Proceedings of Machine Learning Research vol 278:1–8, 2025 2025 2nd International Conference on Machine Learning and Intelligent Computing

R-PBFT: Efficient DAG-based consensus Algorithm for Internet of Vehicles

Kedong Niu NKD@GS.ZZU.EDU.CN
School of Cyber Science and Engineering, Zhengzhou University, Zhengzhou, China

Yangjie Cao* CAOYJ@ZZU.EDU.CN
School of Cyber Science and Engineering, Zhengzhou University, Zhengzhou, China

Jie Li LIJIECS@SJTU.EDU.CN
School of Cyber Science and Engineering, Zhengzhou University, Zhengzhou, China
School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai, China

Editors: Nianyin Zeng, Ram Bilas Pachori and Dongshu Wang

Abstract

With the increase in the number of vehicles in residential households, the traffic flow on roads has shown a significant growth trend, which places higher demands on the capacity of vehicular networks. It is worth noting that the traditional PBFT algorithm experiences a significant decline in consensus efficiency as the number of nodes increases, which may pose a key constraint on the information exchange efficiency in vehicular networks. Based on this, this study proposes an R-PBFT consensus algorithm based on DAG blockchain. This algorithm optimizes the consensus mechanism and significantly improves the information transmission rate between roadside units and vehicles. Experimental results show that, compared to traditional consensus algorithms, the proposed solution effectively improves consensus efficiency while reducing communication costs.
Keywords: Internet of Vehicles, Blockchain, DAG, Consensus Algorithm

1. Introduction

The application of blockchain technology in vehicular networks provides an innovative solution for constructing distributed communication networks. It effectively addresses key issues such as data privacy protection, security, and reliability in information sharing, significantly enhancing the security capabilities of vehicular networks (Kang et al., 2018). Consensus algorithms, as a core component of blockchain, play a crucial role in ensuring consensus among distributed nodes (Li et al., 2018). Currently, a significant amount of research focuses on consensus algorithms for vehicular networks. Many of these studies rely on common consensus algorithms, including Proof of Work (POW), Proof of Stake (POS), Delegated Proof of Stake (DPOS), and Practical Byzantine Fault Tolerance (PBFT) (Liu et al., 2019). However, in vehicular networks, vehicles have limited computational resources, which prevents them from performing heavy computational tasks. Furthermore, the POS and DPOS consensus algorithms rely on tokens to determine stakes, which can lead to unfair situations (Zhang and Chen, 2019). Ayaz et al. (2020) compared POW, POS, and PBFT, and concluded that PBFT has the greatest potential for development in vehicular networks. However, traditional PBFT algorithms suffer from high communication complexity, with a communication complexity of $O(N^2)$. This means that as the number of consensus nodes increases within the network, the consensus efficiency significantly decreases. Although many studies in the field of vehicular networks are based on PBFT consensus algorithms, most of these studies are based on traditional single-chain structures (Kudva et al., 2021).

In terms of DAG blockchain, research specifically focused on DAG-based blockchain consensus algorithms is relatively scarce (Wu et al., 2022). Existing DAG-based blockchains often have more complex ledger structures and are heavily dependent on resource-intensive consensus mechanisms (Zhang et al., 2024). For example, existing DAG-based blockchains typically use Proof of Work (POW) as a consensus mechanism, confirming each new block or multiple consecutive blocks (Yang et al., 2023). While this approach helps ensure blockchain security, it inevitably leads to increased confirmation delays, which in turn affects the overall system efficiency. Therefore, combining PBFT consensus with DAG blockchain and designing a PBFT algorithm based on DAG blockchain can, on the one hand, improve the consensus efficiency of the traditional PBFT algorithm, and on the other hand, effectively avoid the resource wastage caused by the Proof of Work mechanism in DAG, making it more suitable for vehicular networks with limited resources.In order to address the issue of low consensus efficiency of the traditional PBFT algorithm in large-scale node networks, which is unable to meet the high concurrency and low latency requirements in vehicular network information sharing scenarios, the contributions of this paper are as follows:

- We proposes a two-layer network consensus algorithm based on DAG blockchain—R-PBFT. The algorithm divides the entire network into multiple local networks as the second layer and then selects master nodes from these local networks to form the first layer network.
- We designs a master node selection strategy based on the PageRank algorithm, which dynamically selects master nodes in the network based on node load conditions, thereby avoiding the issue of a single master node failure.

