Security Analysis of a Fork-Delay-Based Coalition Policy Algorithm for Improving Proof-of-Stake Consensus in Delay-Tolerant IoET Networks

Woo Yong Lee
Mobile Communication Research Division
Electronics and Telecommunications Research Institute (ETRI)
Daejeon, Republic of Korea
wylee@etri.re.kr

Keunyoung Kim
Mobile Communication Research Division
Electronics and Telecommunications Research Institute (ETRI)
Daejeon, Republic of Korea
kykim12@etri.re.kr

***Abstract*— Exploration equipment for extreme environments like the Antarctic region constraints in power consumption, size, and weight. Furthermore, unmanned mobile exploration in environments with distributed IoET (Internet of Extreme Things) nodes requires long-range, delay-tolerant wireless communication. For these extreme environments, delay-tolerant communication systems can consider distributed ledgers as a way to record gains and losses to ensure coalition and reliability among nodes. However, Proof-of-Work (PoW), the most widely studied method for securing distributed ledger reliability, is simple to operate but highly energy-consumption. Proof-of-Stake (PoS) offers an energy-efficient alternative. This paper assumes a partially Δ-synchronized distributed system model for security analysis in PoS and analyzes the impact of network delays on the system. This analysis is an interpretation to identify methods for securing stability against balance attacks in public systems from the perspective of a partially Δ-synchronized model. The proposed technique is a game-theoretic approach that uses honest nodes to form a coalition to control delay. This study investigates the possibility of expanding the upper bound of the security region according to the attacker's occupation rate in a balanced attack by controlling the time delay required for nodes in a partially Δ-synchronized communication network to transmit messages to each other.**

Keywords—— Consensus Algorithm, Proof-of-Stake, Fork-Delay, Security Region, Internet of Extreme Things

I. INTRODUCTION

Equipment used for exploration in extreme cold regions is subject to limitations in power consumption, size, and weight. However, operating the system in this environment where multiple IoET nodes are distributed requires long-range, delay-tolerant, and high-speed communication [1]. Given a network with limited communication capacity and computational resources, is the blockchain Nakamoto consensus security against attackers' attacks at a given block generation rate? Analysis of the Nakamoto consensus algorithm to date has not answered this question [2]. This is because, in a bounded-delay model, the block processing speed limits of nodes that cause congestion when blocks are generated in rapid succession are not known in a timely manner. In this paper, we will examine the potential trade-off between security and performance for the proof-of-stake Nakamoto consensus in a bounded-capacity model.

Meanwhile, game theory [3] can be applied as an alternative solution for distributed ledger communication networks. Game theory is a mathematical model of strategic interactions between rational decision makers [4]. Therefore, game theory can be used to analyze the strategies of cooperative and consensus nodes and the interactions between them. Through game theory analysis, nodes can learn and predict each other's mining behavior and select optimal response strategies based on Nash equilibrium analysis. These optimal response strategies can be used as a mechanism to prevent node malfunctions or attacks. Therefore, game theory can be a natural consideration for modeling the decision-making processes of all consensus nodes in a distributed ledger communication network.

In this paper, we analyze the performance improvements of consensus algorithms in a partially Δ-synchronized model [5] for a delay-tolerant payment channel, applying game theory and fork delay techniques to an public blockchain system. We also analyze the impact of network delays when using a delay control method where nodes cooperate to defend against attackers, and propose a new security region.

II. ANALYSIS OF THE SECURITY UPPER BOUND OF A FORK-DELAY-BASED COALITION POLICY CONSENSUS ALGORITHM AGAINST BALANCED ATTACKS

This analysis seeks to interpret the impact of a coalition policy between nodes on the Proof-of-Stake consensus mechanism under conditions of network delay and balanced attacks. This analysis examines the extent to which balanced attacks impact the PoS consensus scheme from the perspective of a partial Δ-synchronous model. It analyzes the upper bound on the security of the blockchain consensus mechanism when honest nodes form a cooperative and use a strategy to fork-delay or expedite messages based on the preferences of neighboring nodes.

