차량 네트워크 내 블록체인 기반 연합학습 자원 최적화를 위한 점수기반의 블록 검증

전정민° 홍충선*

경희대학교 컴퓨터공학과

{jmjeon0212°, cshong* }@khu.ac.kr

Optimizing Resources in Blockchain-based Federated Learning for Vehicular Networks Using Score-based Block Validation

Jeongmin Jeon°, ChoongSeon Hong*

Department of Computer Science and Engineering, Kyung Hee University

요 약

차량 네트워크는 자율주행, 트래픽 예측 및 지능형 의사결정을 가능하게 하는 인공지능을 적용하고 있다. BFL 프레임워크가 최근 개인 정보 인식 및 효과적인 차량 통신 네트워킹을 위한 분산 연합학습으로 도입되고 있다. 하지만 본 프레임워크는 높은 컴퓨팅 자원을 소비하는 PoW를 사용하는 마이닝 프로세스의 기본 개념을 사용한다. 본 논문에서는 채굴자의 자원을 최적화하기 위해 점수기반 블록 검증을 사용하는 경량 PoW를 제안한다. 차량 소유자의 데이터는 민감한 정보를 최소화하기 위해 연합학습을 적용한 RSU를 고려한다. 기존 PoW 합의 프로토콜과 비교하여 채굴자의 컴퓨팅 자원을 최적화하는 점수기반 블록 검증을 사용하여 경량 PoW가 자원을 최적화하는 것을 확인하였다. 본 논문의 주요 목적은 컴퓨팅 비용이 많이 드는 PoW 합의 프로토콜을 제거하고 통신 관점에서 자원, 신뢰성, 전송 지연 및 프라이버시를 최적화하는 것이다. 마지막으로 차량 네트워크에서 BFL 모델 중독 공격에 대한 관련 향후 연구 방향을 강조한다.

1. 서 론

미래의 무선 네트워크는 언제 어디서나 심지어 이동 중에도 낮은 지연과 초고 신뢰성을 보장할 것으로 예상이 된다. 이는 자율 주행 차량에 대한 실시간 통신 제한을 충족시킬 것이다. 이를 위해 차량에서 on-device Machine Learning이 필요하다. 이는 각 차량이 최상의 학습 모델을 유지할 수 있도록 하여 연결이 끊어졌을 때 올바른 의사결정 솔루션을 가능하게 한다. 이를 위해 각 차량에서 연합학습이 필요하지만 올바른 모델을 학습하려면 인접 차량과 데이터를 공유해야 한다[1][3].

주요 문제 중 하나는 데이터 샘플이 각 차량에 의해 생산이 되고 소유 권한 또한 차량 소유주가 된다는 것이다. 따라서 공유된 데이터와 지식 고윳값은 데이터의 다른 이웃 차량으로부터 비공개로 유지되어야 한다. 연합학습을 사용하게 되면 원시 데이터를 재생할 수 없으므로 [1]에 따르면 Blockchain based Federated Learning(BFL) 모델은 자율주행 차의 우수한 성능과 프라이버시 보존을 위해 블록체인과 연합학습을 결합하여 제안하였다. 전통적인 퍼블릭 블록체인의 합의 알고리즘인 Proof of Work(PoW)를 사용하는 BFL 프레임워크는 중앙 집중식 제어 없이 차량 내 머신러닝을 성공적으로 가능하게 하여 종단 간 시스템 지연에 대한 통찰력을 제공한다. 그러나 [1][2] 자원은 PoW를 사용하여 블록체인의 블록을 생성하고 운영함으로써 자원의 낭비를 일으킨다. 채굴자는 자신의 컴퓨팅 자원을 사용하여 블록을 전파하고 Broadcast 한다. 따라서 자율주행 차량뿐만 아니라 산업 분야에서도 자원이 보존되지 않고 자원과 에너지 효율성이 가장 중요한 문제 중 하나이다. 본 논문에서는 고가의 PoW 방식을 계산하여 채굴을 제거하고 자원을 최적화하는 점수기반의 블록 검증 메커니즘을 제안한다.

이 논문은 2020년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2019-0-01287, 분산 엣지를 위한 진화형 딥러닝 모델생성 플랫폼). *Dr. CS Hong is the corresponding author.

