극한지(Antarctica) 지연 허용(Delay-tolerant) 무선통신 망에서 블록체인 합의 알고리즘 적용을 위한 안전성(Security) 분석에 관한 연구

이우용, 김근영
한국전자통신연구원, 6G 무선방식연구실

{wylee, kykim12}@etri.re.kr

A Study on Security Analysis for Application of Blockchain Consensus Algorithm in Antarctica Delay-tolerant Wireless Communication Network

Lee Woo Yong and Kim Keunyoung

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

요 약

극한지(Extreme Cold Region)와 같이 소모전력, 장비의 크기와 무게 등이 제한되지만 여러 IoET (Internet of Extreme Things)노드들이 분산되어있는 환경에서 무인 탐사를 위한 조건은 장거리 무선통신을 요구한다. 우리는 이러한 극한지 통신망을 지연 허용(Delay tolerant) 무선통신 망으로 모델링하고 다중 경로 라우팅 체계가 작동한다고 가정한다. 분산원장의 신뢰성 확보를 위해 지금까지 가장 많이 연구된 작업증명 블록체인 기법은 매우 간단하지만, 여전히 에너지 낭비가 매우 심하다. 이를 극복하기 위한 비잔틴(Byzantine) 기법은 투표 기반으로 구현되어 서로 경쟁하지 않고 합의에 도달하므로 일반적으로 에너지 소비가 적다. 그들의 주요 단점은 합의에 도달하기 위해 통신 망을 통해 전달되어야 하는 메시지의 수와 참여 노드를 미리 검증해야 하는 비공개 망으로 제한된다. 또 다른 대안으로 지분증명 기법은 에너지 효율적인 대안이다. 우리는 지분증명 기법을 IoET 노드들에 적용하기 위하여 비잔틴 기반 기법의 주요 단점인 통신복잡도도 줄여야 하는 매우 도전적인 문제에 대한 해결 가능성을 분석해 본다. 본 논문에서는 지연 허용 망에 대한 분석을 부분 Δ-동기화된 지분증명 블록체인 모델 기반으로 수행하였다. 본 연구에서는 통신망 지연이 지연 허용 프로토콜에 어떤 영향을 끼칠 수 있는지 분석했다.

Ⅰ. 서 론

극한지(Extreme Cold Region)와 같은 도전적인 환경을 탐사하기 위한 장비는 소모전력, 장비의 크기와 무게 등이 제한되며, 장비(노드)들이 분산되어있는 극한 환경에서 안전하게 무인 탐사 데이터를 모으기 위한 조건 중 하나는 장거리 무선통신이다. 장거리 무선통신망을 통해 센서 망(SN: sensor networks)를 상호 연결하는 남극과 같은 환경에서, 우리는 동토층 연구의 데이터 수집을 자동화하는 극한지 사물 인터넷 원격 측정 서비스 구축을 목표로 한다.

극한지 환경의 통신망은 고정된 센서의 전력소모와 움직이는 무인 자율 로봇의 위치에 다른 열악한 통신환경에 따라 수집해야 할 데이터를 대량으로 전송하기 위하여 DTN(지연 허용 망, Delay tolerant network)의 기회적(opportunistic) 기술을 사용하여 이러한 도전적인 목표 서비스를 제공한다. 이러한 무선 통신망 특성으로 인해 망은 정체(congestion)과 패킷 손실을 발생시킬 수 있다. 우리는 망 정체와 손실 상황에서 이 문제 해결을 위한 방법을 찾기 위한 목표, 신뢰성에 가장 적합한 요구사항을 만족할 수 있는 후보 해결책에 대한 평가와 전송 프로토콜 분석을 요구한다[1].

