데이터 프라이버시 및 성능을 개선한 P2P 연합학습 프레임워크

김영애, 허가빈, 도인실*
이화여자대학교*
youngae@ewhain.net, gjrkqls@ewhain.net, *isdoh1@ewha.ac.kr

Peer to Peer Federated Learning Framework for Enhanced Data Privacy and Performance

Youngae Kim, Gabin Heo, Inshil Doh*
Ewha Womans University

요 약

최근 인공지능 기술이 크게 발전하면서 데이터를 통한 학습 과정에서 발생하는 개인정보 노출 문제를 개선하는 방법으로 연합학습(Federated Learning)이 제안되고 이를 기반으로 다양한 연구가 이루어지고 있다. 연합학습은 분산방식으로 학습을 진행함으로써 개인의 정보를 보호할 수 있으나 중앙서버에 클라이언트가 연결된 방식의 기본 구조는 중앙서버에 크게 의존하여 단일 장애 지점 문제가 있고 확장성이 떨어진다는 문제가 존재한다. 이를 보완하는 방안으로 P2P 기반의 연합학습에 관한 연구가 제안되었으나 여전히 효율성의 문제를 갖는다. 본 연구에서는 개선된 P2P 연합학습 프레임워크로 P2P 네트워크 내에서의 통신량을 줄이고 보다 효과적으로 연합학습을 진행할 수 있도록 하는 방안을 제시한다.

Ⅰ. 서 론

인공지능이 상용화되면서 인공지능의 학습에 사용되는 데이터를 수집하는 과정에서 발생하는 개인정보 침해에 대한 문제가 대두되고 있다. 이 문제를 해결하기 위해 연합학습(Federated Learning)이 제안되었다. 연합학습은 분산형 학습 기법으로 다양한 기기와 기관이 분산된 데이터를 직접 공유하지 않고 협력하여 인공지능 모델을 학습한다.

연합학습의 기본적인 구조는 중앙서버에 클라이언트가 연결된 구조이다. 각 클라이언트는 자신이 학습한 결과, 즉 로컬 업데이트를 중앙서버로 전송하고, 중앙서버는 이를 통합하여 글로벌 모델을 수정 및 배포한다. 그러나 이 방식은 중앙서버에 과도하게 의존하며, 중앙서버에 문제가 발생할 경우 단일 장애 지점(Single Point of Failure) 문제와 확장성 부족 문제가 있다[1]. 이러한 문제들을 해결하기 위해 탈중앙화(Decentralized) 방식의 연합학습에 관한 연구가 진행되고 있다[2]. 중앙서버를 없애고 클라이언트끼리 연결되는 P2P(Peer-to-Peer) 방식을 연합학습에도 적용하여 중앙서버로 인해 발생하는 문제를 해결할 수 있다. P2P 연합학습은 특히 개인정보 보호가 중요한 의료 현장과 같은 환경에서 중요한 역할을 한다.

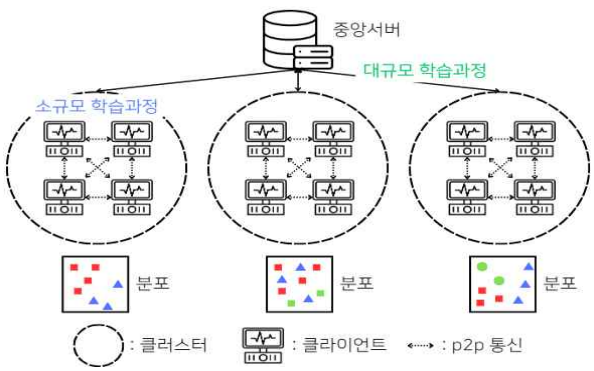
본 연구에서는 더욱 효과적인 학습을 위한 P2P 연합학습 프레임워크를 제안한다. 각 클라이언트는 메디컬 센터로 가정한다. 메디컬 센터는 일반 IoT 장치와 달리 충분한 컴퓨팅 능력과 통신 인프라를 갖추었으므로 각자 학습을 한 후 P2P 통신을 통해 충분히 다른 클라이언트와 학습 결과를 결합할 수 있다.

