지연 허용 IoET 망에서 지분증명 합의 알고리즘 개선을 위한 안전성(Security) 분석에 관한 연구

이우용, 김근영, 조동욱°

한국전자통신연구원, 6G 무선방식연구실, 충북도립대학교°

{wylee, kykim12}@etri.re.kr, ducho@cpu.ac.kr

A Study on Security Analysis for Performance Improvement of Proof-of-Stake Consensus Algorithm in IoET Delay-tolerant Network

Lee Woo Yong, Kim Keunyoung, and Cho Dongwook°

6G Wireless Technology Research Section
Telecommunication & Media Research Laboratory
Electronics and Telecommunications Research Institute (ETRI) and
Chungbuk Provincial University°

요 약

남극(Antarctica)에서 매년 다양한 분야에서 많은 연구가 수행되며 다량의 데이터가 수집되고 있다. 이러한 자료 중 일부는 센서를 이용하여 관련 데이터를 수집하는데, 남극 대륙의 특성상 통신 자원의 부족은 이러한 자료 수집을 자동화할 가능성을 매우 어렵게 만든다. 극한지의 경우 대부분의 자료수집이 수동으로 이루어지므로 자연과학 연구 수행에서 시간과 공간에 대하여 제한을 받는다. 지난 몇 년 동안 극한지에 원격 무선 센서 망을 설치하기 위한 몇 가지 대안이 연구되었다. 본 논문에서는 남극 대륙과 같은 지역에서 과학기술 자료 수집의 협력과 신뢰성을 확보를 위하여, IoET (Internet of Extreme Things) 망에 지분증명 블록체인 모델을 적용했을 때 안정성을 분석하였다. 본 연구에서는 공격자가 전체 해시 파워의 50% 미만에서 최장 체인 분산원장을 안전하게 유지할 수 방법을 찾기 위해, IoET 망에서 지연과 공격자 점유율에 따라 지분증명 프로토콜에 어떤 영향을 끼칠 수 있는지 분석했다.

Ⅰ. 서 론

남극 대륙과 같은 극한 환경의 통신망은 움직이는 무인 자율 로봇의 위치에 따른 열악한 통신 채널 상태와 부족한 전력에 적응적으로 데이터를 전달해야 한다. 이러한 통신망은 때로는 대량의 데이터를 전송하기 위하여, DTN(Delay-tolerant network)의 기회적(opportunistic) 기술을 사용하여 도전적인 목표 서비스를 제공해야 한다. 극한지 무선 채널 특성으로 인해 IoET 망은 정체(congestion)과 패킷 손실을 발생시킬 수 있다[1]. 우리는 이러한 망의 정체와 손실 상황에서 문제 해결을 위한 방법을 찾기 위한 목표, 신뢰성에 가장 적합한 요구사항을 만족할 수 있는 후보 기술에 대한 평가와 전송 프로토콜 분석을 요구 받는다.

수집 데이터의 신뢰성 확보를 위하여 블록체인 기술을 적용했을 때 성능을 확장하는 가장 인기 있는 후보 기술은 다음과 같다. 후보로 소규모(side) 블록체인은 블록의 해시를 보다 크고 신뢰할 수 있는 블록체인에서 주기적으로 커밋하여 신뢰성을 얻는다. 소규모 블록체인의 블록 순서는 신뢰하는 블록체인의 해시 순서에 따라 결정된다. 이 소규모 블록체인의 보안은 신뢰하는 블록체인의 보안에서 직접 파생된다. 이 메커니즘은 간단하고 실용적이며 효율적이다[2]. 왜냐면 소규모 블록체인 블록의 의미(semantics)를 저장, 처리 또는 검증할 필요가 없고 해시만 저장하기 때문이다. 비트코인과 이더리움 모두에서 실행되는 여러 소규모 블록체인과 함께 실제적으로 매우 인기가 있다; 예를 들면 기부 추적(Binance 자선 단체[3])과 졸업장과 자격 증명 확인(MIT 에서 사용하는 BlockCert[4])이 있다. IoET 에 이러한 블록체인 프로토콜을 적용하는데 주요 유사점은 장치가 일반적으로 하드웨어 자원이 적고 처리 능력이 낮아 채굴 작업을 극도로 어렵게 만든다는 면에서 소규모 블록체인과 같다[5]. 한편 이런 분산원장 기술의 안전성 보장에 대한 분석을 위하여, [6]은 공통 체인 접두, 체인 품질, 그리고 체인 성장의 주요한 속성을 정의하여 블록체인 안전성 분석을 시작한다.

본 논문에서는 IoET 망의 지분증명 블록체인 프로토콜에서 공격자의 해시 파워의 50% 미만에서 최장 체인 프로토콜을 안전하게 유지할 수 방법을 찾기 위해 망 지연이 허용되고 공격자가 있는 상황에서 어떤 영향을 끼치게 되는지 분석했다.

Ⅱ. 주기적 d-시간 분기지연 지분증명 방안제안 및 분석

블록체인 프로토콜에서 그림 1 과 같이 블록을 주기적으로 일정시간 d 만큼 분기하지 못하도록 막는 기법을 제안할 수 있다. 분지 확률보행은 가지(tree)의 꼭지점들(vertices)에서 번호메김(labelling)이 주기 d

지연 이후 시작되기 때문에 평균 대기시간 W_v 의 로그 라플라스 변환은 다음 식으로 나타낼 수 있다[7].

