Security Analysis for Applying the Proof-of-Stake Consensus Algorithm to IoET Network in Antarctica

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

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

***Abstract*— In Antarctica, many studies in various fields are conducted every year. Some of these studies use sensors to collect relevant data for scientific research. However, Antarctica's lack of communication resources makes it difficult to automate this data collection. In most cases, this collection is done manually and the time and space of the study are limited. Over the past few years, several alternatives for deploying remote wireless sensor networks in Antarctica have been explored. Therefore, in this paper, the analysis of the delay-tolerant network was performed based on the partial Δ-synchronized proof-of-stake (PoS) blockchain model. 82% (=1-1/(2e)) of active honest nodes must satisfy the quorum to ensure the security of the proof-of-stake blockchain. If the adversary has less than 18% of the total stake and sets the overall growth rate low, the longest chain protocol is secure. However, as Nakamoto argues in proof-of-stake blockchain protocols, an adversary cannot secure the longest-chain protocol at less than 50% of total stake. In this study, we analyzed how this network delay and balance attack could affect the proof-of-stake consensus protocol in order to find a way for an adversary to secure the longest-chain protocol at less than 50% of the total stake.**

Keywords— Proof-of-stake, IoET, Consensus Algorithm, Antarctica

I. INTRODUCTION

The communication network in the extreme cold region environment must collect a large amount of data according to the power consumption limits of fixed sensors and the changing position of moving unmanned autonomous robots. As an alternative to providing these services, the opportunistic technology of delay-tolerant networks (DTNs) can be used to achieve this challenging goal. Due to the characteristics of these wireless communication networks, these networks may cause congestion and packet loss [1]. We request these network protocols analysis and evaluation of candidate technologies that can satisfy the most suitable requirements for reliability and goal to find a way to solve problems in these network congestion and packet loss situations.

In spite of various problems in DTN, the data collected through multiple paths must be agreed upon as the same data value in all nodes. These consensus techniques can be classified into two main types: proof-based consensus and Byzantine consensus [2]. The first group is related to blockchain technology where all participants compete with each other to mine blocks, the most commonly used protocols being proof-of-work, proof-of-stake, and variants thereof. The main drawback of applying these protocols for IoET (Internet of Extreme Things) is that the devices usually have low hardware resources and low processing power, which makes mining operations on the blockchain extremely difficult. Byzantine-based protocols, on the other hand, implement voting-based techniques to reach consensus without competing with each other, which generally consumes less resources. However, the main drawback of Byzantine-based techniques is the large messages that must be transmitted across the network to reach agreement. In extreme conditions such as IoET, we face a challenging problem of reducing the complexity of the communication network.

As a distributed ledger technology to overcome this waste of computing power and communication, proof-of-stake is an energy-efficient alternative. To analyze the security guarantee of this distributed ledger technology, [3] started the blockchain security analysis by defining the main attributes of common chain prefix, chain quality, and chain growth. When applying the proof-of-work protocol to the lock-by-step-continuous-circulation model for solving the longest chain protocol, the common chain prefix property is very difficult to interpret. Then, if the number of attacker blocks in the long window technique is uniquely smaller than the number of successful honest blocks, the guarantee condition for stability will be met [3]. A similar block-aggregation analysis was performed in the case of a partially Δ-synchronous model [4].

In this paper, we will evaluate the safety of the longest blockchain protocol in terms of the partial Δ-synchronous model for proof-of-stake blockchain protocols. However, in general PoS blockchain protocols, the longest chain protocol cannot be secured by an adversary with less than 50% of the total stake, as Nakamoto argued [5]. In this study, to find the scheme to safely keep the longest chain protocol under 50% of adversary's stake, we analyzed how it can affect the proof-of-stake consensus protocol in the event of network delay.

