

Learning Agent를 활용한 연합학습 수행 기법 연구

김현배, 이채은, 이주형, 이웅희

한성대학교

{gusqo14, rjh2436, wngud1798, whlee}@hansung.ac.kr

A Study on Conducting Federated Learning using Learning Agent

Hyunbae Kim, Chae-Eun Lee, Juhyung Lee, Woonghee Lee

Hansung University

요약

오늘날 다양한 스마트 기기 및 IoT와 같은 IT 기술의 발전으로 개인이 여러 대의 개별 기기를 보유하게 되었고 이를 활용하여 분산된 개별 기기에서 독립적으로 생산, 수집 및 저장되는 데이터를 활용한 연합학습이 등장하였다. 그러나 일반적인 연합학습은 참여기기 주변의 가용 유휴 기기를 사용하지 않으므로 더 높은 컴퓨팅 성능을 보유한 유휴 기기가 존재하는 상황에서도 이러한 기기들을 연합학습에 적절히 활용하지 못한다는 한계가 존재한다. 따라서 본 논문에서는 주변 가용 유휴 기기를 Learning Agent로 활용하는 기법을 제안하고 Learning Agent에 학습 task를 할당하는 시점을 결정하는 알고리즘을 고안하였다.

I. 서론

오늘날 많은 사람들은 스마트폰을 비롯하여 태블릿, 웨어러블 기기 등 다양한 기기를 사용하고 있다. 그러나 기존의 연합학습 시스템에서는 이러한 유휴 기기를 적절히 활용하지 않고 있다. 연합학습에 참여하는 클라이언트 기기 주변에 클라이언트보다 성능이 뛰어난 CPU 또는 GPU를 탑재한 유휴기기를 활용해 클라이언트 대신 로컬학습을 진행한다면 보다 빠른 연합학습이 가능하다. 그에 따라, 본 논문에서는 Learning Agent 개념을 제안한다. Learning Agent는 연합학습에 참여하는 클라이언트의 주변에 위치하며 클라이언트보다 좋은 연산성능을 가지고 있어서 클라이언트를 대신하여 학습을 수행하는 기기를 의미한다. Learning Agent를 통해 학습을 할 경우, 연합학습의 전체 소요 시간을 단축하는 효과를 얻을 수 있다. 비슷한 개념으로는 단일 조직의 IT 서비스를 제공해주는 Cloud인 'Private Cloud'가 있다[1]. 하지만 엣지 클라우드 등을 활용하는 기존 방식과는 달리, 무선 기기 사용자 소유의 유휴 장치들을 활용함으로써 프라이버시 보호라는 연합학습의 가장 중요한 장점 또한 그대로 가지게 된다. 이에 본 논문에서는 Learning Agent를 고려한 연합학습 기법을 제안한다.

II. 연합학습

연합학습이란 하나 이상의 클라이언트 학습 작업이 중앙 서버에 의해 조정되고 클라이언트는 서버에서 유지 관리되는 글로벌 모델에 대한 업데이트를 제공하는 기술을 의미한다. 그림 1은 기존의 연합학습 개념도를 보여준다. ① 중앙 서버에서 초기 학습 모델을 클라이언트에게 배포하고 ② 각 클라이언트에서는 로컬 데이터를 바탕으로 모델을 학습하고 ③ 업데이트한다[2]. ④ 이후 업데이트 된 학습 모델을 중앙 서버에서 취합하고 ⑤ 서버 모델을 업데이트한다. 연합학습을 활용할 경우, 분산되어있는 독립적인 데이터들을 활용한 학습이 가능해질 뿐 아니라 프라이버시 보호와 보안을 향상시킬 수 있다는 장점이 존재한다[3].