2. 관련연구

2.1 합의 매커니즘

합의 프로토콜은 구조 및 계산 및 통신 요구 사항 측면에서 블록체인의 가장 중요한 부분을 구성한다. 작업증명 (PoW) 프로토콜은 V2V 및 V2I 블록체인에 적용되고 있다 [4] [5]. 기존 퍼블릭 블록체인 네트워크는 PoW 메커니즘을 기반으로 개발되었습니다. 기본적으로 PoW 기반 블록체인 네트워크의 노드는 각 노드가 제안된 새 블록에 대한 nonce 값을 찾아야 하는 솔루션 검색 프로세스에 참여하여 합의에 도달한다. nonce, 이전 블록 해시 및 블록과의 트랜잭션이 해시 함수에 대한 입력으로 사용되는 경우 (예 : SHA-256) 해시 함수 출력은 블록이 허용될 수 있도록 목표 범위 내에 있어야 한다. 해시 함수의 속성으로 nonce는 출력 대상 범위 [6]

내에 있을 때까지 다른 nonce 값에서 반복적인 시도를 통해서만 찾을 수 있다.

참가자가 nonce 값을 찾으면 트랜잭션과 함께 블록을 다른 노드로 Broadcast 한다. 다음으로 새 블록이 확인되고 체인의 마지막 블록 이후로 채굴된 첫 번째 블록으로 결정된다. 현재 체인이 통합되어 체인의 최신 블록이 된다. PoW에서 참가자는 거래를 통해 블록을 다른 노드에 Broadcast 하는 최초의 채굴자가 되기 위해 서로 경쟁하는 메커니즘이다. 그리고 참가자들은 먼저 올바른 임시값을 찾기 위해 경쟁한다. 참가자가 참가자 네트워크에서 우승자로 선정될 확률은 다음과 같다.

$$p_i = \frac{c_i}{\sum_{j=1}^{K} c_j} \quad \cdots\cdots\cdots\cdots ①$$

c_j가 참가자의 해시 비율 i인 경우, ① 은 PoW 합의 메커니즘을 사용하여 해시 비율을 증가시켜 참가자가 리더가 될 가능성을 높이는 블록체인에 많은 양의 에너지 소비로 이어진다. 하지만 리더는 이더리움과 같은 보상을 받고 있다[6]. 이는 이 메커니즘에 계산 비용이 많이 드는 문제가 있음을 의미한다.

2.2 연합 학습에서 블록 체인의 역할

Google의 Federated Learning (GFL)의 한계를 해결하기 위해 [9] [10] [11]는 GFL의 중앙 서버를 제거하고 블록 체인을 적용하고 BFL 접근 방식을 제안하는 블록체인을 활용했다. 네트워크 시스템은 보상을 제공하고 확인하면서 차량에서 로컬 모델 업데이트를 보낼 수 있다.

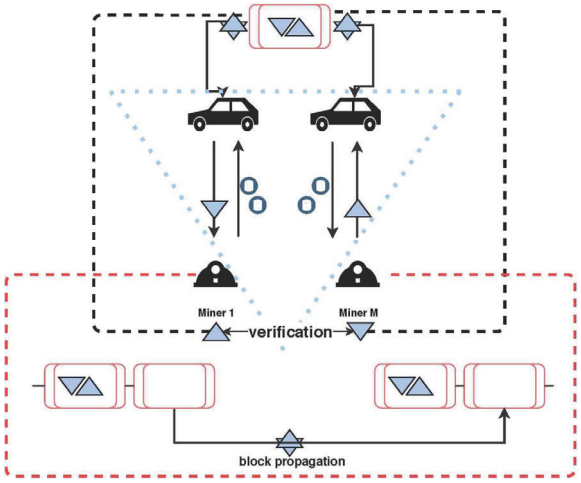

그림 1. A blockchain-based federated Learning approach for vehicular network[1].

그림 1은 채굴자가 비교적 계산적으로 강력한 채굴 프로세스인 네트워크 에지 (WiFi 액세스 포인트 또는 기지국)에서 이동 차량 또는 노드일 수 있음을 보여준다. 모든 채굴자는 상호 작용하고 모든 로컬 모델 업데이트를 확인한 다음 작업 증명을 실행한다. 채굴자가 합의를 완료하면 검증된 로컬 모델 업데이트를 기록하여 새 블록을 생성한다. 기존 작업에서 문제는 블록체인 시스템의 PoW에 통신 및 계산 지연이 있다는 점입니다 [1]. 본 논문에서는 점수기반 블록검증인 새로운 블록 검증 메커니즘을 제안한다.