2. Related Work

Consensus algorithms are an essential part of blockchain technology. As a method or mechanism that can achieve consistency in distributed networks, they play an important role in maintaining the security, decentralization, and scalability of blockchain networks (Hussein et al., 2023).Due to the resource limitations inherent in vehicular networks, existing research on vehicular network consensus algorithms mainly focuses on the PBFT algorithm. Li et al. (2019) proposed the EPBFT scheme, which uses a verifiable random function to implement dynamic node selection, while optimizing the checkpoint protocol and view switching process. This allows the algorithm to maintain low communication overhead and good adaptability in dynamic networks. Xu et al. (2022) in response to the blockchain application requirements in vehicular networks, designed a distributed consensus algorithm called SG-PBFT. This algorithm optimizes the node communication mechanism, significantly reduces network transmission overhead while maintaining Byzantine fault tolerance, and achieves better throughput performance than traditional PBFT, effectively adapting to the real-time data processing requirements in the high-dynamic environment of vehicular networks. BullShark is a high-performance consensus protocol based on the Narwhal DAG, which achieves zero communication overhead by employing an anchor mechanism and garbage collection optimization, resulting in low latency and high throughput(Spiegelman et al., 2022). Tusk as an extension of Narwhal DAG, optimizes throughput through pipelined processing and lightweight broadcasting. It complements BullShark, reaching a balance between latency and performance (Danezis et al., 2022),.

3. Methodology

This paper proposes a region-based RSU organization optimization method with a two-layer network structure. In the first layer, RSUs are grouped by region, reducing communication delay and improving data transmission efficiency due to shorter spatial distances. Each region elects a master RSU to coordinate the operations of other RSUs, forming a collaborative network. This design ensures efficient local communication and global network scalability. As shown in Figure 1, the first layer consists of master nodes, while the second layer consists of regional nodes. The R-PBFT algorithm includes three stages: initialization, intra-region consensus, and global network consensus, as detailed below.

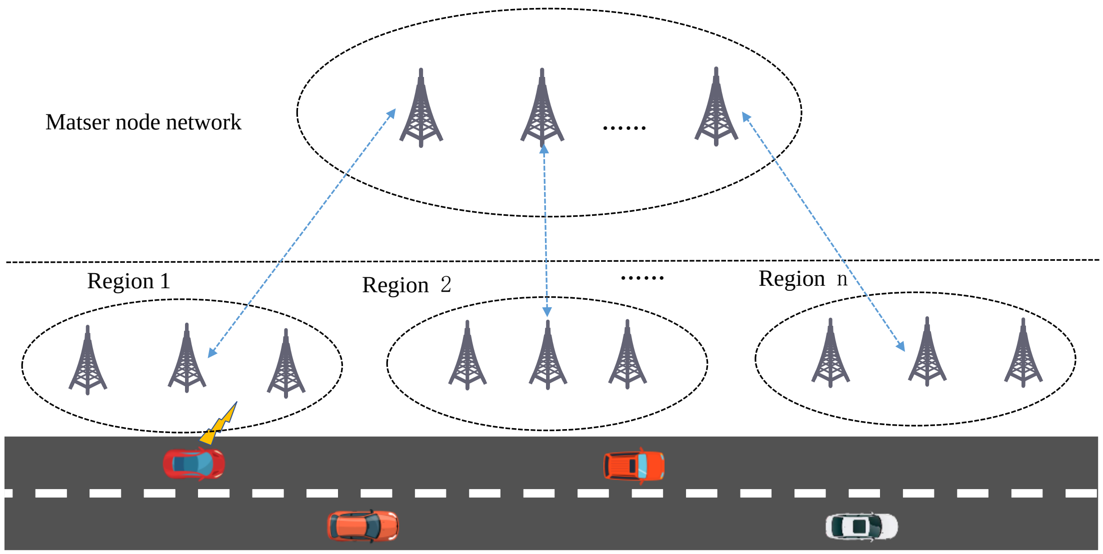

Figure 1: Consensus Algorithm Mode

3.1. The Initialization Stage

During initialization, each RSU's 160-bit unique identifier ($\mathrm{RSU}_{\mathrm{id}}$) is generated based on geolocation:

$$\mathrm{RSU}_{\mathrm{id}} = R_{ij} \parallel S_{\mathrm{random}} \tag{1}$$

R_{ij} (32-bit): *Regional encoding* where i=region ID, j=RSU index within region. S_{random} (128-bit): Unique random value, The system maintains an RSU information table with matrix-based logical structure:

$$\mathbf{R} = \begin{bmatrix} R_{11} & \cdots & R_{1j} \\ \vdots & \ddots & \vdots \\ R_{i1} & \cdots & R_{ij} \end{bmatrix} \tag{2}$$

where co-region RSUs (R_{ij}) are presumed geographically proximate with minimal communication latency.

