

在优化单层结构的基础上, 考虑到容错性、速度以及基站可信度等问题, K-PBFT 及树形结构存在参数不确定、动态结构调整复杂等问题, 造成一定系统时延开销, 考虑到车联网场景对时延要求较高, 因此从双层结构进行考察。在两种双层结构中, 为保证速度快、扩展性强, 即随车辆高速运动, 网络结构需有良好扩展性以适应拓扑结构的快速变化, 本文采用自下而上的双层共识协议。

2.3 基于信任值的 RSU 组领导节点选举

综合车辆与基站考虑, 其组领导选举主要因素有节点参与程度、工作完成情况及消息价值度。相关定义如下。

定义1 节点参与程度 b , 其中每个基站的活跃程度, 都由其参与节点决定, 车辆活跃度可与其发送消息频率有关, 则对于第 i 个基站 RSU_i , 其参与程度集合为 $\beta = \{b_1, b_2, b_3, \dots, b_n\}$, 其中 b_n 表示在 Δt 时间内第 n 辆参与车辆的发送消息频率, 则每个基站的参与程度指标 B 计算如式(1)所示。

$$B = \frac{\sum \beta}{n} = \frac{\sum_{i=1}^n b_i}{n} \quad (1)$$

定义2 节点共识完成率 C , 表示基站在共识中表现情况, 假设 RSU 基站完成事件个数为 s , 未完成事件个数为 f , 则节点共识完成率 C 计算如式(2)所示。

$$C = \frac{s}{s+f} \quad (2)$$

定义3 平均每条消息价值度 V , 在固定的选举周期 Δt 内, 假设 RSU 共处理事件 n 件, 其事件集合为: $M_{\Delta t} = \{M_1, M_2, M_3, \dots, M_n\}$, 对于每个事件发生概率, 根据贝叶斯公式评定集合为 $P_{\Delta t} = \{P_1, P_2, P_3, \dots, P_n\}$, 并且所有参与车辆的信任值集合为 $T_{\Delta t} = \{T_1, T_2, T_3, \dots, T_n\}$, 其中 T_n 代表对于事件 n , 参与车辆信任值集合, 假设参与事件共 i 辆车, 表示为 Num_of_ i , 则 $T_n = \{t_1, t_2, t_3, \dots, t_i\}$ 。在知道上述条件情况下, 基站 RSU 的平均每条消息价值度表示如下。

$$V = \frac{\sum_{i=1}^n P_i T_i}{\text{Num_of_}i} \quad (3)$$

定义4 区域 i 的基站 j 的可信度 D_{ij} , 将上

表3 不同共识协议结构优缺点对比
Table 3 Comparison of advantages and disadvantages of different consensus protocol structures

共识结构	存在问题	对比原有单层结构改进后的优点
双层共识	需要增添额外协议保证安全	自下而上: 两次共识减少通信复杂度, 速度最快, 扩展性强
	车联网场景下共识次数可继续减少	自上而下 ^[19] : 通信复杂度低, 扩展性强, 确定条件下容错率高, 速度快
树形结构 ^[23]	可靠性问题、层次确定、动态调整复杂度	通信复杂度降低, 树形结构易扩展
单层共识	速度慢、时延长	—
K-PBFT ^[18]	K 值确定问题、通信复杂度最小确定问题、中心节点更换问题	相似度聚类便于监督管理, 降低通信复杂度, 速度快

述可信度影响因子综合起来,在每次选举领导节点时,区域 i 的基站 j 的可信度如式(4)所示,其中 n 代表基站 j 收集交通信息的参与车辆集,共处理事件 m 个, V'_{ij} 表示前一次可信度的测量值。

$$D_{ij} = B_{ij} \cdot V_{ij} \cdot C_{ij} + (1 - C_{ij})V'_{ij} = \frac{\sum_{k=1}^n b_k}{n} \cdot \frac{s}{s+f} \cdot \frac{\sum_{k=1}^m P_k \cdot T_k}{n} + \frac{f}{s+f} \cdot \frac{\sum_{k=1}^m P'_k \cdot T'_k}{n'} \quad (4)$$

