통신망 지연 영향에서 분할 조정 연합 정책 합의 기법의 보안 분석

이우용, 김근영

한국전자통신연구원
{wylee, kykim12}@etri.re.kr

Security Analysis of the Forking Adjust Coalition Policy Consensus Algorithm under the Impact of Network Delay

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 따라 안전하기 못하다[7]. 분할 조정 합의 기법은 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 전략은 개인 이익뿐만 아니라 다른 채굴자의 이익에도 좌우된다. 본 분석은 개방형 시스템을 부분 Δ-동기 모델의 관점에서 분석했을 때, 공격자의 공격(Teasing Attack)에 대하여 안정성을 확보하기 위한 방안을 찾기 위한 사전분석이다. 제안된 기법은 분할 조정 정책 기법에 대한 적용으로 정직한 노드들이 연합하여 지연을 조절하는 방법이다. 본 연구는 부분 Δ-동기화된 통신망에서 연합한 노드가 서로 메시지를 전달하는 시간과 블록 분할을 연합 조정을 제어함으로써 공격자 점유율에 따른 안전 영역 상한선 확장 가능성을 조사하는 것이다.

Ⅰ. 서 론

분산원장의 신뢰성 검증을 위하여 다양한 형태의 블록체인에 대한 해석적 분석이 통신모델 기반으로 수행되어 왔다[1]. 이 최장 체인 프로토콜은 단순하지만 강력한 합의 알고리즘이라는 것이다[2]. 이 분산원장의 안전성 보장에 대한 분석을 위하여, 접두 공통 체인 품질과 체인 성장의 주요한 속성들에 대한 블록체인의 안전성(security, 보안) 분석이 시작되었다[3]. 최장 체인 프로토콜 해석을 위하여 잠금-단계별(lock step)-연속-순환 모델에 대한 작업증명(Proof of Work) 기법을 적용할 때 해석하기 매우 어려운 특성인 공통 체인 접두 특성은 긴 창(window) 기법에서 공격자 블록의 수가 성공한 정직한 블록 수보다 독보적으로 적다면 충족된다[4]. 그리고 유사한 블록-집계 분석은 부분 Δ-동기(partially simultaneous) 모델 환경에서 분석되었다[4].

통신망에서 특정 체인에 더 많은 채굴자가 참여할수록 해당 블록체인의 가치가 높아지므로 채굴자의 이익뿐만 아니라 다른 채굴자의 이익에도 좌우된다[5]. 채굴자의 전략이 대다수 채굴자의 전략과 일치하지 않으면 채굴자는 수익이 없어진다. 연합에 참여하는 플레이어는 블록체인 사용자이자 채굴자이고, 유틸리티를 극대화하려면 두 개의 포크 체인 중 하나를 선택해야 한다[5]. 여기서 블록체인 사용자의 효용성은 두 개의 포크 체인 사이의 사용자 분포, 계산 능력, 채굴 보상 및 다른 채굴자의 체인 선택에 따라 결정된다.

본 논문에서는 지연허용 부분 Δ-동기화된 모델에서 [6], 개방형 블록체인 시스템에 대한 분할 조정 기법을 적용했을 때 합의 알고리즘의 성능 개선을 분석하고자 한다. 공격자의 공격을 방어하기 위한 기법으로 노드들이 서로 연합하는 조정하는 방식을 사용했을 때 통신망 지연 영향을 분석하고 새로운 안전한 영역을 제안한다.

Ⅱ. 부분 Δ-동기 모델의 관점에서 합의 알고리즘의 안전성에 대한 상한 분석

통신망 환경에서 부분 Δ-동기화된 노드 전체 수를 n 이라 하고, 공격자 수 f 라 하자. 하나의 시간 간격에서 어떤 노드가 하나의 블록을 제안할 확률을 p 라면, 공격자가 참여할 기대 값을 β라 하고, 정직한 노드의 기대 값을 α라 하면 다음 식과 같이 표현될 수 있다.

$$\beta = pf,\ \alpha = p(n-f)$$

부분 Δ-동기화된 통신망에서 지연을 Δ라고 할 때, 공격자 노드가 참여할 기대 값 β이 <1/2 일때, 안정성을 보장할 수 있다[6].

