HiLL PUBLISHING

Advances in Computer and Communication, 2024, 5(4), 205-209
https://www.hillpublisher.com/journals/acc/
ISSN Online: 2767-2875

Node Selection Methods Among Distributed Devices for Wireless Consensus

Sungho Lee*, Inoh Chu, Jaeuk Kwon

ICT Convergence Research Division/Future Mobile Communication Research Center, Gumi Electronics and Information Technology Research Institute (GERI), Gumi 39171, South Korea.

How to cite this paper: Sungho Lee, Inoh Chu, Jaeuk Kwon. (2024) Node Selection Methods Among Distributed Devices for Wireless Consensus. *Advances in Computer and Communication*, 5(4), 205-209.
DOI: 10.26855/acc.2024.10.001

Received: July 25, 2024
Accepted: August 22, 2024
Published: September 18, 2024

***Corresponding author:** Sungho Lee, ICT Convergence Research Division/Future Mobile Communication Research Center, Gumi Electronics and Information Technology Research Institute (GERI), Gumi 39171, South Korea.

Abstract

As numerous services and applications are developed within wireless networks, a significant number of wireless devices in future 6G networks are expected to communicate and exchange data with one another to collaboratively make reliable decisions based on the data collected in distributed environments. To address security issues in these environments, blockchain technology has been introduced to ensure data integrity and consistency. Furthermore, to overcome the low performance and scalability challenges associated with blockchain, research has actively focused on wireless consensus and node selection to facilitate fast and reliable decision-making among wireless devices. However, the methods for designating participating nodes in wireless consensus have not been thoroughly analyzed, resulting in performance degradation during the consensus process. Therefore, in this paper, we analyze the consensus failure probability (CFP) and the total communication trials (TCT) for varying numbers of selected nodes using different node selection methods in wireless consensus, specifically reliability-based node selection and average successful transmission probability (STP)-based node selection. We then explore strategies to reduce both the CFP and TCT in wireless consensus.

Keywords

6G; Wireless Consensus; Node Selection

1. Introduction

In future 6G networks, the massive and full connectivity among intelligent devices is expected to be one of the prominent features. For example, numerous interconnected sensors can be deployed for fast decision making such as in e-healthcare, smart grid, and surveillance networks. In addition, autonomous systems can also make more accurate decisions based on their connectivity, enabled by 6G technologies [1]. However, the security concerns in 6G networks have also been raised as more devices are expected to be connected to make cooperative decisions in distributed environments [2].

The blockchain has attracted attention as a unique solution to address those security issues as various types of data are securely managed including military data, network functions, intelligent transportation systems (ITS), and artificial intelligence (AI)- driven applications [3, 4]. The blockchain is a distributed ledger, shared among participants, to ensure the data immutability and the data integrity in a distributed environment. The ledger can be updated only when participants reach agreement on data after performing a pre-defined consensus protocol, such as proof-of-work (PoW), practical Byzantine fault tolerance (PBFT), and Raft. For example, in [3], participating organizations use the blockchain to make reliable decisions based on military surveillance data, delivered by unmanned aerial vehicles (UAVs). In [4], the blockchain-enabled crowdsourced indoor navigation system using 6G communications is proposed to process user requests for path detection using the smart contract in the blockchain.

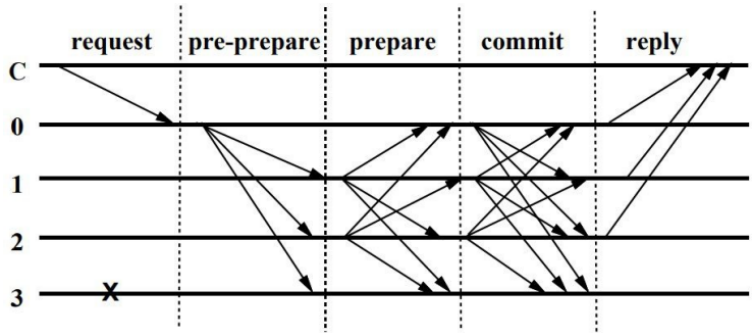


Figure 1. The operations of PBFT [9].

However, blockchain-enabled systems inevitably experience low performance and low scalability [5]. To overcome the low performance of the blockchain, in some recent works, wireless consensus protocols have been considered in [6, 7] by eliminating costly ledger management. Specifically, being different from the conventional consensus protocols in wired scenarios, the wireless consensus protocols are quickly conducted by distributed devices over wireless channels, especially on ephemeral and short-lived data. By doing so, even though the data immutability cannot be guaranteed, reliable decision-making can be quickly obtained for appropriate actions. For example, in [6], a novel wireless consensus protocol, termed random representative consensus (R2C), is proposed to make valid control actions in a proper order among distributed sensors and actuators in cyber-physical systems (CPS). In [7], Raft is designed through vehicle-to-vehicle (V2V) communications for lane-changing decisions among neighboring autonomous vehicles to prevent collisions and then analyzed using Markov probabilistic models in terms of consensus reliability.