2.4 分层共识过程

在实际车联网运行环境中,考虑车辆活动范围,离车辆较远地区的基站,则可以暂时不更新。因此分层共识协议中,事务排序需增加距离、信任度等进行衡量,并在分层共识选举领导时,引入可信度,基站可信度的衡量主要依赖车辆与基站本身,其分层共识协议流程(如图6所示)如下。

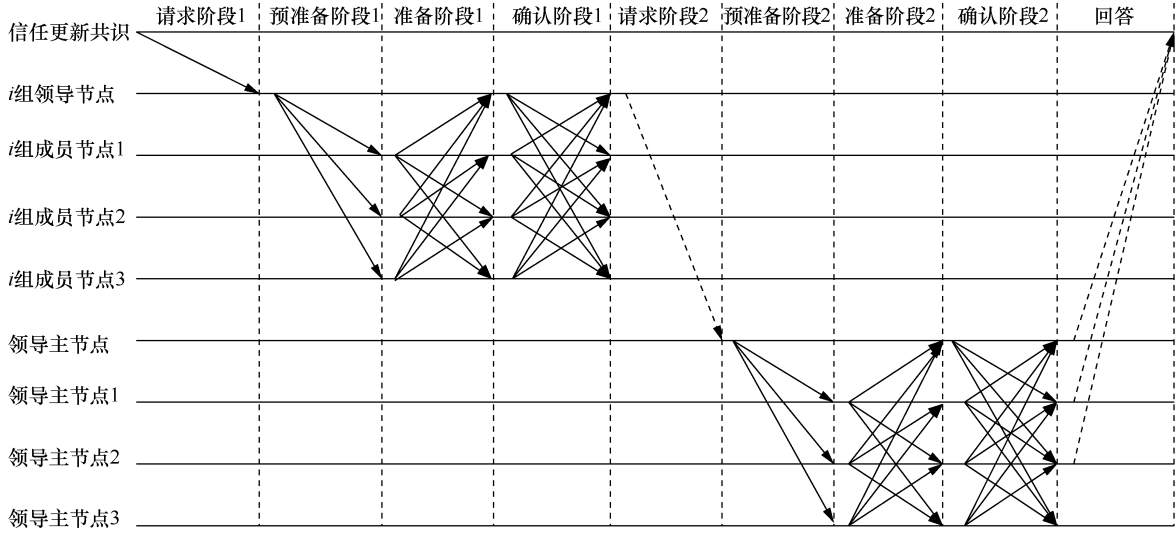


图6 分层共识协议流程
Figure 6 Process of hierarchical consensus protocol

选举组领导节点,进行局部共识,局部共识后,在组领导节点中选举可信度最高节点作为领导主节点(见2.3节),进行全局共识。

1) 区域划分:根据通信复杂度计算公式,计算出最佳分组数目。

2) 选举组领导节点:依据信任度影响因子进行可信度评估,选举出每个区域可信度最高的RSU基站作为组领导节点。

3) 局部共识。

① 提出请求,假设对于基站 i 有 n 辆车需要进行信任值更新,则申请消息为: $m: (t'_{i1}, t_{i1}), (t'_{i2}, t_{i2}), (t'_{i3}, t_{i3}), \dots, (t'_{in}, t_{in}) >_{\sigma_i}$, 其中 σ_i 为签名。

② 预准备阶段,领导节点对收到的请求分配序列号,向组内所有节点群发预准备消息 $<< \text{PRE-PREPARE}, v, n, d >_{\sigma_{\text{leaderi}}}, m >$, 其中 m 表示请求消息, v 表示视图编号, n 表示序列号,

d 表示请求消息的摘要,组领导节点将上述消息签名打包后进行签名,并附上消息 m ,广播至组内。

③ 准备阶段,当节点接受预准备消息时,信息验证准确后节点接受预准备消息进入准备阶段。此时节点向组内所有节点广播准备消息 $< \text{PREPARE}, v, n, d, i >_{\sigma_i}$ 。

