Data Sharing Strategy Based on PBFT Algorithm in VANETs

杜雪 江晓明 吴昊 方婧茹
江苏大学计算机科学与通信工程学院

优胜奖

## 摘要

With the development of Intelligent Transportation Systems (ITS) and 5G communication technology, Vehicular Ad-Hoc Networks (VANETs) are playing an increasingly important role in enhancing road safety, improving traffic efficiency and providing online entertainment experience [1]. However, the information insecurity brought by the traditional centralized mode of VANETs is still a very challenging problem. To solve this problem, a 5G-enabled hierarchical network in VANETs is proposed through the research of blockchain and 5G technology. On this basis, a data sharing scheme based on Practical Byzantine Fault Tolerance (PBFT) algorithm is proposed, which realizes data storage and transmission effectively with its characteristics of data immutability and decentralization. The ideal expected result is that the scheme realizes data storage effectively and the security of data transmission and ensures the reliable transmission of data with lower computing time.

## 提出的方法

This paper designs a hierarchical network supported by 5G network in VANETs. In addition to the characteristics of high data transmission rate and low latency, another key characteristic of 5G is the hierarchical coexistence of heterogeneous networks. Here, the heterogeneity refers not only to cells of various sizes but also to different protocols and standards[1]. So 5G render a promising enabler for VANETs hierarchical network. On this basis, a data sharing scheme based on PBFT algorithm is proposed to effectively realize data storage and disseminate. The bottom layer is the vehicle node layer. In this layer, information exchange service is realized through P2P communication between vehicles, such as vehicle position, speed, direction and brake status beacon data exchange and cooperative awareness. The second layer is the blockchain node layer, where vehicle nodes upload road conditions or accident information to the blockchain nodes. Blockchain nodes store and transmit these important information through PBFT algorithm. The third layer is the cloud layer, which uses a large number of storage resources of cloud computing to calculate vehicle information, road condition information and other data, and predict the better vehicle driving plans for the next phase in advance.

In this paper, the proposed architecture takes the city as a unit and designs VANETs as a consortium blockchain, which includes vehicle nodes and blockchain nodes. When a vehicle node travels to a certain region, it accesses a blockchain node in the region one by one through asymmetric encryption technology[10]. Using asymmetric encryption technology to solve the vehicle security issues between the vehicle nodes and blockchain nodes. When the number of vehicles is too large, the vehicles within the adjacent range and in the same direction are divided into a cluster according to the clustering algorithm[11][12], and one cluster corresponds to a blockchain node.

At the vehicle layer, the vehicle nodes share beacon information through the IEEE 802.11p protocol. When the vehicle collects emergency information closely related to safety, it uploads the emergency information to the connected blockchain node. At the blockchain system layer, blockchain nodes use the PBFT algorithm to combine data blocks in chronological order into chains and use cryptography to ensure that it's difficult to tamper and forge. PBFT algorithm realizes consensus mechanism through message passing. The object of consensus is every transaction and the process of message consensus is parallel. It can be said that there is no block concept in PBFT. On the one hand, in the traditional PBFT algorithm, there is a large number of P2P communication between nodes to reach a consensus, which will occupy a large amount of communication resources. On the other hand, it is almost impossible for a blockchain node in a certain region to become a malicious node after setting up. So we simplify and improve the traditional PBFT algorithm refering to an improved PBFT efficient consensus mechanism based on credit[13]. When the nodes are first set up, a complete consensus process takes place to ensure that all nodes are up and running. When the vehicle updates data, the blockchain node performs a simplified consensus process to achieve information recording and transmission. In the absence of Byzantine faulty nodes, we simplify the complete consensus process, as shown in Fig.3 below. When vehicle nodes transmit the safety information to the blockchain nodes, they send the request massage to Replica0. The primary node Replica0 sends a pre-prepare' message to all the backup nodes to conduct the consensus process. All backup nodes reply a prepare' message if they agree. When Replica0 receives 3f prepare' messages, This safety information is broadcast to other backup nodes to implement the consensus. If the primary node does not receive 3f prepare' information, the complete consensus process is entered.

