Group-based PBFT Consensus Algorithm Considering Node Location and Latency

Jinsung Cho
Department of Electrical, Electronics, information and Computer Engineering
Chungbuk National University
Chungju, Korea
cjs97111@chungbuk.ac.kr

Gwangyong Kim
Department of Electrical, Electronics, information and Computer Engineering
Chungbuk National University
Chungju, Korea
brightdragom@chungbuk.ac.kr

Geunmo Kim
Department of Electrical, Electronics, information and Computer Engineering
Chungbuk National University
Chungju, Korea
rootmo96@chungbuk.ac.kr

Bongjae Kim*
Department of Computer Engineering
Chungbuk National University
Chungju, Korea
bjkim@chungbuk.ac.kr

Min Choi
Department of Information and Communication
Chungbuk National University
Chungju, Korea
mchoi@chungbuk.ac.kr

ABSTRACT

In the blockchain, a consensus algorithm can be used to record and manage the distributed ledger identically. The consensus algorithm is one factor that significantly influences the performance of the blockchain network. PBFT, a voting-based consensus algorithm, has improved safety but has a problem in that liveness is relatively low. In this paper, we propose a group-based PBFT algorithm that considers location-based clustering and inter-node latency to enhance the performance of PBFT in terms of the time required for consensus. Through the analysis of the experimental results, it was confirmed that the proposed group-based PBFT algorithm has an advantage in terms of performance over the random group-based PBFT algorithm.

KEYWORDS

Blockchain, Consensus Algorithm, PBFT

1 INTRODUCTION

Blockchain is a distributed ledger technology that operates on a peer-to-peer network. The blockchain is almost impossible to delete or modify maliciously. Also, decentralization is possible by applying blockchain. Recently, hybrid blockchains that properly combine decentralized and centralized structures and methods are also used for efficient service expansion [1].

A blockchain appropriately chooses and uses a consensus algorithm suitable to the characteristics of the blockchain for the unified decision-making of nodes participating in the blockchain network. Blockchain can be typically divided into the following three types. There are public blockchains, private blockchains, and consortium blockchains. In the case of private and consortium blockchains suitable for industry and business, the PBFT-based consensus algorithm is mainly used [2]. In the case of private and consortium blockchain, only nodes approved in advance can participate in consensus and its blockchain network.

Consortium blockchains are currently used in various industry and business fields. Representative application fields where consortium blockchain is applied include healthcare, trade, and smart factories [3][4]. These application fields generally require high-performance processing speed and high reliability. The consensus algorithm is one of the important factors that determine the performance and reliability of a blockchain. For this reason, to improve performance and reliability, various studies are being conducted to improve the reliability of the PBFT-based consensus algorithm for the consortium blockchain and the time required for consensus [5][6].

This paper proposes a group-based PBFT algorithm that dynamically manages groups of its blockchain network by reflecting the node location and the latency between nodes during the consensus process. The proposed algorithm first do clustering nodes participating in consensus based on their location. Afterward, the nodes in the same cluster are randomly grouped in units of 4. Each node of the blockchain network records the latency with the node communicated in the consensus processes. And each node sends its collected latency information to the agent node at regular intervals. The agent has the role of managing the groups in our group-based PBFT algorithm. Agent dynamically changes and readjusts the configuration of each group by using the collected latency information between each node. A blockchain network environment consisting of 160 nodes was set up and simulated to evaluate the performance of the proposed algorithm. According to the experimental results, it was confirmed that it reduces the consensus time compared to the random group-based PBFT algorithm.

The rest of this paper is organized as follows. Chapter 2 describes the proposed group-based PBFT algorithm while considering node

* Corresponding Author

location and latency and Chapter 3 describes experimental results. Chapter 4 concludes this paper with future works.

2 PROPOSED ALGORITHM

Several studies effectively reduced the communication complexity of PBFT and improved liveness. However, it does not consider the network latency, which is an important factor in the performance of PBFT in terms of consensus time. It can be seen that there is a problem that several studies proposed so far do not always guarantee optimal performance. This paper proposes a group-based PBFT algorithm considering location information and network latency. The proposed algorithm clusters nearby nodes through location information. After that, by configuring groups by reflecting the latency between nodes in the same cluster, it is possible to reduce the total number of communication and the time required for consensus.