This paper organizes RSUs within a region into a set. For region R_i, the RSU collection is defined as:

$$R_{\mathrm{i}} = \left\{ \mathrm{r}_{ij} \left| r_{i1}, r_{i2} \text{ ......}, r_{\mathrm{ij}}, 0 \leq j \leq n \right. \right\} \tag{3}$$

where n denotes the number of RSUs within region R_i.The system randomly selects one RSU as the master node within each region R_i (i.e., the RSU set of the i-th region). These elected master nodes form a master node set as defined in Equation 4, which collaborates with ordinary RSUs in the second-layer regions to construct a two-layer network structure.

$$R_{\mathrm{i}} = \{R_{\mathrm{i}}, 0 < \mathrm{i} \leq \mathrm{k}\} \tag{4}$$

In the process of electing the master node, an improved PageRank algorithm is designed to evaluate the RSU nodes within the region. The simplified formula for the PageRank algorithm is:

$$PR(A) = \frac{1-d}{N} + d \sum_{i \in M(A)} \frac{PR(i)}{L(i)} \tag{5}$$

When applied to vehicular networks, Equation 6 is obtained, where N_i represents RSU nodes in the network. The damping coefficient d denotes the probability of vehicles transmitting information to RSUs, typically set to 0.85 in this chapter. k represents the total number of RSUs in the target region. $L(N_j)$ indicates the number of outgoing links from node N_j, reflecting its connectivity with other nodes. $W(N_i, N_j)$ is a dynamic

$$P(N_i) = \frac{1-d}{k} + d \sum_{j \in M(N_i)} \frac{P(N_j) \cdot W(N_i, N_j)}{L(N_j)} \tag{6}$$

During the network initialization phase, the system acquires the number of RSUs (N) in each region, sets the damping coefficient (d), and initializes the weight function parameters ($W(N_i, N_j)$) and the (P)-values for all nodes. The (P)-values are then iteratively updated using Equation 6 until the changes in all (P)-values become negligible (below a predefined threshold), indicating convergence. The node with the highest (P)-value in each region is then selected as the master node. Given the dynamic nature of vehicular networks, where parameters frequently change, a dynamic adjustment mechanism is introduced. This mechanism periodically updates the (P)-values and dynamically reselects master nodes to adapt to time-varying network demands and traffic conditions.

3.2. The Intra-region Consensus Stage

According to the RSU information table maintained by the system, the RSUs are constructed into a two-layer network structure. The first layer is mainly composed of the master nodes of each region, while the second layer is composed of the RSU nodes within each region. RSUs in these two layers can join or exit their respective networks, after which the regional consensus phase begins. First, vehicles collect surrounding environmental information and package it into a transaction, which is then directly sent to nearby RSU nodes. These RSU nodes have independent memory pools, with each node maintaining a separate set of received transactions. The nodes retrieve transactions from the queue and send them to the master node according to their priority. The regional consensus phase uses the PBFT algorithm for consensus, with the core process including the Pre-Prepare Phase, Prepare Phase, and Commit Phase. The process is shown in Figure 2.

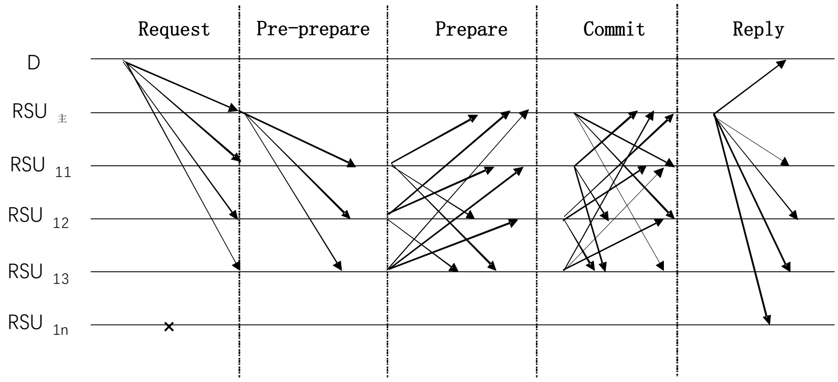

Figure 2: Flow chart of the consensus algorithm within the region

3.3. The Global Network Consensus Stage

After the RSU nodes within a specific region reach a consensus on a shared piece of information, the master node of that region will immediately forward the consensus message to the master node network, thereby transmitting the consensus result of the message to the global blockchain network. The master node network is composed of the master nodes of each region, which represent different consensus areas. When a master node of a region receives the consensus message, it quickly broadcasts the message to all RSU nodes within its region. In this way, the information can be rapidly and widely disseminated within the RSU network, ensuring that all relevant nodes can promptly obtain the latest consensus results.