Ⅱ. 관련 연구

최근 P2P 환경에서 연합학습을 하는 연구들이 많이 진행되었다. [3]의 연구에서는 의료 현장을 위해 P2P 탈중앙화 방식의 연합학습 프레임워크 BrainTorrent를 제안하였다. 해당 프레임워크는 중앙서버를 없애고 메디컬 센터끼리 직접 연결되어 학습을 진행한다. BrainTorrent 방식은 중앙서버에 의존하는 기존 방식의 문제점을 보완하고 풀링된 데이터로 학습된 모델과 비슷한 성능을 보이지만, 한 클라이언트가 다른 클라이언트의 최신 업데이트 가중치를 받으면 무조건 업데이트하면서 발생하는 단점을 갖는다. [4]의 연구에서는 이러한 BrainTorrent의 학습 알고리즘을 두 가중치를 비교한 후 업데이트하는 것으로 개선하였다. 하지만 중앙서버 방식보다 성능이 낮다는 단점이 있고 가중치를 비교하면서 오버헤드가 발생할 수 있다. [5]의 연구에서는 P2P 네트워크에서 통신량이 많은 문제를 해결하기 위해 통신 효율적인 Score-and-Model 기반 연합학습 알고리즘 FedSnM을 제안하였다. Push 과정에서 Score를 주변 클라이언트에게 전달하고, 필요한 경우에 Model을 전달받는 방식이다. P2P 네트워크 환경에서 기존보다 적은 통신량으로 학습이 가능하다는 장점이 있지만 한 클라이언트씩 업데이트를 진행하기 때문에 모든 클라이언트가 Best Model로 수렴하기까지 학습 과정을 반복해야 한다는 단점이 있다.

Ⅲ. 본론

본 연구에서는 P2P 네트워크 환경에서 효율적인 클러스터링을 통해 통신량을 줄이고 보다 효과적으로 연합학습을 진행할 수 있도록 하는 방안을 제시하고자 한다. 제안하는 시스템은 [그림1]과 같은 구조를 갖는다.



[그림 1] 제안 시스템의 전체 구조

(1) 단계별 프로세스

A. 클라이언트 간 클러스터 형성

a. 실루엣 분석을 기반으로 실루엣 계수가 0.5 이상인 K값들을 범위로 설정한다.

b. 설정된 K값 중 가장 큰 값으로 K-means 클러스터링을 진행한다.

B. 클러스터 내 소규모 학습 진행

a. 클라이언트 C1이 나머지 클라이언트에게 accuracy score를 요청한다.

b. 나머지 클라이언트들은 자신의 accuracy score를 전송한다.

c. C1이 클러스터 내의 모든 클라이언트의 accuracy score를 비교한다.

(i) C1의 accuracy score가 가장 좋을 경우, C1의 모델을 모든 클라이언트에게 전송한다.

(ii) 다른 클라이언트의 accuracy score가 더 좋을 경우, accuracy score가 가장 높은 클라이언트에게 모델을 요청하고 해당 클라이언트가 모든 클라이언트에게 자기 모델을 전송할 수 있도록 한다.

d. K값을 감소시킨 후 K-means 클러스터링을 하고 a부터 c의 과정을 진행한다.

e. 최적의 K값이 될 때까지 a부터 d의 과정을 반복한다.

C. 클러스터 간 대규모 학습 진행

a. 각 클러스터에서 best model과 데이터 샘플을 중앙서버로 전송한다.

b. 중앙서버에서는 여러 클러스터의 결과를 기반으로 global model을 수정한다.

c. 중앙서버가 수정된 global model을 배포하면 이를 받은 클라이언트는 각자 자신이 가진 데이터 샘플로 모델을 검증하여 중앙서버가 배포한 모델이 좋은 경우 자신의 모델을 업데이트한다.

(2) 프로세스별 고려사항

A. 클러스터링 과정

실루엣 분석은 각 데이터 포인트가 속한 클러스터 내부의 밀도와 다른 클러스터와의 거리를 비교하여 군집화의 적합성을 평가하는 방법이다. 이를 통해 클러스터의 일관성을 측정하고 최적의 K값을 찾는다. 실루엣 계수의 값이 0.5 이상이면 optimal 하다고 판단하여 본 연구에서는 실루엣 점수 0.5 이상을 가지는 K값 범위를 활용한다[6].

B. 소규모 학습 과정

비슷한 데이터셋의 클라이언트끼리 클러스터링하여 accuracy score를 비교할 수 있게 하였다. 가중치 대신에 score를 사용하여 각 클라이언트의 로컬 학습 결과를 직관적으로 비교할 수 있다.