Assuming this balanced (or stakeless) attack model to be a machine performing branching random walks, the total number of attacker blocks on a chain branch increases exponentially with time slot t [7]. Specifically, if the attacker growth rate is λ_a, the branching random walk model amplifies the attacker growth rate by $e\lambda_a$. From the perspective of the partial Δ-synchronous model, the upper bound on the attacker growth rate can be expressed [6]. Assuming that honest nodes cooperate with each other to increase their influence and use a transmission policy that delays messages by increasing or decreasing the delay Δ_f for nodes depending on their preference, the growth rate can be defined as follows.

$$e\lambda_a < \frac{\lambda_{hf} + \lambda_{h-f}}{1 + (\Delta - \Delta_f)\lambda_{hf} - (\Delta + \Delta_f)\lambda_{h-f}}$$

Here, λ_{hf} is the growth rate of the node that reduces the delay, and $\lambda_{h\text{-}f}$ is the growth rate of the node that increases the delay. At this time, we assume $\lambda_h = \lambda_h + \lambda_{h\text{-}f}$. If the delay of each node can be managed for an arbitrary control variable $1>\gamma\geq 1/2$, it can be simply expressed as the following inequality.

$$e\lambda_a < \frac{\lambda_h}{1+\{\Delta-\Delta_f(2\gamma-1)\}\lambda_h}$$

In an average partial Δ-synchronous network environment, let $\hat{\Delta}=\Delta-\Delta_f(2\gamma-1)$, the expected value of the attacker node's participation is assumed to be β_b. In addition, if the total mining speed is λ, the upper bound of $e\beta_b$ for the number of blocks mined per network delay $\Delta\lambda$ is derived as follows:

$$e\beta_b < \frac{1-\beta_b}{1+(1-\beta_b)\hat{\Delta}\lambda}$$

The inequality for the second-order equation of β_b for the above inequality can be simplified into the following equation.

$$e\hat{\Delta}\lambda\beta_b^2-(1+e+e\hat{\Delta}\lambda)\beta_b+1>0$$

At this time, if β_b is represented as a graph against $\frac{1}{\hat{\Delta}\lambda}$, it is the same as the purple solid line in Figure 1. This solid line graph is the same as the true security threshold for the POSpace model in reference [7]. Meanwhile, since the attacker's block generation speed is doubled by the influence of the balanced attack and must satisfy $e\hat{\Delta}\lambda_a = e\hat{\Delta}\lambda\beta_b < \frac{1}{2}$, the upper bound of β_b is the minimum of the two boundaries, as shown in the following equation.

$$\beta_b < \min_{\frac{1}{\hat{\Delta}\lambda}>0}\left(\frac{1}{2e\hat{\Delta}\lambda},\ \frac{1}{2}+\frac{e+1}{2e\hat{\Delta}\lambda}-\sqrt{\left(\frac{1}{2}\right)^2+\frac{e-1}{2e\hat{\Delta}\lambda}+\left(\frac{e+1}{2e\hat{\Delta}\lambda}\right)^2}\right)$$

At this time, the intersection point of the two upper bounds is $\frac{1}{\hat{\Delta}\lambda}=\frac{2e}{2e+1}$ from the above equation, and $\beta_b=1/(2e+1)$. Meanwhile, a method can be considered in a blockchain protocol that prevents blocks from branching for a certain amount of delay time d. Since the labeling of the vertices v of the branching stochastic walk tree begins after d, the log Laplace transform of the average waiting time W_v can be expressed as follows [8]. According to reference [7, Theorem 1.3], the minimum value of the average waiting time, W^*_k is the limit value of the log Laplace transform of the average waiting time, and the following equation represents the stable state.

$$\lim_{k\to\infty}\frac{W_k^*}{k}=\sup_{s>0}\frac{\log\left\{\left(\frac{s}{\lambda_a}+1\right)^d-1\right\}}{s}\cong\frac{d\log(e+1)}{e\lambda_a}$$

In a proof-of-stake blockchain protocol, if the block branch is delayed by a certain period time d, the minimum average waiting time becomes $1/\lambda_a$, so the attacker's growth rate slows down to λ_a. In a proof-of-stake blockchain protocol, as Nakamoto claimed, it is possible to find a certain delay period d that allows an attacker to safely maintain the longest chain protocol with less than 50% of the total hash power.

