통신망 지연 영향에서 개인 공격(Private Attack)에 대한 제휴정책의 안전성(Security) 분석

이우용, 김근영
한국전자통신연구원

{wylee, kykim12}@etri.re.kr

Security Analysis of Coalition Strategy against Private Attacks in Network Delays

Lee Woo Yong and Keunyoung Kim
Electronics and Telecommunications Research Institute (ETRI)

요 약

제한된 통신 용량과 컴퓨터 연산 자원을 가진 네트워크가 주어졌을 때, 블록체인은 나카모토 합의(Nakamoto consensus)는 주어진 블록 생성 속도에서 공격자의 공격 능력에 대해 안전한가? 지금까지 나카모토 합의 알고리즘의 분석은 이 질문에 답하지 못한다. 한편, 게임이론은 제한된 용량의 통신망에 적용되는 블록체인 합의 알고리즘을 개선하기 위한 솔루션으로 적용될 수 있을 것이다. 제안된 용량의 통신망에서 특정 체인에 더 많은 채굴자가 참여할수록 해당 블록체인의 가치가 높아지므로 채굴자의 게임이론 전략은 개인 이익뿐만 아니라 다른 채굴자의 이익에도 좌우된다. 본 분석은 개방형 시스템을 부분 Δ-동기 모델의 관점에서 분석했을 때, 개인공격(Private Attack)에 대하여 안정성을 확보하기 위한 방안을 찾기 위한 사전분석이다. 제안된 기법은 게임이론적 기법에 대한 적용으로 정직한 노드들이 제휴하여 지연을 조절하는 방법이다. 본 연구는 부분 Δ-동기화된 통신망에서 제휴한 노드가 서로 메시지를 전달하는 시간 지연을 제어함으로써 개인공격에서 공격자 점유율에 따른 안전 영역 상한선 확장 가능성을 조사하는 것이다.

Ⅰ. 서론

통신 용량과 컴퓨터 연산 자원이 제한된 네트워크가 주어졌을 때, 블록체인은 나카모토 합의는 주어진 블록 생성 속도에서 공격자의 공격 능력에 대해 안전한가? 지금까지 나카모토 합의 알고리즘의 분석은 이 질문에 답하지 못한다[1]. 제한된 지연(bounded-delay) 모델에서 블록이 빠르게 연속적으로 생성될 때 혼잡을 유발하는 노드의 블록 처리 속도 제한을 제때에 알지 못하기 때문이다. 제한된 용량(bounded capacity) 모델에서 작업 증명(Proof of Work) 나카모토 합의에 대한 보안성과 성능 사이의 절충을 계산할 수 있는 가능성을 검토해 보고자 한다.

한편, 게임이론[2]은 제한된 용량의 통신망에 적용되는 블록체인 합의 알고리즘을 개선하기 위한 솔루션으로 적용될 수 있다. 이 게임이론은 의사 결정자들의 합리적인 전략적 상호간 작용에 관한 수학적 모델이다[3]. 따라서 게임이론은 협력 및 합의 노드의 전략과 그들 간의 상호 작용을 분석하는 데 사용될 수 있다. 게임이론 분석을 통해 노드들은 서로의 채굴 행위를 학습하고 예측할 수 있으며, 내쉬 균형(equilibrium) 분석을 기반으로 최적의 반응 전략을 선택할 수 있다. 이러한 최적 반응 전략은 노드가 오작동하거나 공격을 시작하는 것을 방지하는 메커니즘으로 사용될 수 있다. 따라서 게임이론은 분산원장 통신망의 모든 합의 노드의 의사 결정 과정을 모델링하기 위한 자연스러운 고려 사항이다.

분산원장 통신망에서 특정 체인에 더 많은 채굴자가 참여할수록 해당 블록체인의 가치가 높아지므로 채굴자의 게임이론 전략은 개인 이익뿐만 아니라 다른 채굴자의 이익에도 좌우된다[4]. 조정 게임에서 채굴자의 전략이 대다수 채굴자의 전략과 일치하지 않으면 채굴자는 수익이 0이 되며, 이 게임은 고유한 내쉬 균형을 허용한다. 게임에 참여하는 플레이어는 블록체인 사용자이자 채굴자이며, 유틸리티를 극대화하려면 두 개의 포크 체인 중 하나를 선택해야 한다[5]. 여기서 블록체인 사용자의 효용성은 사용자가 특정 체인을 선택하는 분포, 거래 수수료, 채굴자의 게임이론 전략에 따라 결정된다. 채굴자의 효용성은 두 개의 포크 체인 사이의 사용자 분포, 계산 능력, 채굴 보상 및 다른 채굴자의 체인 선택에 따라 결정된다.