C1의 역할은 모든 노드가 순서를 정해 돌아가면서 수행한다. 한 클라이언트씩 요청을 보내고 업데이트를 하며 모든 클라이언트가 best model로 수렴하길 기다리는 것이 아니므로 통신량이 줄어들고 시간이 단축될 수 있다. 요청을 보내는 노드의 순서가 정해져 있으므로 악의적인 클라이언트의 무분별한 요청으로 학습을 방해하기 어렵다는 장점이 있다.

B-e번 과정에서 클러스터의 수를 점진적으로 줄임으로써 더 다양한 데이터 분포를 포함하는 학습 결과를 얻을 수 있으며, 이는 시스템 전체의 성능 향상에 기여한다. 특히, 중앙서버에 문제가 발생하는 경우 P2P 학습은 중단 없이 계속되면서 중요한 역할을 하게 되므로, 이 과정을 통해 P2P 학습의 효과성을 높이는 것이 중요하다. 이렇게 클러스터 내의 데이터 다양성과 신뢰성을 증진하는 것은 결국 전체 네트워크의 학습 퍼포먼스 향상을 돕는다.

C. 대규모 학습 과정

효과적으로 accuracy score를 비교하기 위해 비슷한 데이터셋의 클라이언트끼리 클러스터링하였지만, 이 경우 과적합(Overfit) 문제가 발생할 수 있다. 또한, 데이터 분포가 다양한 시스템 환경에서는 클러스터 개수가 많아지기 쉽다. 제안하는 구조는 중앙서버가 여러 클러스터를 종합하여 과적합 문제를 방지하고 학습 다양성을 보장할 수 있다.

또한, 중앙서버에 문제가 생기면 학습이 중단되는 기존의 연합학습과 달리 제안하는 구조는 클러스터 내에서 P2P 방식으로 학습을 계속 이어 나갈 수 있다. 중앙서버가 오염된 모델을 배포하더라도 C-c의 과정으로 중앙서버의 모델을 검증하기 때문에 영향을 받지 않는다. 이에 더해, 정상적으로 학습이 진행된 각 클러스터의 학습 결과가 중앙서버로 전송되면서 오염되었던 중앙서버가 회복될 가능성을 기대할 수 있다.

Ⅲ. 결론

본 연구에서는 개인정보를 중시하는 의료 현장에 적용할 수 있는 개선된 P2P 연합학습 프레임워크를 제안하였다. 제안된 기술을 사용하여 P2P 네트워크 내에서의 통신량을 줄이고 보다 효과적으로 연합학습을 진행할 수 있다. 중앙서버 구조를 통해 P2P 단독 구조보다 성능을 향상할 수 있고 중앙화 구조에서 발생하는 문제를 개선할 수 있다.

컴퓨팅 파워가 약한 IoT 디바이스의 경우 클러스터 내에서의 학습이 오버헤드를 발생시킬 수 있으므로 향후 연구에서는 계산 오버헤드를 줄여 더욱 효율적인 P2P 연합학습이 가능하도록 제안 기법을 개선하고자 한다.

ACKNOWLEDGMENT

이 논문은 2023년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2023R1A2C1005712) (교신저자: 도인실)

참 고 문 헌

[1] Zhang, C., Xie, Y., Bai, H., Yu, B., Li, W., & Gao, Y. (2021). “A survey on federated learning,” *Knowledge-Based Systems*, 216, 106775.

[2] Li, Y., Chen, C., Liu, N., Huang, H., Zheng, Z., & Yan, Q. (2020). “A blockchain-based decentralized federated learning framework with committee consensus,” *IEEE Network,* 35(1), 234-241.

[3] Roy, A. G., Siddiqui, S., Pölsterl, S., Navab, N., & Wachinger, C. (2019). “Braintorrent: A peer-to-peer environment for decentralized federated learning,” *arXiv preprint arXiv:1905.06731.*

[4] Du, H., Thudumu, S., Singh, S., Barnett, S., Logothetis, I., Vasa, R., & Mouzakis, K. (2023, January). “Decentralized Federated Learning Strategy with Image Classification using ResNet Architecture,” In *2023 IEEE 20th Consumer Communications & Networking Conference (CCNC)* (pp. 706-707). IEEE.

[5] 박성환, & 이재우. (2023). “FedSnM: P2P 네트워크에서 효율적인 통신을 위한 Score-and-Model 방식을 활용한 연합학습,” *Journal of the Korea Institute of Information & Communication Engineering,* 27(2).

[6] Supandi, A., “Saefuddin, A., & Sulvianti, I. D. (2021). Two step cluster application to classify villages in Kabupaten Madiun based on village potential data,” *Xplore: Journal of Statistics*, 10(1), 12-26.