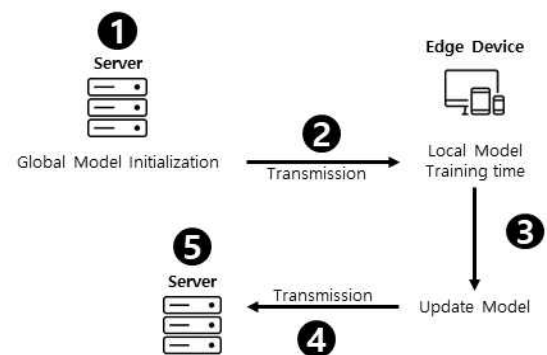


그림 1. 기존 연합학습 개념도

III. Learning Agent 활용 연합학습 기법

1. 제안 기법

그림 2는 Learning Agent를 활용한 연합학습 기법의 흐름을 보여준다. ① 먼저 서버가 글로벌 모델을 초기화한다. ② 이후 Edge Device로 글로벌 모델을 전송한다(Server to Edge Device). ③ Edge Device는 주변의 유휴 기기를 탐색하여 Learning Agent로 사용할 기기를 찾고, ④ Learning Agent가 존재할 경우 학습 데이터와 글로벌 모델을 전송한다(Edge Device to Learning Agent). ⑤ Learning Agent는 로컬 학습 및 모델 업데이트를 수행하고, ⑥ 업데이트 된 모델을 Edge Device로 전송한다(Learning Agent to Edge Device). 이후 ⑦ Edge Device는 Learning Agent에서 받은 모델을 서버로 전송한다(Edge Device to Server). ⑧ 서버는 전송받은 모델들을 집계하여 글로벌 모델을 업데이트하며 한 라운드를 마무리한다. ⑨ 과정 ①~⑧을 정해놓은 round만큼 반복적으로 수행한다. 이때 그림 2에서 설명된 과정에 필요한 학습시간 및 전송시간 만큼의 시간이 소요된다.

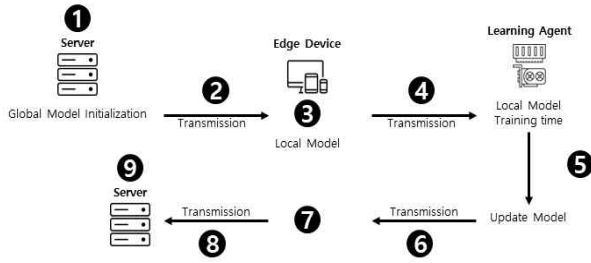


그림 2. Learning Agent를 활용한 연합학습 기법

2. Learning Agent 활용 판단 알고리즘

제안한 기법은 다음 과정을 거쳐 학습을 수행한다. 첫 번째로 Learning Agent의 유무를 확인하는 ‘Checking the users’ idle devices’를 통해 Edge device 사용자의 소유 기기이며, Edge device 보다 뛰어난 computing power를 가지는, 네트워크 상태가 원활하고, 학습이 가능한 유휴상태에 있는 Learning Agent를 찾는다. 두 번째로 ‘Select Training Device’ 과정을 수행한다.

기호	정의	기호	정의
M	모델 크기	R_{tr}^{LA}	1초에 LA가 전송할 수 있는 데이터 크기
D_t	학습 데이터셋 크기	R_t^{LA}	1초에 LA가 처리할 수 있는 연산량
W_t	학습 데이터셋 연산량	D_t^{LA}	LA가 학습에 사용할 학습데이터의 양
p	데이터 전송 성공 확률	T_{LA}	LA가 남은 학습데이터를 연산하는데 소모되는 시간
R_{tr}^E	1초에 Edge가 전송할 수 있는 데이터 크기	T_{rq}	수신 버퍼에서의 큐잉 지연시간
R_t^E	1초에 Edge가 처리할 수 있는 연산량	T_{sq}	송신 버퍼에서의 큐잉 지연시간
T_E	Edge가 학습데이터를 연산하는데 소모되는 시간	T_t	Edge가 남은 학습데이터와 모델을 전송하는데 소모되는 시간
U_{device}	참여기기의 지연시간 상한선	X	Edge의 연산 비율