III. Analysis Results and Conclusions

This analysis provides an upper bound on the safe region for the adversary ratio when an attacker attempts a balanced attack in a delay-inducing network environment. From the results in Figure 1, we can see that the actual attacker ratio is greatly expanded and reproduced by the network delay (d=5.7) and the attack type rather than the pure attacker generation rate (λ_a) [8]. This significantly reduces the stability of delay-tolerant IoET networks, reducing the security region. To overcome this attacker effect, we confirmed that increasing the periodic fork delay (d=5.7) significantly improved the security region.

Figure 1 plots the upper bound of the security region (red) for attackers attempting a balanced attack in a communication system that induces an average delay Δ. To mitigate the attacker's attack, we analyzed the case where an alliance between honest nodes was formed and a delay-adjustment policy was applied to message transmission, achieving a 50% ($\Delta_f=\Delta/3$, γ=75%) control. To overcome the effects of these attackers, forming coalitions between honest nodes and applying fork-delay control techniques can expand the bound of these security regions.

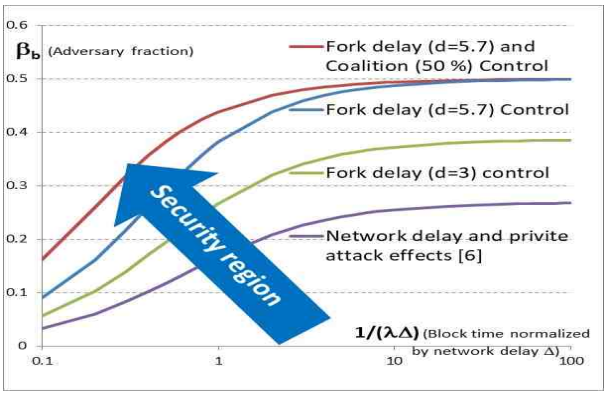

Fig. 1. An example of extending the upper bound of the security region of the consensus algorithm in the balanced attacker ocupation rate β_b for the transmission delay control policy between affiliated nodes when the branch is periodically delayed by a certain amount of time d in a communication network delay situation.

Acknowledgment

This paper is a research conducted with the support of the Korea Institute of Marine Science & Technology Promotion (KIMST) funded by the government (Ministry of Science and ICT) in 2025. [No. 2021-0626, Development of Polar Region Communication Technology and Equipment for Internet of Extreme Things (IoET)].

References

[1] A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A. N. W. Y. Lee, D. Yoo, D. Y. Lee, and M. Choi, "Added text on the Requirements of distributed ledger systems (DLS) for secure human factor services," ITU-T Question 24 Study Group 16, Apr. 2020.

[2] L. Kiffer, J. Neu, S. Sridhar, A. Zohar, and D. Tse, "Nakamoto Consensus under Bounded Processing Capacity," ACM SIGSAC Conference on Computer and Communications Security, pp. 363-377, Dec. 2024.

[3] R. B. Myerson, Game Theory. Cambridge, MA, USA: Harvard Univ. Press, 2013.

[4] Z. Han, D. Niyato, W. Saad, T. Basar, and A. Hjørungnes, Game Theory Wireless Communication Networks: Theory, Models, Application. Cambridge, U.K.: Cambridge Univ. Press, 2012.

[5] J. Neu, E. N. Tas, and D. Tse, "Ebb-and-Flow Protocols: A Resolution of the Availability-Finality Dilemma," IEEE Symposium on Security and Privacy, pp. 446-465, Sept. 2021.

[6] A. Dembo, S. Kannan, E. N. Tas, D. Tse, P. Viswanath, X. Wang, and O. Zeitouni, "Everything is a race and Nakamoto always wins," Proceedings of the 2020 ACM SIGSAC, pp. 859-878, 2020.

[7] Zhan Shi, "Branching Random Walks," volume 2151 of Lecture Notes in Mathematics, Springer Verlag, New York NY, 2015.

[8] J. Garay, A. Kiayias, and N. Leonardos, "The bitcoin backbone protocol: Analysis and applications," in Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 281-310, Springer, 2015.