DTN 개념은 깊은 우주 통신의 심각한 지연과 패킷 오류에 대처할 수 있는 망 기술 관련한 행성간 인터넷 (IPN: interplanetary internet)의 개발을 기반으로 2003년 Fall [2]에 의해 지상 망 환경에 대비하여 DTN 용어를 사용하기 시작했다. DTN의 경우 여러 문제로 발생하는 지연, 끊김, 정체를 대응해야 하기 때문에 기존 지상 망에서 활용되는 규약과 색다른 특징을 지니게끔 개발이 되어왔다[3]. DTN을 위한 프로토콜은 데이터를 망에서 각 노드에 저장하고 다른 노드로 라우팅될 때 전달하게 된다. 이러한 데이터 전송기법을 저장 그리고 전달(store-and-forward)이라고 하는데, DTN에서 핵심이 되는 표준 번들(bundle) 프로토콜의 기반이 된다.

DTN에서 여러 가지 전달 문제도 불구하고 다중 경로로 수집된 동일한 데이터는 모든 노드에서 같은 데이터 값으로 동의(합의)되어야 한다[4]. 이러한 합의 프로토콜은 증명 기반(proof-based) 합의와 비잔틴 합의(동의)의 두 가지 주된 기법으로 분류될 수 있다. 첫 번째 그룹은 모든 참가자가 블록을 채굴하기 위해 서로 경쟁하는 블록체인 기술과 관련이 있으며 가장 일반적으로 사용되는 프로토콜은 작업 증명, 지분 증명, 및 그 변종이다. IoET에 대한 이러한 프로토콜을 적용하는데 주요 단점은 장치가 일반적

으로 하드웨어 자원이 적고 처리 능력이 낮아 블록체인의 채굴 작업을 극도로 어렵게 만든다는 것이다[4]. 반면에 비잔틴 기반 프로토콜은 투표 기반 기법을 구현하여 서로 경쟁하지 않고 합의에 도달하므로 일반적으로 자원 소비가 적다. 그러나 비잔틴 기반 기법의 주요 단점은 합의에 도달하기 위해 망을 통해 전달되어야 하는 메시지의 수가 많다는 것이다. IoET와 같은 극한지 상황에서는 통신 망의 복잡도도 줄여야 하는 도전적인 문제에 직면하게 된다.

이러한 에너지와 통신 낭비를 극복하기 위한 기술로 지분증명 기법은 에너지 효율적인 대안이다. 그러나 그것은 상당히 복잡하고 보안에 보다 취약하고, 순수한 비공개(체인) 공격에 대해서만 보안을 유지하는 것으로 알려져 있다. 본 연구에서는 통신망 지연이 지분증명 프로토콜에 어떤 영향을 끼칠 수 있는지 분석했다. 우리는 부분 Δ-동기화된 모델의 관점에서 분석하려고 시도했고, 복잡한 해석 과정은 생략하고 직관적으로 설명해 보려 했다.

Ⅱ. 지연 허용 망에서 지분증명 합의 적용을 위한 지연 영향에 관한 분석

부분 Δ-동기화된 통신망 환경에서 전체 노드 수를 n 이고 오염된 공격자 수를 f 라 하자. 주어진 시간 간격(time slot)에서 어떤 노드가 하나의 블록을 제안할 확률을 p 라고 하면, 공격자 노드가 참여할 기대 값 β과 정직한 노드의 기대 값 α은 다음 식으로 정의될 수 있다[5].

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

부분 Δ-동기화된 통신망에서 지연을 Δ라고 할 때, 공격자 노드가 참여할 기대 값 β는 다음 조건을 만족해야 안정성을 보장할 수 있다[5].

$$\beta < \alpha(1-2\Delta pn)$$

여기서, 공격자의 공격 유형을 망 지연으로 한정할 수 있고, 지연은 평균 Δ이라고 할때 최대 2Δ가 되다. 이때 (1-2Δpn) > 0 이여야 하므로, Δpn < 0.5 이고, 동시에 블록 제안이 지연된 경우도 오염된 공격으로 판단하게 되므로 2Δpn < 0.5 이다. 위 수식들을 이용하면 공격자 노드와 정직한 노드가 참여할 기대 값의 비율을 구할 수 있다.