실제 분산 시스템은 네트워크 지연이 불규칙하게 발생하는 경우가 많으므로, 부분 Δ-동기식 모델에서의 분석은 매우 중요하다. 이 모델은 프로토콜의 복원력에 대해 또 다른 흥미로운 통찰을 제공하며, 특히 클라이언트 모델의 영향력이 어떻게 변화하는지를 보여준다. 부분 Δ-동기식 환경의 가장 핵심적인 특징은 클라이언트 모델의 영향력이 거의 사라진다는 점이다. 즉, 클라이언트가 졸림 상태인지, 통신이 가능한지와 무관하게 달성 가능한 안전성-활성성 복원력 쌍이 거의 동일하게 나타난다. 이러한 특성은 부분 Δ-동기식 모델이 다양한 클라이언트 환경에 대해 매우 "견고함(robustness)"을 가짐을 의미한다.

이 모델에서는 오래 전부터 알려진 $2\beta + \alpha/2 < 1$ 이라는 강력한 불가능성 결과가 존재한다[7]. 이 제약은 복원력에 대한 근본적이고 엄격한 상한선을 설정하기 때문에, 클라이언트의 성능을 아무리 향상시켜도 이 한계를 넘어설 수 없다. 즉, 클라이언트 모델이 제공할 수 있는 이점이 원천적으로 차단되는 것이다. 이 모델의 '견고함'이 역설적으로 과거 분산 시스템 문헌에서 클라이언트 모델링이 상대적으로 주목 받지 못했던 '사각지대'를 만들었던 이유를 이 지점에서 찾을 수 있을 것이다.

개방(permission less) 환경에서 분산원장을 유지하는 데 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. 총 채굴 속도를 $\lambda(=\lambda_h+\lambda_a)$라 하면, $\Delta\lambda$는 통신망 지연당 채굴된 블록 수가 된다. 위 수식을 등식으로 풀면, 나카모토의 핵심 주장으로 이어진다[2]. 블록체인 속도를 높이기 위해 보다 적극적으로 채굴 속도를 높이면 이 보안 임계 값을 줄이게 된다. 그러므로 참고문헌[8]의 정리 2, 3 에서 해석한 결론, 즉 모든 활성화된 정직한 노드의 2/3 이상의 정족수가 되어야 거래에 대한 보장을 할 수 있다는 것이다. n>3f 를 만족한다면 다음 같은 조건이 되어야 한다.

$$\Delta\lambda_a < \frac{n-2f}{n-f} < \frac{1}{3}$$

위 결론은 $\Delta\lambda_a < 1/3$ 가 되어야 안전을 보장받을 수 있다는 것이다.

부분 Δ-동기 통신망 환경에서 공격자 노드가 참여할 기대 값 β_d 과 총 채굴 속도를 λ 라 할 때, $\lambda\Delta$ 는 통신망 지연당 채굴된 블록 수라고 할 때 β의 상한 값은 다음 식으로 나타낼 수 있다.

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

위 부등식에 대하여 β_d의 2 차 방정식의 해는 다음 부등식의 상한 값으로 나타낼 수 있다.

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

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[8]의 POW 모델에 대한 참 안전 문턱 값(True security threshold)과 같다.

Ⅲ. 안전성 상한 결과

그림 1 은 통신시스템이 평균지연 Δ 를 유발하는 상황에서 공격자가 공격을 시도했을 때 공격자 비율 확대에 대한 안전영역 상한선을 표시한 것이다. 통신망 지연으로 공격자의 점유율이 확대되어 블록체인 시스템의 안전성이 감소하는 정도를 나타낸다.

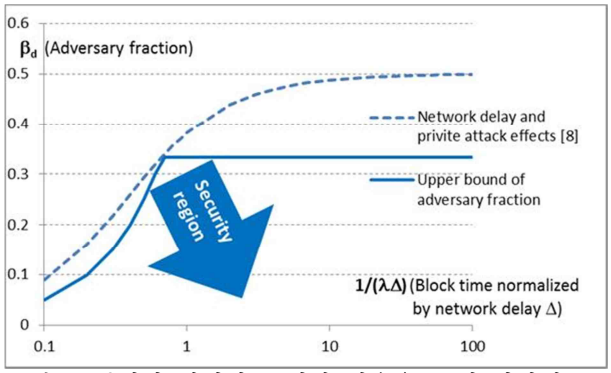

그림 1. 통신망 지연과 공격자 점유율 β_d의 상한선.

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] 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.

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

[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. Gilbert and N. Lynch, "Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web services," SIGACT News, vol. 33, no. 2, pp. 51-59, Jun. 2002.

[6] 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.

[7] S. Sridhar, E. Tas, J. Neu, D. Zindros, and D. Tse, "Consensus Under Adversary Majority Done Right," arXiv:2411.01689v3, 2025.

[8] 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.