4. Experiments

To evaluate the performance advantages of the proposed consensus algorithm, simulation experiments were conducted in Python, with comparative analysis against traditional PBFT and SG-PBFT (Xu et al., 2022) schemes. The test environment (Intel Core i5-10500@3.10GHz,16GB DDR4, Windows 11) measured three core metrics: consensus delay, throughput, and communication frequency. In the experimental design, RSU nodes were modeled as consensus participants in the blockchain network. By varying the number of nodes, vehicular network scenarios were simulated, with inter-node consensus processes reflecting real-world RSU information exchange. The node counts in the setup were [40, 80, 120, 160, 200]. Experimental results were obtained through multiple trials, with the average value taken.

4.1. Consensus delay

The client sends requests to simulate the RSU nodes sending requests to the main node, with the time taken for the client to receive a reply set as the delay time of the consensus algorithm. Figure 3 demonstrates comparable latency among PBFT, SG-PBFT, and R-PBFT in small-scale networks. As nodes increase, PBFT exhibits significant latency escalation. When exceeding 120 nodes, both R-PBFT and SG-PBFT achieve lower delays than PBFT, with R-PBFT outperforming SG-PBFT beyond 160 nodes. These results confirm R-PBFT's superior latency control in large-scale networks, attributed to its zoned consensus mechanism that partitions the network into localized clusters. By dynamically regulating cluster sizes during network expansion, this approach effectively mitigates the quadratic latency growth inherent in PBFT.

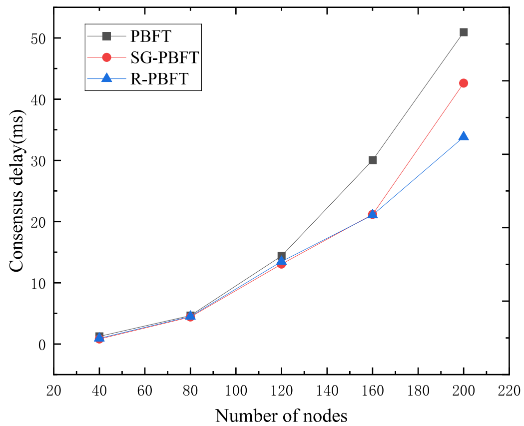

Figure 3: Consensus delay

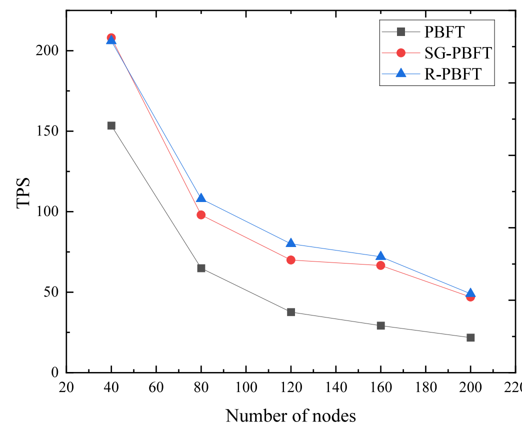

Figure 4: System throughput

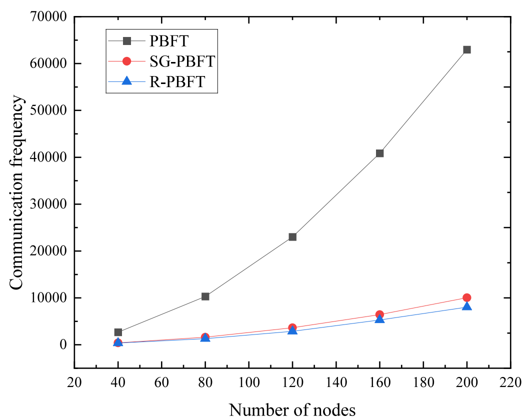

Figure 5: Communication frequency

4.2. System throughput

TPS (Transactions Per Second) refers to the number of transactions that a blockchain system can process within a unit of time. Figure 4 indicates throughput degradation for all three algorithms as nodes increase (due to network congestion from message overload). The proposed R-PBFT achieves significantly higher throughput than PBFT and marginally outperforms SG-PBFT, demonstrating superior transaction processing capacity per unit time that better aligns with vehicular networks' high-throughput requirements.