④ 确认阶段,当节点收到来自 $2f+1$ 个准备消息时对每条消息做上述验证,验证均正确时,进入确认阶段。此时节点将 $< \text{COMMIT}, v, n, D(m), i >_{\sigma_i}$ 广播到域内,当组领导节点收到超过 $2f+1$ 个确认消息,且验证通过时,完成确认阶段,此时组领导节点将向领导主节点发出申请。

4) 选取领导主节点,领导主节点的选取与组领导选举相同,即选取可信度最高的节点作为领导主节点。

5) 进入全局共识,在全局共识中,与局部共

识相似，组领导节点将一定时间此区域内需要更新的信任值列表打包发出申请， $m \leq (t'_{i1}, t_{i1}), (t'_{i2}, t_{i2}), (t'_{i3}, t_{i3}), \dots, (t'_{in}, t_{in}) >_{\text{leader}}$ 。其中 σ_{leader} 为领导主节点签名。并且在领导层进行全局共识，同样经过预准备阶段、准备阶段、确认阶段。详细过程与组内共识类似，不再赘述。

6) 回复消息与域内广播，当第二层共识节点，即各个域组领导节点收到 $2f+1$ 条确认消息，并且消息均通过验证，向提出申请基站进行回复，同时各个组领导节点进行域内信任值列表更新广播。

3 实验结果与分析

本文实验将从安全性、通信复杂度、时延、容错率方面对车联网所需指标进行分析。

3.1 安全性分析

(1) 安全目标

1) 基于 RSU 身份签名消息的不可伪造性，在共识过程中，请求、预准备、准备等阶段中，RSU 为身份唯一的半可信实体且签名采用其私钥，因此基于 RSU 签名具有不可伪造性。

2) 对安全攻击的抵抗性。本文所提共识协议，可抵抗重放攻击、中间人攻击、女巫攻击、日蚀攻击、窃听及篡改攻击等。

3) RSU 身份不可伪造性。RSU 作为半可信实体，不会借用其身份主动发起攻击，且 TA 与 RSU 间传输信道安全，在初始 TA 为其颁发身份时，敌手无法获取。

4) RSU 共识数据不可篡改性。当 RSU 被敌手控制时，篡改数据库，将虚假消息进行共识请求，RSU 在摆脱攻击后应能恢复数据库并进行正确信息共识，覆盖原有错误信息。

(2) 攻击模型

从攻击者角度分析，下面将从两类攻击模型展开讨论。

1) 底层节点，由于节点分层时以地理位置划分，因此底层攻击者可根据实际地理位置，控制邻近 RSU，且由于节点在参与程度、工作完成情况、消息价值度等衡量指标中是不确定且动态改变的，因此底层节点共识与普通拜占庭容错共识一样。二者容错率都为 $1/3$ ，所以当

敌手控制组内 $2/3$ 以上节点时，即可完成组内攻击；如果敌手控制底层节点被选举成组领导节点，即可对更新数据进行篡改攻击等，并扰乱第二轮共识。

2) 领导层节点，当敌手控制组领导节点，此时在第一轮共识的基础上，敌手可更改信息，扰乱第二次共识；领导层节点完成共识后，敌手在组内广播信息时展开攻击。

(3) 正确性分析

对本协议进行正确性分析时，主要判断所提共识协议结构是否满足安全目标。

1) 基于 RSU 身份签名消息的不可伪造性、RSU 身份具有不可伪造性。由于共识算法中消息包含公钥签名、消息验证编码及基于哈希函数生成的消息摘要，因此可防止消息被破坏；由于共识算法中消息包含公钥签名、消息验证编码及基于哈希函数生成的消息摘要，因此可防止消息被破坏。由于 TA 和 RSU 之间信道安全，因此敌手无法窃听其身份信息，同时不会发动与身份相关类型攻击。