II. Analysis of Security Guarantee Conditions of Proof-of-Stake Consensus Algorithm

An important property of the longest chain protocol used to maintain distributed ledgers in an public environment is security. An adversary privately grows a private chain to outperform the longest public blockchain, replacing it when the depth of one block is longer on the main blockchain. If λ_a and λ_h are the creation rates of attackers and honest nodes, respectively, it is obvious from the large number law that if $\lambda_h < \lambda_a$, no matter how long the epoch depth k is, the attacker will succeed with a high probability. Conversely, if $\lambda_h < \lambda_a$, the probability of success of the attack decreases exponentially with k. The conditions for safety in a partial Δ-synchronous network environment are as follows [6].

$$\lambda_a < \frac{1}{\frac{1}{\lambda_h}+\Delta} = \frac{\lambda_h}{1+\Delta\lambda_h} \tag{1}$$

where $1+\lambda_h\Delta$ is the effect of network delay on the honest chain's growth rate. λ $(=\lambda_h+\lambda_a)$ is the total growth rate and $\lambda\Delta$ is the number of blocks produced by network delay. Solving the above equation leads to Nakamoto's core argument [5]. If the adversary has less than 50% of the total stake and sets the overall growth rate low, the longest chain protocol will be secure. Increasing the growth rate more aggressively to speed up block generation reduces this security threshold. Therefore, the above formula is the relationship between security and block generation speed including communication network delay. For a certain time slot t, λ_h and λ_a respectively yield the following conditions.

$$\lambda_a t = pf < \frac{\lambda_h t}{1+\Delta\lambda_h} = \frac{p(n-f)}{1+\Delta\lambda_h} \tag{2}$$

By rearranging the above inequality in terms of $\Delta f\lambda_h$, the following equation can be obtained. This can obtain an upper bound on the added to which the adversary's participation expectation value pf is amplified by the delay Δ in unit time t.

$$\frac{\Delta pf}{t} < \frac{n-2f}{n-f} \tag{3}$$

Here, since $\lambda_a t = pf$, the above equation can guarantee the security of the transaction only when signatures of more than 2/3 of total nodes are honest. If $n > 3f$ is satisfied, the above expression must satisfy the following condition.

$$\Delta\lambda_a < \frac{n-2f}{n-f} < \frac{1}{2} \tag{4}$$

This is the same as the condition that the security of the proof-of-stake blockchain can be guaranteed only when a 2/3 quorum of active honest nodes is satisfied [6].

On the other hand, we provide an example for the adversary forking in terms of Branching Random Walk (BRW) [7]. When $I_k = \{i_1, ..., i_k\}$ as a collection of k-tuples for positive integers, $\mathbf{I} = \cup_{k>0} I_k$. We can show elements of **I** as the labeling of the vertices of an infinite tree rooted. At this time, I_k represents the vertices of the k-generation in the branch by numbering as follows: vertex $\mathbf{v} = (i_1, ..., i_k) \in I_k$ is the vertex of the number (label) k-1 $(i_1, ..., i_{k-1})$ is the i_kth child. An example of numbering can be represented as in Figure 1. For $j = 1, ..., k$, if $\mathbf{v}^j = (i_1, ..., i_j)$ is defined, then $\mathbf{v}^j$ becomes the parent of **v** at number j ($\mathbf{v}^k$ = **v**). For convenience of notation, $\mathbf{v}^0 = \mathbf{0}$ is set as the root of the branch.

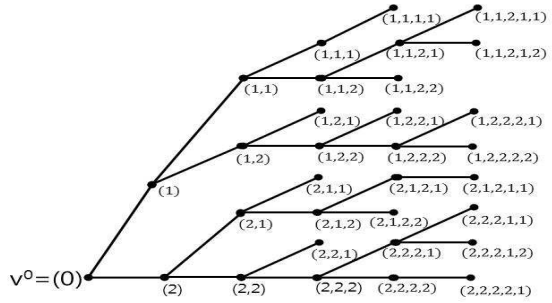

Figure 1. An example of labeling in a branching random walk machine.