3. 제안 사항

3.1 시스템 모델

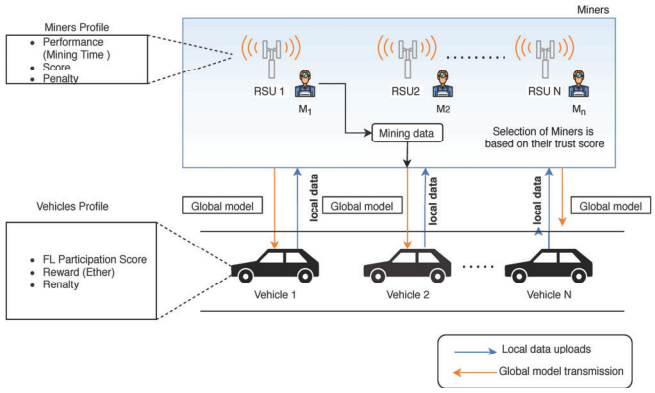

그림 2. BFL approach based on proposed scheme

본 논문에서는 차량과 Road Side Unit(RSU)가 포함된 [1]에서 제안한 BFL 프레임워크를 고려한다. 각 차량 소유자는 자신의 데이터를 소유하고 자체적으로 센서 데이터 또는 모델 업데이트를 생성한다. 우리는 그것을 공유할 의사가 있다고 가정한다.

[11]은 블록체인 기술을 위한 엣지 컴퓨팅 영역을 도입하였다. 이는 계산 비용이 많이 드는 PoW를 엣지 노드로 오프로드하여 채굴 차량으로 블록을 채굴함으로써 블록 생성 지연을 줄일 수 있다. 또한 자율주행 차량의 에지 클라우드 컴퓨팅을 사용하여 블록 전파 지연을 줄일 수 있다 [12].

그림 2에서 볼 수 있듯이 N 차량은 RSU와 같은 자체 로컬 데이터를 에지로 보내고 연관 학습에 직접 참여하는 차량에 대한 보상으로 이더리움를 제공한다. 대부분의 채굴은 RSU에 의해 처리되어 더 빠른 블록 전파가 가능하며, 본 논문에서 제안한 점수 기반 블록 검증 메커니즘은 채굴 개념을 제거한다. 각각의 N개의 RSU와 차량에는 프로필이 있으며 성능, 즉 채굴 시간에 따라 점수와 패널티가 할당된다. RSU는 각각의 점수를 기반으로 블록을 확인 및 전파하고 Boradcast하고 블록을 기록 할 수 있다.

Algorithm 1. the workflow of the proposed scheme

1) At time t, suppose there are 4 miners. Initially, all miners are assigned a minimum score of 100.
2) Then two miners are selected randomly, say M1 and M4. To enforce justice and fairness, the selected miners will not be selected in the subsequent round.
3)The selected miners will compete to determine their performance based on their mining time. If M4 is the winner then M4 will get an increment of 50 to its initial score.
4) If the mining time can not be performed within the defined threshold then the miner gets a penalty.
5) Then, at time t+1 suppose M2 and M3 are selected.
6) compete with two miners. which miner is good performance (mining time). M2 is the winner, and the M2 gets 50 more scores.
7) After t+2, all of the miners get their own score and penalty.

8) If the miner gets 400 more scores. then their score is reset. and broadcast as usual block recording.
9) The participating vehicles get an incentive as ether to motivate them for joining the FL model updates.

4. 성능평가

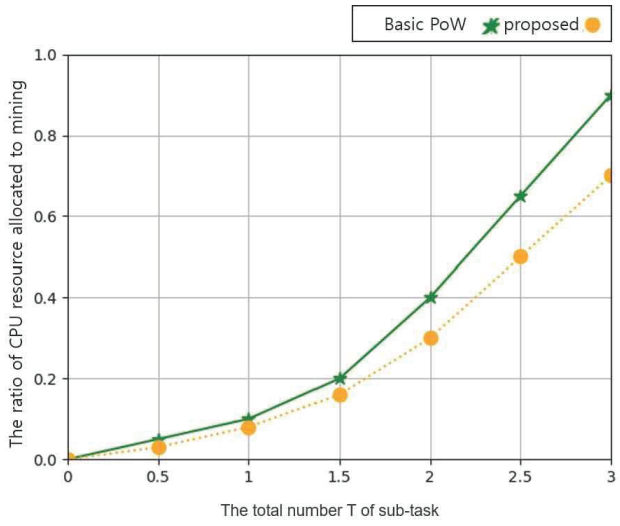

그림 3 The number of computing tasks T original PoW versus the utility our proposed mechanism