표 1 수식에 사용된 기호 및 정의

먼저 일반적인 연합학습인 Edge device에서 학습하는 경우의 소요 시간은 수식 (1)과 같이 Training time과 Transmission delay(from Edge device to Server)를 합쳐 계산된다.

$$\frac{W_t}{R_t^E} + \frac{M}{R_{tr}^E} \times \frac{1}{p} \quad (1)$$

본 논문에서 제안된 기법을 활용하여 Learning Agent에서 학습을 수행하는 경우는 학습된 결과를 Learning Agent가 바로 서버에게 보내는 경우와 Edge device를 거쳐 보내는 경우로 나눌 수 있다.

먼저 수식 (2)와 같이 Learning Agent에서 학습 후 바로 서버로

전송하는 경우에는 Transmission delay(from Edge device to Learning Agent)와 Training Time, Transmission delay(from Learning Agent to Server)를 합쳐 소요시간을 계산한다.

$$\left(\frac{D_t + M}{R_{tr}^E} + T_{sq} + T_{rq} \right) \times \frac{1}{p} + \frac{W_t}{R_t^{LA}} + \frac{M}{R_{tr}^{LA}} \times \frac{1}{p} \quad (2)$$

Learning Agent에서 학습 후 Edge device를 거쳐 전송할 때의 소요시간은 수식 (3)과 같이 Transmission delay(from Edge device to Learning Agent)에 Training Time과 Transmission delay(from Learning Agent to Edge device, from Edge device to Server)를 합쳐 계산한다.

$$\left(\frac{D_t + M}{R_{tr}^E} + T_{sq} + T_{rq} \right) \times \frac{1}{p} + \frac{W_t}{R_t^{LA}} + \frac{M}{R_{tr}^{LA}} \times \frac{1}{p} + \frac{M}{R_{tr}^E} \times \frac{1}{p} \quad (3)$$

수식 (1)~(3)을 바탕으로 Edge device에서 학습을 수행할지 아니면 Learning Agent에서 학습을 수행할지 결정하는 알고리즘은 수식 (4)와 같다. A는 Edge device에서 학습하는 경우의 소요시간, 즉 일반적인 연합학습의 소요시간을 나타내며, B는 Learning Agent에서 학습하는 경우의 소요시간을 나타낸다. 즉, Edge device는 A와 B를 예상하여 A가 더 짧을 경우 Edge device에서 학습을 수행하며, B가 더 짧을 경우 Learning Agent를 활용하여 학습을 수행한다.

$$Localtraining = \begin{cases} A, & A < B \\ B, & A > B \end{cases} \quad (4)$$

and $Localtraining \leq U_{device}$

IV. 결론

본 논문에서는 기존 연합학습이 다양한 주변 유휴기기를 활용하지 않는 한계점을 해결하기 위해 Learning Agent를 활용한 연합학습 기법을 제안하였다. 그 과정에서 다양한 상황을 종합적으로 고려하여 Learning Agent의 활용을 판단하는 알고리즘을 제안하였다. 향후에는 본 논문에서 제안한 알고리즘으로 바탕으로 다양한 시뮬레이션 및 실제 디바이스를 이용한 테스트베드를 구축하여 실험 및 평가를 진행할 계획이다.

ACKNOWLEDGMENT

이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. 2021R1G1A1092939).

참 고 문 헌

- [1] A. Finn, H. Vredevort, P. Lowndes & D. Flynn.(2012). Microsoft private cloud computing. John Wiley & Sons.
- [2] Li, Tian, et al. "Federated learning: Challenges, methods, and future directions." IEEE Signal Processing Magazine 37.3 2020
- [3] McMahan, Brendan, et al. "Communication-efficient learning of deep networks from decentralized data." Artificial intelligence and statistics. PMLR, 2017.