Let the following expression $\{\mathbf{t}_v\}v \in \mathbf{I}$ be an independent and identically distributed set of exponential random variables with the growth rate as a parameter λ_a. For vertex $\mathbf{v} = (i_1, ..., i_k) \in I_k$, set $\mathbf{T}_v = \Sigma_{j\leq ik}\mathbf{t}_{(i1,...,ik-1,\,j)}$ and $\mathbf{W}_v = \Sigma_{j\leq k}\mathbf{T}_{vj}$ for the case $\mathbf{v}^j = (i_1, ..., i_j)$ is such that $\mathbf{v}^j$ measured after the occurrence of v_j-1 appears is the waiting time until **v** and $\mathbf{W}_v$ is the average waiting time until the appearance of **v**. The definition of the Laplace transform with a random variable **T** with an independent identity distribution (i.i.d.) is as follows.

$$E(e^{-sT}) = \int_0^\infty e^{-st}\lambda_a e^{-\lambda_a t}\,dt = \lambda_a\int_0^\infty e^{-(s+\lambda_a)t}dt$$

$$= \lambda_a\left[\frac{1}{s+\lambda_a}e^{-(s+\lambda_a)t}\right]_0^\infty = \frac{\lambda_a}{s+\lambda_a} \tag{5}$$

If we define the log Laplace transform for $W_V = \sum_{j\leq k}T_{vj}$, we get the following equation [7, Theorem 1.4].

$$\log\sum_{v\in I_\infty}E(e^{-sW_v}) = \log\sum_{j=1}^\infty E\left(e^{-s\sum_{l=1}^j t_l}\right)$$

$$= \log\sum_{j=1}^\infty\left(E(e^{-st_1})\right)^j = \log\frac{E(e^{-st_1})}{1-E(e^{-st_1})} = \log\frac{\lambda_a}{s} \tag{6}$$

The minimum value of the average waiting time $\mathbf{W}_v$ until the appearance of **v** can be defined as the following equation.

$$W_k^* = \min_{v\in I_k} W_v \tag{7}$$

According to Reference [7, Theorem 1.3], the minimum value of the average waiting time is the limit value of the log Laplace transform of the average waiting time $\mathbf{W}_v$ and can be expressed as the following equation.

$$\lim_{k\to\infty}\frac{W_k^*}{k} = -\inf_{s>0}\frac{\log\sum_{v\in I_\infty}E(e^{-sW_v})}{s} \tag{8}$$

The above equation is succinctly summarized as follows when substituted with the Laplace transform value of an exponential random variable **T** having an independent identity distribution.

$$-\inf_{s>0}\frac{\log\sum_{v\in I_\infty}E(e^{-sW_v})}{s} = \frac{1}{\lambda_a}\sup_{s>0}\frac{\log\frac{s}{\lambda_a}}{\frac{s}{\lambda_a}} = \frac{1}{e\lambda_a} \tag{9}$$

Therefore, assuming that the adversary's attack is a branch random walking machine, it can be showed that the growth rate amplify to $e\lambda_a$ at the depth of $\mathbf{T}_0(t)$. Thus, to overcome this, the condition of the following equation has to be satisfied.

$$e\lambda_a < \lambda_h \quad (10)$$

If $\lambda_h = e\lambda_a$ in the above formula, $e\lambda_a < 0.5$ must be satisfied. This is a condition in which 82% (=1-1/(2e)) of active honest nodes must satisfy the quorum to ensure the security of the proof-of-stake blockchain. As long as the adversary sets it low, below 18% of the total stake in the blockchain, the longest chain protocol will be secure.

III. Analysis of Proposed Periodic d-Time Forking Delayed Proof-of-Stake Scheme

In the PoS blockchain protocol, a technique can be proposed to prevent the block from forking periodically for a certain period of time delay d.