본 섹션에서는 제안된 점수기반 블록 검증의 전반적인 성능을 평가하고 서로 다른 합의 하에 시스템의 전체 채굴 시간에 대한 중요한 통찰력을 얻는다. 평가에 사용되는 네트워크 설정 및 매개 변수는 기본 PoW 및 사양을 기반으로 한다. 또한 그림 3은 기존 PoW의 컴퓨팅 작업 수와 제안된 메커니즘의 유용성을 보여준다. 그래프는 제안된 방식이 기본 PoW보다 적은 자원를 소비함을 보여준다.

5. 결론 및 향후 연구

본 논문에서는 BFL 프레임워크에서 계산 비용이 많이 드는 PoW 마이닝 프로세스를 제거한다. 점수 기반 블록 유효성 검사를 사용하여 채굴 자원을 보존하고 엣지 노드에서 FL을 수행하여 개인 정보 노출을 최소화하는 것을 보인다. 참가자는 차량의 CPU를 통해 FL에 참여하는 보상으로 이더리움을 제공함으로써 동기를 부여할 수 있다. 마지막으로 향후 작업에서는 모델의 중독공격을 제거하기 위한 연구에 대한 통찰력을 제공한다.

6. 참고문헌

[1] S. R. Pokhrel and J. Choi, “Federated Learning With Blockchain for Autonomous Vehicles: Analysis and Design Challenges,“ in IEEE Transactions on Communications, vol. 68, no. 8, pp. 4734-4746, Aug. 2020, doi: 10.1109/TCOMM.2020.2990686.

[2] Pokhrel, S.R. and Choi, J., 2020, April. A decentralized federated learning approach for connected autonomous vehicles. In 2020 IEEE Wireless Communications and Networking Conference Workshops (WCNCW) (pp. 1-6). IEEE.

[3] S. Niknam, H. S. Dhillon and J. H. Reed, “Federated Learning for Wireless Communications: Motivation, Opportunities, and Challenges,“ in IEEE Communications Magazine, vol. 58, no. 6, pp. 46-51, June 2020, doi: 10.1109/MCOM.001.1900461.

[4] J. Kang et al., “Blockchain for secure and efficient data sharing in vehicular edge computing and networks,” IEEE Internet Things J., vol. 6, no. 3, pp. 4660-4670, Jun. 2019.

[5] M. Liu, F. R. Yu, Y. Teng, V. C. M. Leung, and M. Song, “Computation offloading and content caching in wireless blockchain networks with mobile edge computing,” IEEE Trans. Veh. Technol., vol. 67, no. 11, pp. 11 008-11 021, Nov. 2018.

[6] Blockchain. Hashrate Distribution and Estimation of Hashrate Distribution Amongst the Largest Mining Pools. Accessed: Nov. 3, 2018. [Online].Available: https://www.blockchain.com/pools/

[7] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim, ‘A survey on consensus mechanisms and mining strategy management in blockchain networks,’ IEEE Access, vol. 7,pp. 22328-22370, 2018.

[8] S. Wang, T. Tuor, T. Salonidis, K. K. Leung, C. Makaya, T. He, and K. Chan, “Adaptive federated learning in resource constrained edge computing systems,” IEEE Journal on Selected Areas in Communications, vol. 37, no. 6, pp. 1205-1221, 2019.

[9] C. Decker and R. Wattenhofer, “Information propagation in the bitcoin network,” in IEEE P2P 2013 Proceedings. IEEE, 2013, pp. 1-10.

[10] H. Kim, J. Park, M. Bennis, and S.-L. Kim, “Blockchained on-device federated learning,” IEEE Communications Letters, 2019.

[11] I. Eyal and E. G. Sirer, “Majority is not enough: Bitcoin mining is vulnerable,” Communications of the ACM, vol. 61, no. 7, pp. 95-102, 2018.

[12] Shrestha, R., Bajracharya, R., Shrestha, A.P. and Nam, S.Y., 2020. A new type of blockchain for secure message exchange in VANET. Digital communications and networks, 6(2), pp.177-186.