2.1 Blockchain Network Structure of the Proposed Algorithm

Figure 1 shows an example of the network structure of the proposed algorithm. The roles of nodes of the blockchain network are divided into three main categories: Agent Node, Group-Primary Node, and Normal Node. Agent Node (AN) manages the blockchain network and collects the latency information between nodes of the blockchain network. It also manages and configures groups. In the consensus process, the consensus results of each group are collected to the agent node, and a final consensus result is made. The agent node is a secure node authenticated by a group or institution. There can be existed multiple Agent Nodes to prevent system down in the blockchain network. Group-Primary Node (GPN) acts as the leader of each group. It sends the consensus result of its group to the agent node. Normal Nodes (NN) act as general nodes participating in consensus in each group.

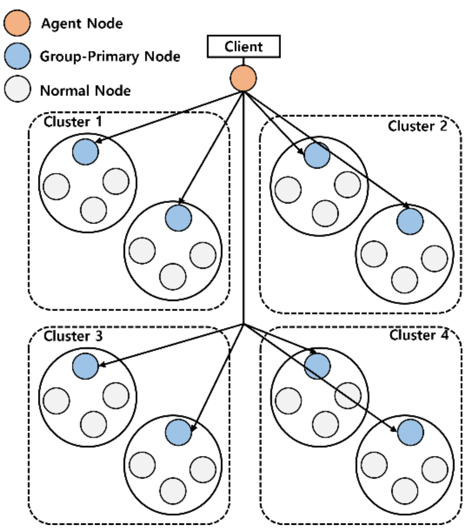

Figure 1: An example of the network structure of the proposed algorithm

2.2 Operation Sequences of the Proposed Algorithm

The proposed algorithm clusters all nodes of the blockchain networks based on their location information at first. Then, each cluster consists of multiple groups by the proposed algorithm. The organization of each group is dynamically changed by the latency information by the proposed algorithm. Figure 1 shows an example of the blockchain network structure when the total number of nodes is 33 including the agent node, and the cluster is 4. The process of the proposed algorithm in this paper is as follows.

(Step 1) All nodes can provide location information when participating in the blockchain network. We assume that the proposed algorithm is for the consortium blockchain, and location information can be provided without difficulty. The agent node clusters the nodes into two or more clusters using the nodes' location information, as shown in Figure 1.

(Step 2) Nodes in the same cluster are grouped with a unit of four nodes, the minimum number of nodes to satisfy 3F+1, the characteristic of PBFT. Here, F means the number of malicious nodes, and 3F+1 is a structural unit of nodes that can guarantee reliability because there are F malicious nodes. At this time, the nodes of each group are decided by its agent node. However, if the latency information between nodes is not collected until the group designation stage, the group and the group-primary node are randomly assigned.

(Step 3) After the groups and their group-primary node of the blockchain are designated, the agent node sends a consensus message to all group-primary nodes of each group. Then each group-primary node performs the PBFT consensus algorithm within its group. When the consensus is completed, the group-primary node sends the group consensus result to the agent node.

(Step 4) At each group change cycle, each node transmits the recorded latency information to the agent node. The agent node repeats Steps 2 to 3 until all latency information is collected. If all the latency information of all nodes is collected, Step 5 is performed.

(Step 5) When all information about the latency between nodes is collected, the group is redesignated by reflecting the relevant details in the group designation. In group redesignation, the group-primary node is randomly assigned first, and the nodes with the shortest latency are given to the group based on each group-primary node.

(Step 6) The consensus process is continued by randomly replacing the node that will serve as the group-primary node in each cluster at regular intervals.

3 PERFORMANCE EVALUATIONS

Two assumptions were made for the experiment of the proposed algorithm. First, it is assumed that no malicious nodes interfere with the blockchain network's consensus. Safety and robustness issues are not the scope of the proposed algorithm. Second, it is assumed that all nodes have a shorter latency with nodes in the same cluster than those of other clusters. For the experiment, 160 nodes were run on a single computing node. The detailed specifications of the computing node used in the experiment are shown in Table 1.