Similarly, to overcome the low scalability of the blockchain, consensus node selection methods have been considered in [6, 8]. Specifically, being different from the conventional consensus protocols among all participating nodes, a subset of nodes is selected to conduct the consensus protocol. The consensus results are then notified to all the other non-selected nodes for validation, so the burden of involving a large number of nodes in the consensus process can be avoided. For example, in [8], part of nodes is selected based on their credit scores, and then performs credit-based PoW for system security and transaction efficiency in industrial Internet of Things (IIoT) networks. In [6], some nodes are randomly selected as representative nodes, i.e., validators, and others act as acceptors, where the validators generate actions after the consensus protocol, and the acceptors can decide whether to accept or reject the actions.

However, even though wireless consensus and node selection have been recognized to mitigate the drawbacks of the blockchain for 6G networks, where devices are massively and fully connected, the strategies to integrate both of the concepts have not yet been analyzed. In this paper, therefore, we propose and analyze two node selection methods in wireless consensus protocols, i.e., average successful transmission probability (STP)-based node selection and reliability-based node selection. We then show our experiment results for the consensus failure probability (CFP) and the total communication trials (TCT) with different numbers of selected nodes using wireless PBFT. Finally, we discuss some methods to simultaneously achieve lower CFP and TCT.

2. Performance Metrics and Node Selection Methods

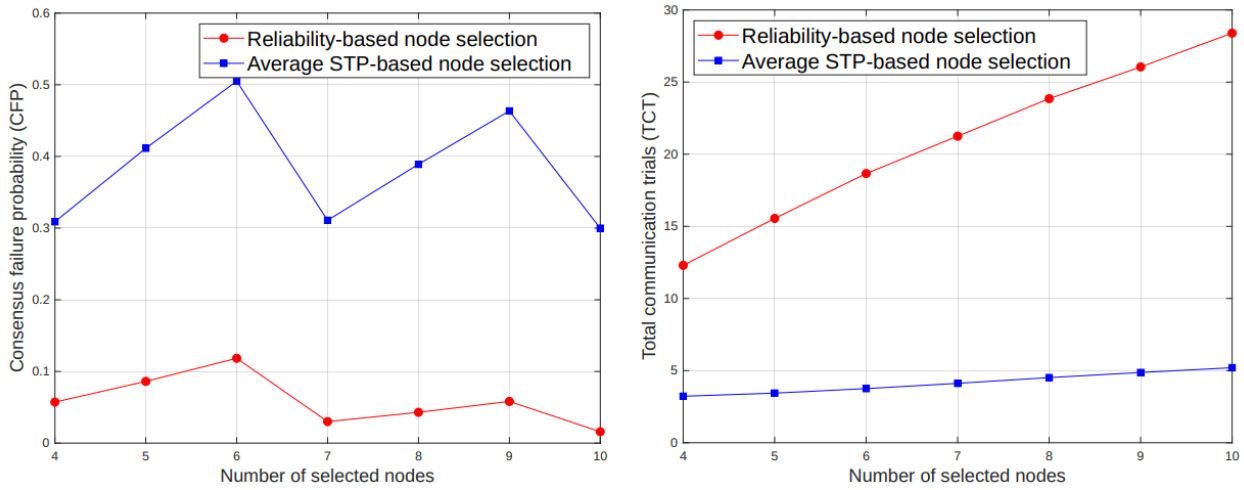
In this section, we give brief explanations of PBFT, which can be practically considered to be implemented on wireless networks. Note that PoW is the most popular consensus protocol, but it is not suitable for being performed over wireless channels. We then explain the main performance metrics of this paper, which are CFP and the TCT. Lastly, we introduce two corresponding node selection methods: the average STP-based node selection and the reliability-based node selection.

2.1 Practical Byzantine Fault Tolerance (PBFT)

The PBFT protocol was designed to provide a new solution to tolerate Byzantine faults in a distributed environment [9]. As shown in Fig. 1, for f Byzantine, i.e., malicious nodes, the PBFT protocol can ensure a reliable decision when the total number of participating nodes is $\boldsymbol{N = 3f + 1}$. Therefore, when $\boldsymbol{N}$ nodes are deployed, the nodes can

tolerate up to $\left\lfloor \frac{N-1}{3} \right\rfloor$ Byzantine nodes. The PBFT protocol consists of three phases: pre-prepare, prepare, and commit phases.