본 논문에서는 부분 Δ-동기화된 통신 모델에서[6], 개방형 블록체인 시스템에 게임이론 기법을 적용했을 때 합의 알고리즘의 성능 개선을 분석하고자 한다. 공격자의 공격을 방어하기 위한 기법으로 노드들이 서로 제휴하여 지연제어 방식을 사용했을 때 통신망 지연 영향을 분석하고 새로운 안전한 이론적 영역을 제안한다.

Ⅱ. 작업증명 블록체인의 합의 알고리즘에 대한 제휴정책의 안전성 분석

개방(permission less) 환경에서 분산원장을 유지하는데 사용되는 최장 체인 프로토콜의 중요한 속성은 보안(안정성)이다. 공격자는 공개된 최장 블록체인을 능가하기 위해 개인적으로 비공개 체인을 성장시켜 공개 블록체인에서 한 블록의 깊이가 더 길어지면 이를 대체한다. λ_a와 λ_h는 각각 해시 파워에 비례하는 공격자와 정직한 노드의 각각 채굴 속도라고 할 때, $\lambda_h < \lambda_a$ 이면, 블록시간가 아무리 길어 지더라도 높은 확률로 공격자가 성공할 것은 큰 수 법칙(large number's law)으로부터 자명하다. 반대로,

$\lambda_h > \lambda_a$ 이라면, 공격의 성공 확률은 블록시간에 따라 기하 급수적으로 급격하게 줄어든다. 부분 Δ-동기화된 통신망 환경에서 안전성에 대한 조건은 아래 수식과 같다[7].

$$\lambda_a < \frac{1}{\frac{1}{\lambda_h}+\Delta} = \frac{\lambda_h}{1+\Delta\lambda_h} \quad (1).$$

여기서, $1+\Delta\lambda_h$ 는 정직한 체인의 성장률에 대한 통신망 지연의 영향이다. 총 채굴 속도를 $\lambda(=\lambda_h+\lambda_a)$라 하면, $\Delta\lambda$는 통신망 지연당 채굴된 블록 수가 된다. 수식(1)을 등식으로 풀면 나카모토의 핵심 주장으로 이어진다[4]. 공격자가 전체 해시 파워의 50% 미만이고 전체 채굴 속도를 낮게 설정하면, 최장 체인 프로토콜은 안전할 것이다. 블록체인 속도를 높이기 위해보다 적극적으로 채굴 속도를 높이면 이 보안 임계 값을 줄이게 된다.

정직한 노드 사이의 영향력을 높이기 위하여 제휴를 하고, 선호 여부에 따라 노드에 대하여 지연 Δ_f 을 가감하여 메시지를 전달하는 전송정책을 사용한다고 가정하면 지연은 다음과 같은 식으로 계산될 수 있다.

$$\lambda_a < \frac{\lambda_{hf}+\lambda_{h-f}}{1+(\Delta-\Delta_f)\lambda_{hf}+(\Delta+\Delta_f)\lambda_{h-f}} \quad (2).$$

여기서 λ_{hf} 는 지연을 감소시킬 노드의 성장속도이고 λ_{h-f} 는 지연을 증가시킬 노드의 성장속도를 말한다. 이때 $\lambda_h = \lambda_{hf}+\lambda_{h-f}$ 를 가정한다. 임의의 제어변수 $1>\gamma\geq 1/2$ 에 대하여 각 노드의 지연을 관리할 수 있다면 식 (2)는 다음 부등식과 같이 간략히 나타낼 수 있다.

$$\lambda_a < \frac{\lambda_h}{1+\{\Delta-\Delta_f(2\gamma-1)\}\lambda_h} \quad (3).$$

평균 부분 Δ-동기 통신망 환경에서 $\hat{\Delta}=\Delta-\Delta_f(2\gamma-1)$ 라 할 때, 공격자 노드의 참여 기대 평균 값을 β_b 라고 가정한다. 또한 총 채굴 속도를 λ 라 할 때, 통신망 지연당 채굴된 블록 수 $\Delta\lambda$ 에 대한 β_b의 상한 값은 식 (3)로부터 다음 부등식과 같이 유도된다.

$$\beta_d < \frac{1-\beta_d}{1+(1-\beta_d)\bar{\Delta}\bar{\lambda}}$$

위 부등식에 대하여 β_d 의 2 차 방정식에 대한 부등식으로 다음 수식으로 표현할 수 있다.