4.3. Number of communications

The number of communications generated by the network nodes participating in the consensus process during their interactions is referred to as the communication count. Figure 5 reveals quadratic growth in communication complexity for PBFT as nodes scale, contrasting with linear increases in SG-PBFT and the proposed R-PBFT. The R-PBFT algorithm demonstrates superior communication efficiency over SG-PBFT, attributed to its zoned consensus mechanism that dynamically adjusts cluster sizes to constrain communication overhead, making it particularly suitable for resource-constrained vehicular environments.

5. Conclusion and Outlook

This paper addresses the issue of the drastic decrease in consensus efficiency of the traditional PBFT consensus algorithm as the number of nodes increases. It combines the PBFT consensus algorithm with a DAG blockchain structure and designs a consensus algorithm, R-PBFT, which first achieves local consensus within regions and then global consensus. In the local consensus phase, an improved PageRank algorithm is used for the election of master nodes to adapt to the dynamic environmental characteristics of vehicular networks. Simulation experiments show that the proposed algorithm performs excellently in terms of consensus delay, throughput, and communication overhead, making it more suitable for high mobility and high concurrency scenarios in vehicular networks.

References

Ferheen Ayaz, Zhengguo Sheng, Daxin Tian, Guan Yong Liang, and Victor Leung. A voting blockchain based message dissemination in vehicular ad-hoc networks (vanets). In *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, pages 1–6. IEEE, 2020.

George Danezis, Lefteris Kokoris-Kogias, Alberto Sonnino, and Alexander Spiegelman. Narwhal and tusk: a dag-based mempool and efficient bft consensus. In *Proceedings of the Seventeenth European Conference on Computer Systems*, pages 34–50, 2022.

Ziad Hussein, May A Salama, and Sahar A El-Rahman. Evolution of blockchain consensus algorithms: a review on the latest milestones of blockchain consensus algorithms. *Cybersecurity*, 6 (1):30, 2023.

Jiawen Kang, Rong Yu, Xumin Huang, Maoqiang Wu, Sabita Maharjan, Shengli Xie, and Yan Zhang. Blockchain for secure and efficient data sharing in vehicular edge computing and networks. *IEEE internet of things journal*, 6(3):4660–4670, 2018.

Sowmya Kudva, Shahriar Badsha, Shamik Sengupta, Ibrahim Khalil, and Albert Zomaya. Towards secure and practical consensus for blockchain based vanet. *Information Sciences*, 545:170–187, 2021.

Lun Li, Jiqiang Liu, Lichen Cheng, Shuo Qiu, Wei Wang, Xiangliang Zhang, and Zonghua Zhang. Creditcoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 19(7): 2204–2220, 2018.

Yixin Li, Zhen Wang, Jia Fan, Yue Zheng, Yili Luo, Chunhua Deng, and Jianwei Ding. An extensible consensus algorithm based on pbft. In *2019 International conference on cyber-enabled distributed computing and knowledge discovery (CyberC)*, pages 17–23. IEEE, 2019.

Xingchen Liu, Haiping Huang, Fu Xiao, and Ziyang Ma. A blockchain-based trust management with conditional privacy-preserving announcement scheme for vanets. *IEEE Internet of Things Journal*, 7(5):4101–4112, 2019.

Alexander Spiegelman, Neil Giridharan, Alberto Sonnino, and Lefteris Kokoris-Kogias. Bullshark: Dag bft protocols made practical. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, pages 2705–2718, 2022.

Huan Yu Wu, Xin Yang, Chentao Yue, Hye-Young Paik, and Salil S Kanhere. Chain or dag? underlying data structures, architectures, topologies and consensus in distributed ledger technology: A review, taxonomy and research issues. *Journal of Systems Architecture*, 131:102720, 2022.

Guangquan Xu, Hongpeng Bai, Jun Xing, Tao Luo, Neal N Xiong, Xiaochun Cheng, Shaoying Liu, and Xi Zheng. Sg-pbft: A secure and highly efficient distributed blockchain pbft consensus algorithm for intelligent internet of vehicles. *Journal of Parallel and Distributed Computing*, 164:1–11, 2022.

Changlin Yang, Ying Liu, Kwan-Wu Chin, Jiguang Wang, Huawei Huang, and Zibin Zheng. A novel two-layer dag-based reactive protocol for iot data reliability in metaverse. In *2023 IEEE 43rd International Conference on Distributed Computing Systems (ICDCS)*, pages 25–36. IEEE, 2023.

Shijie Zhang, Jiang Xiao, Enping Wu, Feng Cheng, Bo Li, Wei Wang, and Hai Jin. Morphdag: A workload-aware elastic dag-based blockchain. *IEEE Transactions on Knowledge and Data Engineering*, 2024.

Xiaohong Zhang and Xiaofeng Chen. Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network. *Ieee Access*, 7:58241–58254, 2019.