In the pre-prepare phase, the leader node broadcasts a pre-prepare message to all replicas. In the preparation phase, each replica validates the pre-prepare message. If the pre-prepare message is validated, the replica sends a prepare message to the other nodes. After receiving $\boldsymbol{2f}$ prepare messages from the other nodes, the replica can move to the commit phase. In the commit phase, the replica broadcasts a commit message, and then the consensus is completed if 2f commit messages are delivered from the other nodes. More detailed information on the PBFT protocol can be found in [9].



(a) CFP **(b) TCT**

Figure 2. CFP and TCT as functions of selected nodes for different node selection methods.

2.2 Performance Metrics

1) Consensus Failure Probability: The CFP is defined as the probability that the selected nodes cannot reach reliable consensus as the number of faulty responses in any phase exceeds $\left\lfloor \frac{N-1}{3} \right\rfloor$, which is the security threshold of PBFT. The number of shared faulty responses depends on the node reliability. Thus, the CFP is lower as the reliabilities of selected nodes are higher, and vice versa.
2) Total Communication Trials: The TCT is defined as the total number of transmissions made by selected nodes to reach consensus. Note that we consider that selected nodes can infinitely retransmit their responses [6]. The total number of transmissions to reach consensus depends on the communication performance of selected nodes. Thus, the TCT is lower as the communication performance of selected nodes is higher, and vice versa.

2.3 Node Selection Methods

1) Reliability-based Node Selection: The reliability-based node selection is a conventional node selection method, which can be readily discovered in literature [8]. In the reliability-based node selection, N nodes with the highest reliability value, quantified as credit, score, and reputation, are consecutively selected to participate in the consensus. Here, the reliability value of the i-th node is evaluated as the complement of its faulty probability.
2) Average Successful Transmission Probability (STP)-based Node Selection: The average STP-based node selection is a newly considered node selection method, which can be used to aim at finishing the consensus over wireless channels, regardless of the consensus results. In the average STP-based node selection, N nodes with the highest average STP are consecutively selected to participate in the consensus. Here, the average STP of the i-th node is defined as the average probability that the i-th node successfully transmits data to all the other nodes.

3. Experiment Results and Discussion

In this section, we show our experiment results for the CFP and the TCT with different numbers of selected nodes, obtained from MATLAB. For our experiments, we consider wireless nodes, which are distributed according to a

Poisson point process (PPP) with density $\boldsymbol{\lambda = 4 \times 10^{-2}}$ [nodes/$\mathbf{m^2}$]. Similar to [10], each of the nodes may generate faulty response at each PBFT phase based on its own faulty probability, which is randomly decided from a faulty probability set $\boldsymbol{F = \{0.1, 0.2, 0.3, 0.4, 0.5\}}$. We also consider that the noise power is $\boldsymbol{N_0 = -10}$ [dB] [11]. In addition, the channel fading gain is considered as Rayleigh fading, whose average is $\mathbf{1}$.

3.1 Experiment Results

Figure 2 shows the CFP and the TCT as functions of the number of selected nodes. From Fig. 2(a), we can see that the CFP repeatedly increases and decreases as N increases since the security threshold of the PBFT is $\left\lfloor \frac{N-1}{3} \right\rfloor$. In other words, increasing N eventually decreases the CFP if the result of $\frac{N-1}{3}$ does not output an integer value, such as $N = 5, 6, 8,$ and $9, \cdots$. In addition, we can also see that the trend of the CFP finally decreases as N increases since the security level also increases with N. From Fig. 2(b), we can also see that the TCT continuously increases as N increases since more communication trials are required to reach a consensus.

From Fig. 2(a), we can also see that the reliability-based node selection can lower the CFP, on the other hand, from Fig. 2(b), the average STP-based node selection can lower TCT. This is because the CFP is affected by the faulty probabilities of selected nodes, and the TCT is affected by the communication performance of selected nodes, as explained earlier. Therefore, there can be pros and cons to the two node selection methods.

3.2 Discussion to Decrease CFP and TCT

In this subsection, we explore possible methods to decrease the CFP and the TCT based on our experiment results.