Since the branch random walk starts labeling at the vertices of the tree after a period d delay, the logarithmic Laplace transform of the average waiting time $\mathbf{W}_v$ can be expressed as the following equation [7].

$$\log \sum_{v \in I_\infty} E(e^{-sW_v}) = \log \sum_{j=1}^{\infty} \left(E(e^{-st_1})\right)^{dj} \quad (11)$$

Simplifying the above expression, it can be expressed by converting it to the following expression.

$$\log \left\{\sum_{j=1}^{\infty} \left[E(e^{-st_1})^d\right]^j\right\} = \log \frac{\{E(e^{-st_1})\}^a}{1-\{E(e^{-st_1})\}^d}$$

$$= \log \frac{\lambda_a^a}{(s+\lambda_a)^d - \lambda_a^d} \quad (12)$$

The minimum value of the average waiting time is the limit value of the logarithmic Laplace transforms of the average waiting time $\mathbf{W}_v$, and the following equation is a stable state expression.

$$\lim_{k\to\infty} \frac{W_k^*}{k} = -\inf_{s>0} \frac{\log \sum_{j=1}^{\infty} \left(E(e^{-st_1})\right)^j}{s}$$

$$= \sup_{s>0} \frac{\log\left\{\left(\frac{s}{\lambda_a}+1\right)^d - 1\right\}}{s} \quad (13)$$

This above equation can be simplified as follows when $s = e\lambda_a$.

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

$$\simeq \frac{d \log(e+1)}{e\lambda_a} \quad (14)$$

In the above formula, the d value, which is a positive number that can change the minimum value of the average delay time, can be represented as the following equation.

$$d \cong \frac{e}{\log(e+1)} \quad (15)$$

In the proof-of-stake blockchain protocol, if the branching of a blockchain is delayed by a certain period d, the minimum average waiting time becomes $1/\lambda_a$, so the adversary's growth rate slows down to λ_a. Therefore, as Nakamoto argues in proof-of-stake blockchain protocols, we can find a constant delay period d that allows an attacker to safely hold the longest blockchain protocol at less than 50% of the overall growth rate.

IV. Simulation Results

Figure 2 is the result of simulating the upper limit of the security area for the adversary's fraction expansion when an adversary attempts a balanced attack in a communication network that causes delay. From this simulation, it can be figured that the upper bound and security area of the adversary's fraction β varies greatly depending on forking delay (d = 4.7) and attack type (d = 1, balanced attack) rather than the effect of pure adversary growth rate (λ_a). This greatly reduces the stability of the delay-tolerant IoET network and reduces the safe area. It was confirmed that the security region was greatly improved when the periodic forking delay (d) was adjusted to overcome the attacker's influence.

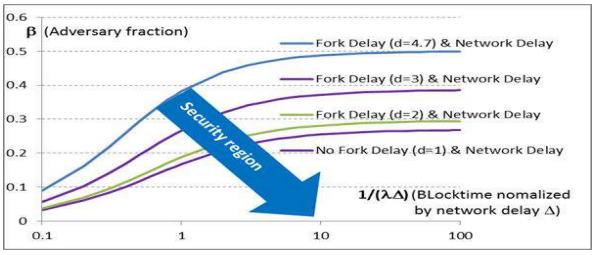

Figure 2. The upper limit and security area of the adversary fraction β when forking is periodically blocked for a certain period of time delay d in the network delay situation.

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 2023. [No. 2021-0626, Development of Polar Region Communication Technology and Equipment for Internet of Extreme Things (IoET)].

References

[1] A. Mallorquí, A. Zaballos, and D. Serra, "A Delay Tolerant Network for Antarctica," IEEE Communications Magazine, pp. 1-7, Aug. 2022.

[2] U. Bodkhe, D. Mehta, S. Tanwar, P. Bhattacharya, P. K. Singh, and W.C. Hong, "A survey on decentralized consensus mechanisms for cyber physical systems," IEEE Access, pp. 54371–54401, Aug. 2020.

[3] 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.

[4] R. Pass, L. Seeman, and A. Shelat, "Analysis of the blockchain protocol in asynchronous networks," in Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2017.

[5] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008, https://bitcoin.org/bitcoin.pdf.

[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 Conference on Computer and Communications Security, pp. 859–878, Oct. 2020.

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