2) 抗攻击分析包括对重放攻击、中间人攻击、女巫攻击、日蚀攻击的分析。由于 PBFT 共识算法本身在接受消息时，判断消息来自不同 RSU 签名消息即消息数量增一，多次重复发送无意义。针对每个 RSU，由于其作为半可信实体，签名消息无法伪造，因此可抵抗有关身份的中间人攻击与女巫攻击。并且 RSU 分组依据地理位置，因此受地理位置约束，可抗日蚀攻击。

当敌手控制底层节点时，敌手需控制组内大多数节点才可以完成篡改后消息的共识，增加敌手攻击难度，并且敌手无法提前预知。当敌手控制组领导节点，扰乱组内共识时，即收到组内大多数节点确认节点，但不上报，由于敌手控制短暂且组领导节点会进行更换，基站在一定时间内收不到回复，可再次发起共识申请；由于节点参与程度、工作完成情况、消息价值度等衡量指标为不确定因素，因此敌手无法准确锁定组领导节点；当敌手扰乱领导层共识时，敌手想控制大多数领导节点难度较高，因此系统可避免此类攻击情况。

3) 共识数据不可篡改性：当敌手控制 RSU

节点时,如果敌手篡改数据并将虚假消息进行共识,但敌手很难控制组内大多数节点,因此共识失败。敌手难以获取 RSU 身份信息,伪造共识发起请求;当 RSU 摆脱敌手控制,发现与链上多数节点数据不一致时,进行改正。

因此,本文所提共识协议结构可实现安全目标,确保系统安全性。

3.2 通信复杂度分析

在 RSU 数量一定的情况下,如何分组,即分多少组,每组多少个 RSU,才可以在总数确定的情况下尽量减少通信次数。为了找到最小值,并与原有 PBFT 方案进行对比,本文将通信过程次数做出如下假设:

假设一共分为 m 个共识小组,每组中有 n 个 RSU,则在 PBFT 的 3 个阶段中,每个阶段的开销分析如下。

子群在第一次共识时,首先进行 PBFT 共识。

(1) 预准备阶段,每小组主节点将消息广播至各个节点,此时通信开销为 $n-1$ 。

(2) 准备阶段,此时各个收到消息的 RSU 节点会向组内除了自己节点外发送验证消息,此时开销为 $(n-1)(n-1)$ 。

(3) 确认阶段,在这个阶段中,所有节点收到了上一个阶段中其他节点发来的验证消息,节点进行确认,并统计收到消息数量,此时开销为 $n(n-1)$ 。

进行第二层节点共识,由于有 m 个小组参与共识,因此在第二层中共有 m 个节点参与。

(1) 预准备阶段,当每个小组信任度最高的主节点接收到小组内的确认反馈时,将此条消息广播至第二层所有节点中,此时通信开销为 $m-1$ 。

(2) 准备阶段与确认阶段的通信开销与底层第一轮共识类似,则其通信开销为 $m(m-1)+(m-1)(m-1)$ 。

(3) 回复与广播阶段,当各个组领导节点完成共识需要回复请求基站,通信量为 m ,且各个组领导节点需要在域内进行共识,则开销为 mn 。

将两轮共识完整实现之后,从客户端向主节点发出请求到主节点完成共识广播至域内,总通信复杂度如式(5)所示。

$$C = 2n^2 + 2m^2 - 2n - m + mn \quad (5)$$

其中,假设总节点数为 T ,则 $T=mn$,将 m 用 T/n 替换,则可得式(6)。

$$C = 2n^2 + 2T^2 / n^2 - 2n - T / n + T \quad (6)$$

此时根据求导公式,求出极值点找到其中合适的点,即可在确保通信复杂度最低的情况下获得最佳小组 RSU 数目。

在分层数目与组内成员个数相同的情况下,本文进一步与文献[19]提出的自上而下分层结构方案进行通信复杂度比较,对比结果如图 7 所示。从图 7 中可以看出,自下而上的方案更有利于通信复杂度的降低。