In the cloud layer, a large number of vehicle information that was obtained from the blockchain nodes will be processing through artificial intelligence technologies such as machine learning, data mining to get the driver and vehicle travel records and preferences. So the traffic distribution intensity or other traffic can be predicted and the different vehicles optimization routes or the optimal solutions can be calculated.

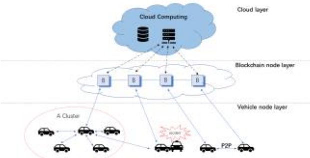


Fig1. Hierarchical network architecture

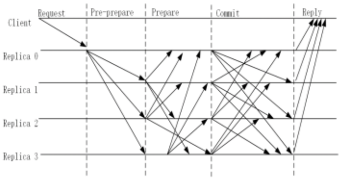


Fig2. Complete PBFT consensus process

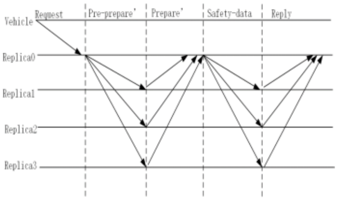


Fig3. Simplified PBFT consensus process

## 性能分析

Different from the traditional VANETs data sharing mechanism, our strategy adopts the distributed blockchain technology based on PBFT algorithm. This strategy does not rely on centralized RSU and reduces the cost of maintaining RSU and data centers. The vehicle nodes package the data into blocks that can be received by other vehicles in the range without passing through the central management node. This also avoids the disadvantage that traditional centralized data storage is vulnerable to centralized malicious attacks. What's more, the PBFT algorithm use cryptographic techniques, such as message authentication coding and digest to ensure that the message delivery process cannot be tampered or destroyed. Therefore, in our proposed strategy, information is not susceptible to tampering and this method of verifying results by consensus algorithm can improve the impact from forged vehicle information and ensure the security of communication.

In the proposed data sharing mechanism, vehicle nodes conduct P2P communication and only blockchain nodes conduct consensus process, so that nodes can achieve consistency faster and with lower delay. Without the Byzantine faulty nodes, our simplified approach does not consume as much computing power as traditional blockchain systems and the throughput of the entire network is greatly improved. We will verify the performance of this strategy through VEINS and MATLAB software platforms in subsequent experiments.

## 结论

Decentralization and data immutability of blockchain technology can be used to improve the security and stability of the communication between vehicles in VANETs. In this paper, a 5G-enabled hierarchical network in VANETs is proposed: the vehicle node layer, the blockchain node layer and the cloud layer. On this basis, a data sharing mechanism based on PBFT algorithm is proposed to realize reliable storage and transmission of data effectively. The simulation results show that the strategy realizes the effective recording and storage of data, ensures the security of data transmission, effectively reduces the communication delay and ensures the reliable transmission of data with low computing time.

## 主要参考文献

[1]Cheng X , Chen C , Zhang W , et al. 5G-Enabled Cooperative Intelligent Vehicular (5GenCIV) Framework: When Benz Meets Marconi[J]. Intelligent Systems, IEEE, 2017, 32(3):53-59.

[2]Bayad K . An Overview of VANET: Architectures, Challenges and Routing Protocols[C]// Netys. 2015.

[3]Baohong H , Yihui Z , Sude Q . Overview of Blockchain Technology[J]. Computer Engineering, 2019.

[4]Shen X , Fantacci R , Chen S . Internet of Vehicles [Scanning the Issue][J]. Proceedings of the IEEE, 2020, 108(2):242-245.

[5]Castro M , Liskov B . Practical Byzantine Fault Tolerance and Proactive Recovery[J]. ACM Transactions on Computer Systems, 2002.

## 联系方式

联系人：杜雪
手机：18221216482
邮箱：2582748126@qq.com