1) Reliability and Communication Co-designed Node Selection: As discussed earlier, there can be pros and cons in the two-node selection methods above. In this sense, we can expect that it is necessary to jointly consider the reliability and communication performance of nodes, tailored for wireless consensus. For example, the node reliability and the STP can be integrated as an evaluation value to decide participating nodes in consensus such as $v_i^{\mathrm{ev}} = \alpha p_i^{\mathrm{rel}} + \beta p_i^{\mathrm{stp}}$, where v_i^{ev}, p_i^{rel}, and p_i^{stp} are the evaluation value, the reliable probability, and the STP of i-th node, respectively. In this evaluation method, α and β are the weights for the node reliability and the communication performance, respectively, which can be properly adjusted to achieve the lowest CFP and TCT.
2) Communication Resource Management for Wireless Consensus: The communication resources can also be a problem, which significantly affects the communication performance in wireless consensus. For example, in [12], the impacts of the communication resources, such as bandwidth, transmit power, and receiver sensitivity, on the wireless Raft are explored to show how the communication performance can affect the security level in wireless consensus. Therefore, some novel resource allocation methods, tailored for wireless consensus, can also be proposed to decrease the CFP and TCT.
3) Node Distribution Methods for Wireless Consensus: Due to the path loss, the average STP can be measured high at some specific nodes, densely crowded in a narrow area. If they are faulty nodes, the node denseness may enable the faulty nodes to collude with each other in making unreliable results as they are frequently selected as participating nodes. Therefore, some node deployment methods, tailored for wireless consensus, can also be considered to avoid frequent consensus node failure by malicious nodes.

4. Conclusions

In this paper, we propose the reliability-based node selection and the average STP-based node selection for wireless PBFT in 6G networks, where wireless devices are massively distributed to make reliable decisions. We then show our experiment results for the CFP and the TCT as functions of a number of selected nodes for consensus using different node selection methods. Finally, we explore future methods to decrease the CFP and the TCT. From our experiments, being different from the conventional scenarios in wired environments, we can see that the communication performance can newly affect the security level in wireless consensus. In addition, we also conclude that reliability and communication performance can be jointly considered for the co-design of wireless consensus. Moreover, communication resources and node distribution can be adjusted to obtain the advantages of the two node selection methods.

Acknowledgment

This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (No. RS-2023-00273011).

References

[1] M. Giordani, M. Polese, M. Mezzavilla, S. Rangan, and M. Zorzi. "Toward 6G networks: Use cases and technologies," *IEEE Commun. Mag.*, vol. 58, no. 3, pp. 55-61, Mar. 2020.

[2] T. Hewa, et al. "The role of blockchain in 6G: Challenges, opportunities and research directions," in *Proc. 6G Wirel. Summit (6G SUMMIT)*, Levi, Finland, Mar. 2020, pp. 1-5.

[3] D. Saraswat, et al. "Secure 5G-assisted UAV access scheme in IoBT for region demarcation and surveillance operations," *IEEE Commun. Stand. Mag.*, vol. 6, no. 1, pp. 58-66, Mar. 2022.

[4] W. Li, Z. Su, R. Li, K. Zhang, and Y. Wang. "Blockchain-based data security for artificial intelligence applications in 6G networks," *IEEE Netw.*, vol. 34, no. 6, pp. 31-37, Nov./Dec. 2020.

[5] S. Lee, et al. "Facing to latency of Hyperledger Fabric for blockchain-enabled IoT: Modeling and analysis," *IEEE Netw.*, vol. 37, no. 6, pp. 232-239, Nov. 2023.

[6] H. Seo, J. Park, M. Bennis, and W. Choi. "Communication and consensus co-design for distributed, low-latency, and reliable wireless systems," *IEEE Internet Things J.*, vol. 8, no. 1, pp. 129-143, Jan. 2021.

[7] Y. Li, Y. Fan, L. Zhang, and J. Crowcroft. "RAFT consensus reliability in wireless networks: Probabilistic analysis," *IEEE Internet Things J.*, vol. 10, no. 14, pp. 12839-12853, Jul. 2023.

[8] J. Huang, et al. "Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism," *IEEE Trans. Industr. Inform.*, vol. 15, no. 6, pp. 3680-3689, Jun. 2019.

[9] M. Castro and B. Liskov. "Practical Byzantine fault tolerance," in *Proc. Symp. Oper. Syst. Des. Implement. (OSDI)*, New Orleans, LA, USA, Feb. 1999, pp. 1-14.

[10] K. P. Sharma and T. P. Sharma. "rDFD: Reactive distributed fault detection in wireless sensor networks." *Wirel. Netw.*, vol. 23, pp. 1145-1160, May 2017.

[11] C. K. Sheemar, L. Badia, and S. Tomasin. "Game-theoretic mode scheduling for dynamic TDD in 5G systems." *IEEE Commun. Lett.*, vol. 25, no. 7, pp. 2425-2429, Jul. 2021.

[12] L. Zhang, H. Xu, O. Onireti, M. A. Imran, and B. Cao. "How much communication resource is needed to run a wireless blockchain network?" *IEEE Netw.*, vol. 36, no. 1, pp. 128-135, Jan./Feb. 2022.