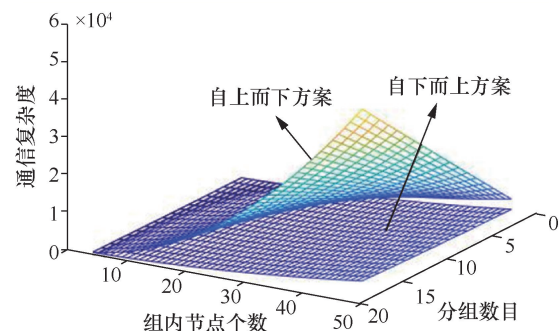


图 7 通信复杂度对比实验示意
Figure 7 Comparison experiment of communication complexity

3.3 分层共识算法时延对比

为了实际研究分层共识的速度提升变化,本实验采用 Java 环境模拟两层协议,实验硬件配置如表 4 所示。在 Java 环境模拟中,节点位置在一定范围内随机生成,并且节点间通信时延与节点间距离成正比。本实验将分组设定为 3,然后与原协议时间对比。本文提出的双层共识协议与单层 PBFT 协议在时间上的对比如表 5 所示。

表 4 实验硬件环境配置
Table 4 Experimental hardware environment configuration

配置项目	配置条件
CPU	Intel(R)Core(TM)i5-4210H
内存	8 GB
操作系统	Windows10 64 位
硬盘	512 GB
显卡	NVIDIA GeForce GTX 950M

表5 双层共识协议与PBFT协议时间对比
Table 5 Time comparison between two-layer consensus protocol and PBFT protocol

分组情况	节点总个数	分层时间/ms	不分层时间/ms
3×13	39	35	51
3×22	48	48	66
3×31	93	46	79
3×34	102	50	108
3×40	120	51	109
3×46	138	67	112
3×52	156	69	121
3×61	183	80	195
3×67	201	98	190

双层共识协议与PBFT协议时延对比如图8所示。

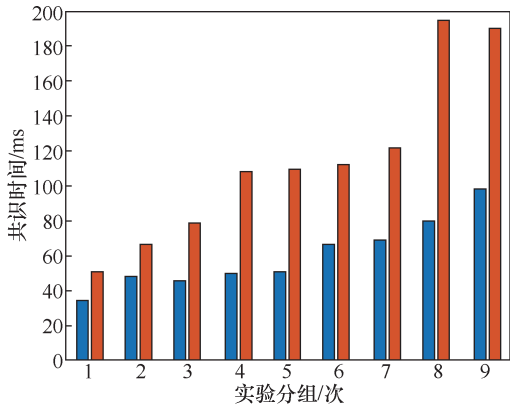


图8 双层共识协议与PBFT协议时延对比
Figure 8 Comparison diagram between the two-layer consensus protocol and PBFT protocol

可以看出,采用分层结构,可大幅度减少时间开销,在最后一组实验中,201个节点的不分层时间比183个节点多,这是因为随着节点个数增加,在模拟实验中,当每次通信超过一定时间限制时则认为超时,即认为投票失效,所以在节点数量多的情况下,应采用分层结构,这样不仅能缩短时间,还能降低节点超时率。

3.4 容错率分析

采用两层共识协议,达成共识的条件为:在底层组内达成共识的前提下,领导层也完成共识。因此,假设事件 $P(A)$ 为底层组内达成共识,事件 $P(B)$ 为领导层达成共识,事件 $P(C)$ 为最终达成共识,则 $P(C) = P(A)P(B|A)$ 。