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

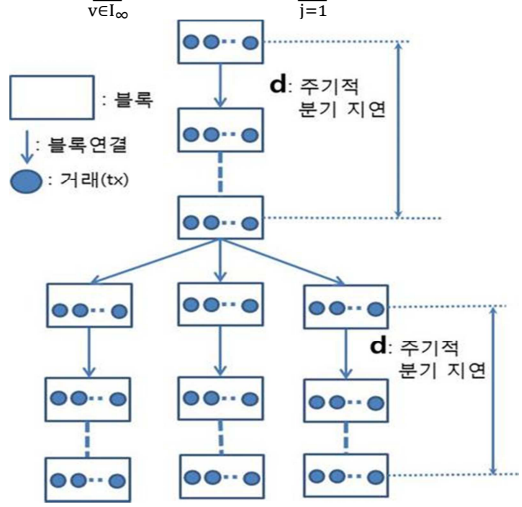

그림 1. 주기적으로 일정시간 d 만큼 분기하지 못하도록 막는 기법.

위 식을 간략하게 정리하면 다음 수식으로 변환하여 나타낼 수 있다.

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

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

참고문헌[8, 정리 1.3]에 의하여 평균 대기시간의 최소값은 평균 대기시간 W_v 의 로그 라플라스 변환의 극한 값으로 다음 식은 정상상태(stable state) 표현이다.

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

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

이 수식은 $s=e\lambda_a$ 일 때, 다음과 같이 간략히 정리할 수 있다.

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

위 수식에서 평균 대기시간의 최소값을 변경할 수 있는 양수인 d 값은 다음 수식과 같이 나타낼 수 있다.

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

지분증명 블록체인 프로토콜에서 블록의 분기를 일정 주기 d 지연 시키면 평균 대기시간의 최소값은 $1/\lambda_a$ 가 되므로 공격자의 성장속도가 λ_a 로 느려진다. 그러므로 지분증명 블록체인 프로토콜에서 나카모토의 주장과 같이 공격자가 전체 해시 파워의 50% 미만에서 최장 체인 프로토콜을 안전하게 유지할 수 있은 일정 지연 주기 d 를 찾을 수 있다.

Ⅲ. 모의 실험 결과

그림 2 은 지연을 유발하는 통신망에서 공격자가 균형공격을 시도했을 때 공격자 비율 확대에 대한 안전영역의 상한선을 모의 실험한 결과이다. 이 분석에서 우리는 실제 공격자 비율이 순수한 공격자 생성속도(λ_a)에 의한 영향보다 통신망 지연(d=5.7)과 공격 유형에 따라 크게 확대 재생산됨(d=1)을 알 수 있다. 이것은 지연허용 IoET 망의 안정성을 크게 떨어뜨려 안전한 영역을 감소시킨다. 이러한 공격자의 영향을 극복하기 위하여 주기적 분기 지연(d)을 늘렸을 때 안전한 영역이 크게 향상됨을 확인하였다.

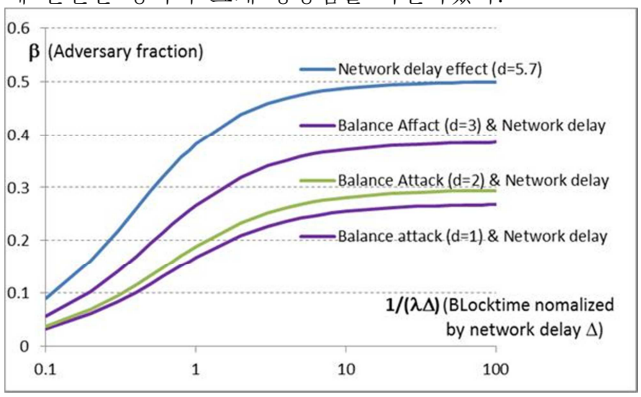

그림 2. 통신망 지연 상황에서 주기적으로 일정시간 d 만큼 분기를 막았을 때 공격자 점유율 β 의 상한선과 안전 영역.

ACKNOWLEDGMENT

본 논문은 2023 년도 정부(과학기술정보통신부)의 재원으로 해양수산과학기술진흥원의 지원을 받아 수행된 연구이다. [No.2021-0626, IoET 를 위한 극한지 통신 및 장비 기술 개발].

참 고 문 헌

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

[2] P. Sheng, B. Xue, S. Kannan, and P. Viswanath, "ACeD: scalable data availability oracle." arXiv preprint arXiv: 2011.00102, 2020.

[3] A. Foti and D. Marino, "Blockchain and charities: A systemic opportunity to create social value," In Economic and Policy Implications of Artificial Intelligence, Springer, pp. 145-148, 2020.

[4] M. Jirgensons and J. Kapenieks, "Blockchain and the future of digital learning credential assessment and management," Journal of Teacher Education for Sustainability 20(1), 145-156, 2018

[5] 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.

[6] 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.

[7] M. Drmota, "The height of increasing trees," Annals of Combinatorics, 12(4):373–402, 2009.

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