Table 1: Specifications of the computing node used in the experiment

Features	Descriptions
CPU	AMD ryzen threadripper 3960X
Memory	DDR4 16G PC4-25600(4ea)
OS	Ubuntu 18.04 LTS

A blockchain network consisting of 160 nodes was constructed to evaluate the performance of the proposed algorithm. All 160 nodes are divided into 4 clusters, each consisting of 40 nodes. Therefore, there are 10 groups in each cluster. The latency with nodes in the same cluster was set at 5 ms to 10 ms, and the latency with nodes in other clusters was set from 5 ms to 30 ms. The total number of consensuses was set to 130, and it was assumed that the agent node changed the group per 10 times consensus was completed. The performance of the proposed algorithm was measured and analyzed by using an application written in the Python programming language. We compared the performance of our proposed algorithm to a random group-based PBFT algorithm.

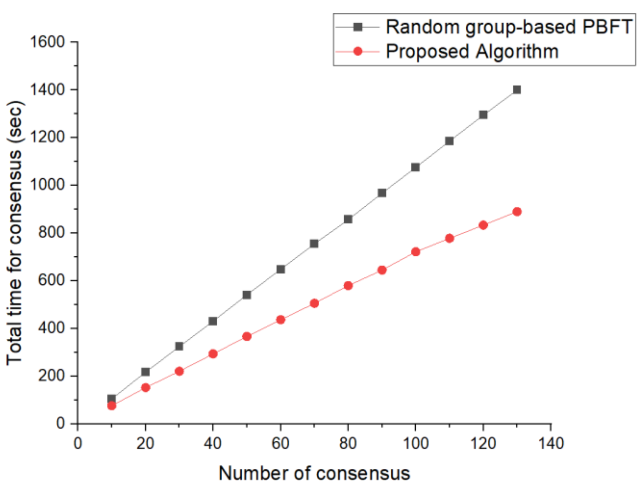

Figure 2: Comparison results of time required for consensus between random group-based PBFT and the proposed algorithm

Figure 2 shows the accumulated consensus time required for the consensus of each algorithm. As shown in Figure 2, in the case of random group-based PBFT, the cumulative consensus time increased more steeply than in the proposed algorithm. In addition, when the 130 consensuses were completed, the proposed algorithm reduced the overall time required by about 63.5% compared to the random group-based PBFT. It can be confirmed that it has a high-performance improvement in consensus time even though the proposed algorithm has the same number of communications as the random group-based PBFT.

In addition, in the case of the proposed algorithm, it can be seen that the slope of the graph is slightly relaxed after the 100th consensus. This is because the agent node completes the collection of latency information among all blockchain network nodes after the change of group occurs 10 times. Therefore, the agent node can do regrouping more efficiently for all blockchain network nodes. Consequently, it can be seen that the proposed algorithm needs additional overhead in the clustering and inter-node latency collection steps but effectively reduces the time required for consensus in the long-term aspects.

4 CONCLUSION AND FUTURE WORKS

This paper proposed a group-based PBFT algorithm considering location information and inter-node network latency. As a result of the performance measurement, it was confirmed that the proposed algorithm showed better performance in all cases when compared to the random group-based PBFT. In future research, we will discuss in detail various problems that may occur, such as when the latency with other cluster nodes is shorter, and propose some solutions.

ACKNOWLEDGMENTS

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. NRF-2017R1E1A1A01075128).

REFERENCES

[1] Androulaki, Elli, et al., "Hyperledger fabric: a distributed operating system for permissioned blockchains", Proceedings of the thirteenth EuroSys conference, 2018.
[2] Castro, Miguel, and Barbara Liskov, "Practical byzantine fault tolerance", OsDI. Vol. 99, No. 1999, 1999.
[3] Agbo, Cornelius C., Qusay H. Mahmoud, and J. Mikael Eklund, "Blockchain technology in healthcare: a systematic review", Healthcare, MDPI, Vol. 7, No. 2, 2019.
[4] Wan, Jiafu, et al., "A blockchain-based solution for enhancing security and privacy in smart factory", IEEE Transactions on Industrial Informatics, Vol. 15, No. 6, pp. 3652-3660, 2019.
[5] Feng, Libo, et al., "Scalable dynamic multi-agent practical byzantine fault-tolerant consensus in permissioned blockchain", Applied Sciences, Vol. 8, No. 10, 2018.
[6] Gao, Sheng, et al., "T-PBFT: An EigenTrust-based practical Byzantine fault tolerance consensus algorithm", China Communications, Vol. 16, No. 12, pp. 111-123, 2019.