在本文协议提出的两层共识中,底层执行经典的PBFT协议,即只要有不超过 $1/3$ 的失效节点,即可成功达成共识。而对于领导层节点来说,在第二层共识时,只要对应组领导节点共识通过,那么组内不需要再进行共识,可以直接广播信任更新信息。因此对于领导层节点来说,其是否接受共识,取决于其失效概率。事件 A 的概率值如式(7)所示。

$$P(A) = \sum_{i=0}^{n/3} C_n^i (1 - P_f)^{n-i} P_f^i \quad (7)$$

其中, P_f 为节点失效概率。

假设在 m 个组中,有 j 组完成了共识,即第二层共识中,有 j 个组领导节点参与,则进入第二轮共识的条件为 $m/3 < j \leq m$ 。则得式(8)。

$$P(B|A) = \sum_{j=m/3+1}^m C_m^j (1 - P_f)^j \cdot P_f^{m-j} \quad (8)$$

事件 A 发生概率如图9所示($n=30$)。

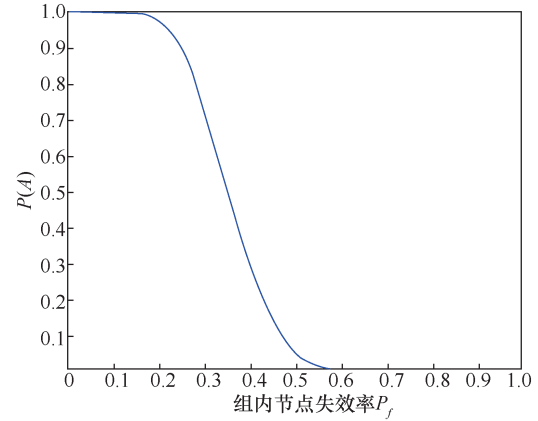


图9 事件 A 发生概率
Figure 9 The probability of event A

根据式(8)可推得式(9)。

$$\begin{cases} P(C) = \sum_{j=m/3+1}^m C_m^j P(A)^j (1 - P(A)^{m-j}) (1 - P_f)^j P_f^{m-j} \\ P(A) = \sum_{i=0}^{n/3} C_n^i (1 - P_f)^{n-i} P_f^i \end{cases} \quad (9)$$