$$\bar{\Delta}\bar{\lambda}{\beta_d}^2-(2+\bar{\Delta}\bar{\lambda})\beta_d+1>0$$

여기서 β_d의 2 차 방정식의 해는 다음 부등식의 상한 값을 갖는다.

$$0 \leq \beta_d \leq \frac{1}{2}+\frac{1}{\bar{\Delta}\bar{\lambda}}-\sqrt{\left(\frac{1}{2}\right)^2+\left(\frac{1}{\bar{\Delta}\bar{\lambda}}\right)^2}$$

β_d를 $\frac{1}{\Delta\lambda}$(block time normalized by network delay Δ)에 대하여 그래프로 그리면 그림 1 의 실선과 같다. 이 실선 그래프는 참고문헌[7]의 POW/POS 모델에 대한 참 안전 문턱값(True security threshold)과 같다. 또한 제한 조건 $\bar{\Delta}\lambda_a=\bar{\Delta}\lambda\beta_d<\frac{1}{2}$를 만족하므로(그림 1 의 점선), β_d 의 상한 값은 두 경계 값의 최소를 가지므로 다음 수식과 같다.

$$\beta_d \leq \min_{\frac{1}{\Delta\lambda}>0}\left(\frac{1}{2\,\Delta\lambda},\ \frac{1}{2}+\frac{1}{\bar{\Delta}\bar{\lambda}}-\sqrt{\left(\frac{1}{2}\right)^2+\left(\frac{1}{\bar{\Delta}\bar{\lambda}}\right)^2}\right)$$

이때 두 상한 값 교차점은 $\frac{1}{\bar{\Delta}\bar{\lambda}}=\frac{2}{3}$이고 β_d =1/3 가 된다(파란색 점선과 실선). 그림 1 은 통신시스템이 평균지연 Δ를 유발하는 상황에서 공격자가 균형공격을 시도했을 때 공격자 비율 확대에 대한 안전영역 상한선(파란색)을 그린 것이다. 공격자 노드의 공격을 완화시키기 위하여 정직한 노드 사이 제휴를 맺고 메시지 전송에 지연 가감정책에 사용하여 50% ($\Delta_f=\Delta$, γ=75%) 제어할 수 있는 경우와 33% ($\Delta_f=\Delta$, γ=66%) 제어할 수 있는 경우에 대하여 분석하였다.

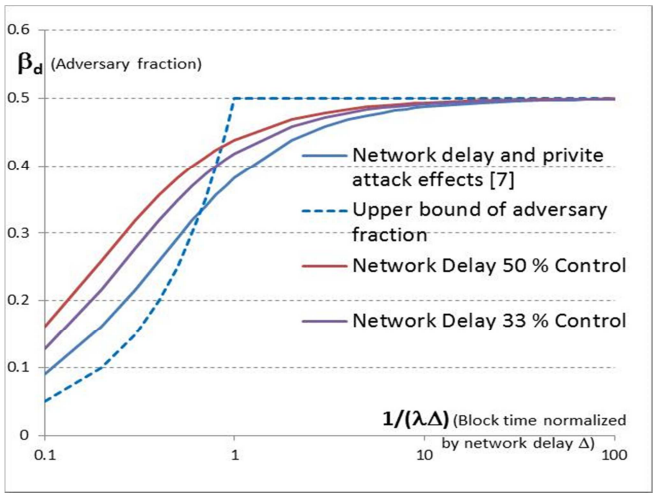

그림 1. 제휴 노드 사이의 전송지연 가감정책에 따른 통신망 지연과 개인 공격에 대한 공격자 점유율 β_d 에서 지연 경감제어 비율에 따른 안전 영역 상한선 확장 예.

ACKNOWLEDGMENT

본 논문은 2025 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] 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.

[2] 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.

[3] V. Bagaria, S. Kannan, D. Tse, G. Fantiz, and P. Viswanath, "Prism: Deconstructing the Blockchain to Approach Physical Limits," ACM SIGSAC Conference on Computer and Communications Security, pp. 585-602, Nov. 2019.

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

[5] 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.

[6] 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.

[7] A. Dembo, S. Kannan, E. N. Tas, D. Tse, P. Viswanath, X. Wang, and O. Zeitouni, "Everything is a race and Nakamoto always wins," ACM SIGSAC Conference on Computer and Communications Security, pp. 859-878, Nov. 2020.