$$1-2\Delta pn > \frac{\beta}{\alpha} = \frac{f}{n-f}$$

위 수식에서 2Δpn 의 상한 값은 전체 노드 수와 오염된 공격자(지연) 수의 비율로 표현할 수 있다.

$$2\Delta pn < 1-\frac{f}{n-f} = \frac{n-2f}{n-f}$$

참고문헌[6]의 정리 2, 3 와 일치 한다. 여기서, pn=α+β이고 2Δpn 는 정직한 노드와 공격자 모두 지연되어 들어온 경우로 오염된 것으로 판단한다. 2Δpn<0.5 를 만족해야 한다면 위 수식은 다음 식의 조건을 만족해야 한다.

$$\frac{n-2f}{n-f} > \frac{1}{2}$$

위 수식을 정리하면 n/3 > f 를 만족해야 한다. 이 조건은 비잔틴 기반 합의 알고리즘과, Libra[7] 및 Algorand[8]와 같은 유형의 지분증명 블록체인인 허가형(permissioned) 블록체인의 안전 확보를 위한 가장 중요한 기본 조건이 된다. 이러한 프로토콜에서 이 조건은 모든 활성화된 노드의 2/3 정족수 서명을 만족해야 거래 완료에 대한 보장을 할 수 있으므로 통신망 분할에서 안전성 확보를 위해 매우 중요하다.

우리는 합의 기법에 대한 통신복잡도하고 분석한 결과를 표 1에 나타내었다. 비잔틴 기반 합의 알고리즘은 투표를 기반으로 하게 때문에 모든 노드에게 현 블록에 대한 찬반 여부를 방송하게 되므로, 통신복잡도 상한선은 노드 수 자승에 비례한다[4]. 한편 동형 암호 기반 지분 증명 블록체인 합의 알고리즘에서는 모든 커밋(Commitment)을 부호화하여 각 노드에게 1회 보내게 되고, 커밋을 복호화하여 진위 여부를 판별하기 때문에 통신복잡도 상한선은 노드 수에 비례하게 된다[9].

Schemes and Analysis	Security Resilience	Communication Complexity Upper Bound
Partially Simultaneous Proof of Stake Consensus with Homomorphic Commitment [9]	f < n/3	O(n)
Byzantine Consensus [4]	f < n/3	$O(n^2)$

표 1. 지연 허용 망에서 합의 알고리즘에 대한 안전성 및 통신복잡도 상한선 분석.

ACKNOWLEDGMENT

본 논문은 2022 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] K. Fall, "A delay-tolerant network architecture for challenged internets," in Proc.SIGCOMM'03, pp. 27-34, Aug. 2003.

[3] K. Fall and S. Farrell, “DTN: an architectural retrospective,” IEEE J. Sel. Areas Commun., vol. 26, no. 5, pp. 828-836, Jun. 2008.

[4] 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.

[5] R. Pass and E. Shi, “The sleepy model of consensus,” in International Conference on the Theory and Application of Cryptology and Information Security, pp. 380-409, Springer, 2017.

[6] J. Neu, E. N. Tas, and D. Tse, “Ebb-and-Flow Protocols: A Resolution of the Availability-Finality Dilemma,” in IEEE Symposium on Security and Privacy, pp. 446-465, Sept. 2021.

[7] Libra Association, “Libra white paper,” 2020, https://libra.org/en-US/whitepaper/.

[8] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich, “Algorand: Scaling Byzantine agreements for cryptocurrencies,” in Proceedings of the 26th Symposium on Operating Systems Principles, ACM, pp. 51-68, 2017.

[9] K. Nazirkhanova, J. Neu and D. Tse, “Information Dispersal with Provable Retrievability for Rollups,” May 2022, https://arXiv:2111.12323v3