事件 C 发生概率($m=30, n=30$)如图10所示,将自下而上方案与自上而下方案^[19]进行比较,如图11所示。

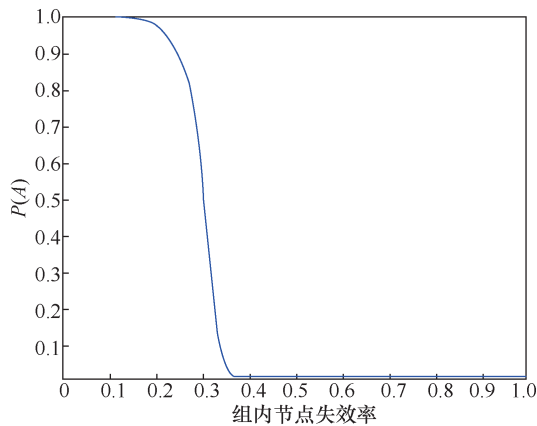


图 10 事件 C 发生概率
Figure 10 The probability of event C

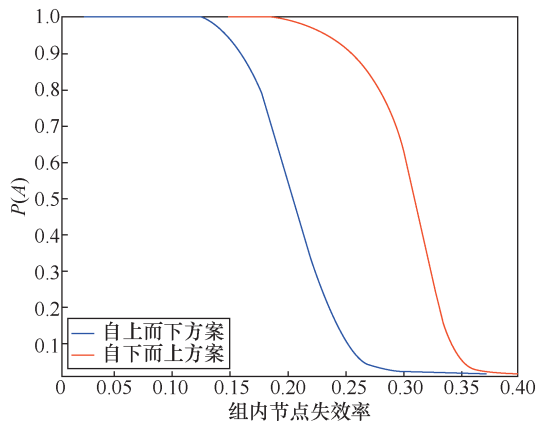


图 11 事件 C 发生概率对比
Figure 11 Comparison of the probability of event C

从图中可看出, 本文方案的容错率更高。在节点失效率达到 0.4 时, 成功率趋于 0, 但在自上而下方案中, 当节点失效率为 0.3 时, 成功率趋于 0。由于在车联网中, 基站需要完成收集交通信息, 计算信息发生概率以及信任更新共识等任务, 在共识过程中, 考虑到信任值更新需要一个基站出发, 更新至全网, 即需要尽可能多的节点参与并成功达成共识, 因此, 需要容错率高的协议。

4 结束语

车联网作为智能交通基础平台, 为解决其数据安全问题的, 可引入区块链技术, 针对实际场景应用中, 为了符合速度、容错率以及减少通信量的需求, 在原有共识结构上进行改造。在对比 4 种典型结构后, 挑选出最符合场景需求的共识结构——自下而上的共识结构。并且划分区域, 引

入车辆信任值、车辆活跃度等因素, 提出了相关领导节点选取算法等。在上述基础之上, 设计具体分层共识步骤。实验验证本文所提双层共识结构符合本场景安全需求; 在确定通信复杂度情况下优于自上而下方案, 同样相较于此方案, 确保安全的前提下, 增大容错率尽量让尽可能多的节点参与, 更适合本场景; 相较于原共识方案, 随着节点数量增多, 可将时延缩短 1/2 以上。综上所述相较于其他结构, 本文提出的自下而上的分层共识结构最适用于本场景。在今后工作中, 可将双层协议拓展至多层, 同时, 也可根据周围车辆信任值考虑共识顺序问题, 进一步提升共识效率, 并对基站进行统一管理工作, 提升系统整体安全性。

参考文献:

- [1] CONTRERAS-CASTILLO J, ZEADALLY S, GUERREIRO-IBÁÑEZ J A. Internet of vehicles: architecture, protocols, and security[J]. IEEE Internet of Things Journal, 2018, 5(5): 3701-3709.
- [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] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[EB].
- [4] CHEN J, YAO S X, YUAN Q, et al. CertChain: public and efficient certificate audit based on blockchain for TLS connections[C]//Proceedings of IEEE INFOCOM 2018 - IEEE Conference on Computer Communications. 2018: 2060-2068.
- [5] DORRI A, STEGER M, KANHERE S S, et al. BlockChain: a distributed solution to automotive security and privacy[J]. IEEE Communications Magazine, 2017, 55(12): 119-125.
- [6] CHEN C, WANG C, QIU T, et al. A secure content sharing scheme based on blockchain in vehicular named data networks[J]. IEEE Transactions on Industrial Informatics, 2020, 16(5): 3278-3289.
- [7] 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.
- [8] WANG S M, YE D D, HUANG X M, et al. Consortium blockchain for secure resource sharing in vehicular edge computing: a contract-based approach[J]. IEEE Transactions on Network Science and Engineering, 2021, 8(2): 1189-1201.
- [9] XIAO H L, CHEN Y H, ZHANG Q Y, et al. Joint clustering and power allocation for the cross roads congestion scenarios in cooperative vehicular networks[J]. IEEE Transactions on Intelligent Transportation Systems, 2019, 20(6): 2267-2277.
- [10] ALSARHAN A, KILANI Y, AL-DUBAI A, et al. Novel fuzzy and game theory based clustering and decision making for VANETs[J].

