지연허용 지불채널(Delay-tolerant Payment Channel)에서 균형 공격(Balance Attack)에 대한 제휴정책의 안전성(Security) 분석

이우용, 김근영, 조동욱°

한국전자통신연구원, 충북도립대학교°

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

Security analysis of Coalition strategy against Balance attack in Delay-tolerant Payment channel

Lee Woo Yong and Kim Keunyoung

Mobile Communication Research Division,
Telecommunication & Media Research Laboratory
Electronics and Telecommunications Research Institute (ETRI) and
Chungbuk Provincial University°

요 약

남극(Antarctica Region)같은 극한 환경에서 탐사하기 위한 장비는 소모전력, 크기와 무게 등이 제한되며 여러 IoT 노드들이 분산되어있는 환경에서 무인 이동 탐사를 위한 조건은 장거리 지연허용 무선통신을 요구한다. 이러한 극한 환경 지연허용 통신 시스템은 노드간 협력과 신뢰성 확보를 위하여 점유하는 이득과 손실을 기록하기 위한 방안으로 분산원장을 고려할 수 있다. 하지만, 분산원장의 신뢰성 확보를 위해 지금까지 가장 많이 연구된 작업증명 기법은 운영이 매우 간단하나 에너지 낭비가 매우 심하다. 이를 극복하기 위한 기술로 지분증명 기법은 에너지 효율적인 대안이다. 본 논문에서는 지분증명 기법에서 안전성 분석을 위하여 부분 Δ-동기화된 분산 시스템 모델을 가정하였고, 이러한 통신망 지연이 시스템에 어떤 영향을 끼칠 수 있는지 분석했다. 본 분석은 개방형 시스템을 부분 Δ-동기 모델의 관점에서 분석했을 때, 균형공격(Balance 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 균형공격에서 공격자 점유율에 따른 안전 영역 상한선 확장 가능성을 조사하는 것이다.

Ⅰ. 서 론

극한지(Extreme Cold Region)에서 탐사를 위하여 사용하는 장비는 소모전력 크기 무게 등이 제한되지만, 다수 IoT 노드들이 분산되어있는 환경에서 시스템 운영을 위한 조건은 장거리 지연허용 고속 통신을 요구한다. 우리는 이러한 극한지 통신시스템에서 노드들의 협력과 신뢰성 확보를 위하여 노드의 통신상태와 신뢰도를 저장하고 기록할 수 있는 채널로 모델링하여 다중 경로 라우팅 체계가 작동할 수 있다고 가정한다.

한편, 게임이론[1]이 분산원장 통신망의 대체 솔루션으로 적용될 수 있다. 이 게임이론은 합리적인 의사 결정자 간의 전략적 상호 작용에 대한 수학적 모델이다[2]. 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[3]. 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[4]. 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 지연허용 지불채널에서 부분 Δ-동기화된 모델에서[5], 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. 균형공격에 대한 제휴정책의 안전영역 상한선 분석

본 논문에서는 통신망 지연이 있고 균형 공격 있는 상황에서 노드들끼리 제휴정책을 사용했을 때 지분증명 기법에 어떤 영향을 끼칠 수 있는지 해석하려고 한다. 이 분석은 부분 Δ-동기 모델의 관점에서 균형공격이 지분증명 합의 기법에 어떤 영향을 끼치고 있는 정도를 분석하는 것이다. 정직한 노드들끼리 제휴를 하여 인접노드의 선호도에 따라 메시지를 지연시키거나 빠르게 보내는 전략을 사용했을 때 블록체인 합의 기법의 안전성의 상한선을 분석하는 것이다.

이러한 균형 (또는 지분 없음) 공격 모델을 분지 확률보행(branching random walks)하는 기계로 가정하면, 체인의 가지에서 총 공격자 블록 수는 시간(time slot) t 에 따라 기하급수적으로 증가한다[7]. 구체적으로 설명하면, 공격자 성장속도를 λ_a 라 할 때, 분지 확률보행 모델은 공격자 성장 속도를 $e\lambda_a$ 로 증폭시킨다. 부분 Δ-동기 모델의 관점에서 공격자 성장속도의 상한선 다음 수식으로 표현될 수 있을 것이다[6].

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

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 정의할 수 있다.

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

여기서 λ_{hf} 는 지연을 감소시킬 노드의 성장속도이고 λ_{h-f} 는 지연을 증가시킬 노드의 성장속도를 말한다. 이때 $\lambda_h = \lambda_h + \lambda_{h-f}$ 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.