- IEEE Transactions on Vehicular Technology, 2020, 69(2): 1568-1581.
- [11] FAN K, PAN Q, ZHANG K, et al. A secure and verifiable data sharing scheme based on blockchain in vehicular social networks[J]. IEEE Transactions on Vehicular Technology, 2020, 69(6): 5826-5835.
- [12] SINGH A K. A multi-layered network model for blockchain based security surveillance system[C]//Proceedings of 2020 IEEE International Conference for Innovation in Technology. Piscataway: IEEE Press, 2020: 1-5.
- [13] RASHID M A, PAJOOH H H. A security framework for IoT authentication and authorization based on blockchain technology[C]//Proceedings of 2019 18th IEEE International Conference on Trust, Security and Privacy In Computing and Communications. 2019: 264-271.
- [14] HOU Y C, LIU W X, LIN H, et al. Multi-layer access control mechanism based on blockchain for mobile edge computing[J]. 2020 IEEE Intl Conf on Parallel & Distributed Processing With Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking, 2020: 285-291.
- [15] AUJLA G S, SINGH A, SINGH M, et al. BloCkEd: blockchain-based secure data processing framework in edge envisioned V2X environment[J]. IEEE Transactions on Vehicular Technology, 2020, 69(6): 5850-5863.
- [16] 丁庆洋, 朱建明, 张瑾, 等. 基于双层架构的溯源许可链共识机制[J]. 网络与信息安全学报, 2019, 5(2): 1-12.
DING Q Y, ZHU J M, ZHANG J, et al. Traceability permissioned chain consensus mechanism based on double-layer architecture[J]. Chinese Journal of Network and Information Security, 2019, 5(2): 1-12.
- [17] DRIVERS M, 0001 S G, NEVEN G, et al. Pixel: multi-signatures for consensus[J]. IACR Cryptology EPrint Archive, 2019, 2019: 514.
- [18] 陈子豪, 李强. 基于 K-medoids 的改进 PBFT 共识机制[J]. 计算机科学, 2019, 46(12): 101-107.
CHEN Z H, LI Q. Improved PBFT consensus mechanism based on K-medoids[J]. Computer Science, 2019, 46(12): 101-107.
- [19] LI W Y, FENG C L, ZHANG L, et al. A scalable multi-layer PBFT consensus for blockchain[J]. IEEE Transactions on Parallel and Distributed Systems, 2020, 32(5): 1146-1160.
- [20] DUAN S S, REITER M K, ZHANG H B. BEAT: asynchronous BFT made practical[C]//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. New York, NY, USA: ACM, 2018: 2028-2041.
- [21] LUU L, NARAYANAN V, ZHENG C D, et al. A secure sharding protocol for open blockchains[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. 2016: 17-30.
- [22] 包振山, 王凯旋, 张文博. 基于树形拓扑网络的实用拜占庭容错共识算法[J]. 应用科学学报, 2020, 38(1): 34-50.
BAO Z S, WANG K X, ZHANG W B. A practical Byzantine fault tolerance consensus algorithm based on tree topological network[J]. Journal of Applied Sciences, 2020, 38(1): 34-50.

[作者简介]



翟宝琴（1996—），女，山西太原人，北京交通大学硕士生，主要研究方向为区块链及车联网安全。



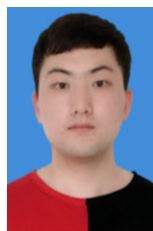
王健（1975—），男，山东烟台人，博士，北京交通大学副教授、博士生导师，主要研究方向为密码应用及区块链、网络安全。



韩磊（1983—），男，内蒙古呼伦贝尔人，博士（后），北京计算机技术及应用研究所高级工程师，主要研究方向为信息安全、密码应用、智能安全。



刘吉强（1973—），男，山东烟台人，博士，北京交通大学教授、博士生导师，主要研究方向为可信计算、隐私保护、云计算安全。



何嘉豪（1997—），男，北京人，北京交通大学硕士生，主要研究方向为区块链及数据安全存储。



刘天皓（1997—），男，北京人，北京交通大学硕士生，主要研究方向为区块链及物联网安全。