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

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

$$e\beta_b < \frac{1-\beta_b}{1+(1-\beta_b)\hat{\Delta}\lambda} \quad (4)$$

위 (4)식에 대한 β_b 의 2 차 방정식에 대한 부등식은 다음 식과 같이 간략히 정리될 수 있다.

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

β_b 의 2 차 방정식의 해는 다음 부등식의 상한 값을 갖는다.

$$0 \leq \beta_b \leq \frac{1}{2} + \frac{e+1}{2e\hat{\Delta}\lambda} - \sqrt{\left(\frac{1}{2}\right)^2 + \frac{e-1}{2e\hat{\Delta}\lambda} + \left(\frac{e+1}{2e\hat{\Delta}\lambda}\right)^2} \quad (5)$$

β_b 를 $\frac{1}{\Delta\lambda}$에 대하여 그래프로 그리면 그림 2 의 실선과 같다. 이 실선 그래프는 참고문헌[7]의 POSpace 모델에 대한 참 안전 문턱 값(True security threshold)과 같다. 한편, 공격자 블록생성 속도는 균형공격의 영향이 배가되어 $e\hat{\Delta}\lambda_a = e\hat{\Delta}\lambda\beta_b < \frac{1}{2}$를 만족해야 하므로(그림 1 의 점선), β_b 의 상한 값은 두 경계의 최소값이므로 다음 수식과 같다.

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

이때 두 상한 값의 교차점은 위 식으로부터 $\frac{1}{\hat{\Delta}\lambda} = \frac{2e}{2e+1}$이고 β_b=1/(2e+ 1)이다.

그림 1 은 통신시스템이 평균지연 Δ 를 유발하는 상황에서 공격자가 균형공격을 시도했을 때 공격자 비율 확대에 대한 안전영역 상한선(적색)을 그린 것이다. 공격자 노드의 공격을 완화시키기 위하여 정직한 노드 사이 제휴를 맺고 메시지 전송에 지연 가감정책에 사용하여 50%(Δ_f=Δ/3, γ=75%) 제어할 수 있는 경우와 33%(Δ_f=Δ/3, λ=50%) 제어할 수 있는 경우에 대하여 분석하였다.

이 분석에서 우리는 실제 공격자 비율이 순수한 공격자 생성속도(λ_a)에 의한 영향보다 통신망 지연과 공격 유형에 따라 크게 확대 재생산됨을 알 수 있다. 이를 극복하기 위한 방안으로 정직한 노드 사이에 제휴를 맺어 지연경감 방안을 적용하면 안전한 영역의 상한선을 확장시킬 수 있다.

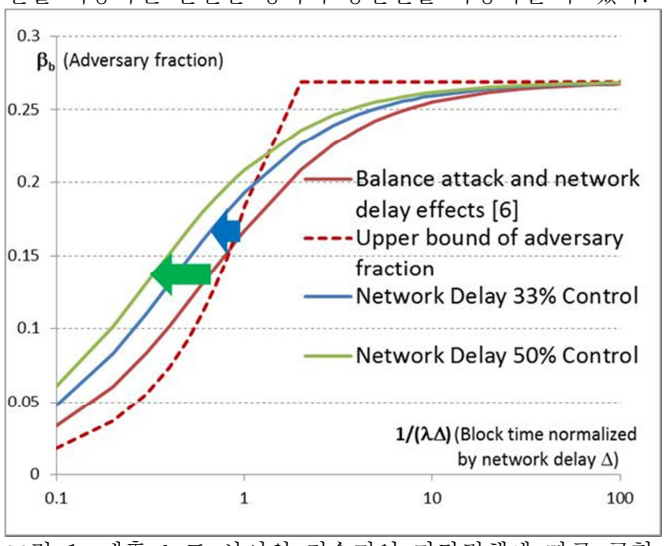

그림 1. 제휴 노드 사이의 전송지연 가감정책에 따른 균형공격자 점유율 β에서 지연경감제어 비율에 따른 안전 영역 상한선 확장 예.

ACKNOWLEDGMENT

본 논문은 2024 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] R. B. Myerson, Game Theory. Cambridge, MA, USA: Harvard Univ. Press, 2013.

[2] 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.

[3] C. Barrera and S. Hurder, "Blockchain upgrade as a coordination game," Prysm Group, Bristol, U.K., Tech. Rep. SSRN 3192208, 2018.

[4] J. Abadi and M. Brunnermeier, "Blockchain economics," MIMEO, New York, NY, USA, Tech. Rep.1254, 2018.

[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.