# 개인화 연합 학습을 위한 부분 공유 방안에 따른 성능 비교에 관한 연구

김미르, 권민혜*
숭실대학교

48rlaalfm@soongsil.ac.kr, *minhae@ssu.ac.kr

# Performance Analysis of Partial-share Solution for Personalized Federated Learning

Miru Kin, Minhae Kwon*
Soongsil University

요 약

연합 학습 상황에서, 학습에 참여하는 단말 기기의 데이터가 각각 개별적인 특성을 가질 경우 개인화된 모델을 생성하기 위한 개인화 연합 학습(Personalized Federated Learning) 방법이 필요하다. 이를 위해 모델 정보의 일부만을 공유하는 부분 공유 연합 학습방법이 제안되었다. 이러한 부분 공유 연합 학습에서, 단말 기기의 모델을 학습하기 위한 알고리즘으로 FedSim 과 FedAlt 알고리즘이 제안되어왔다. 본 논문에서는 기존의 학습 알고리즘에 따른 성능 비교 연구를 진행하였다. 성능 비교 결과, FedAlt 알고리즘이 FedSim 에 비해 좋은 성능을 보이는 것을 확인하였다.

## Ⅰ. 서 론

디지털 기술의 급격한 발전으로 인해 통신 단말 기기의 수가 급증하면서, 각 단말 기기에서 데이터를 수집 및 생성하는 분산된 데이터 환경이 조성되고 있다. 이러한 분산된 데이터 환경에서, 데이터의 직접적인 공유 없이 각 단말 기기를 위한 인공지능 모델을 학습하기 위해 연합 학습 방법(Federated Learning)이 제안되었다[1,2,3,4,5].

연합 학습 방법 이전의 인공지능 모델을 학습하기 위해서는 각 단말 기기의 데이터를 중앙 서버에 전송하는 중앙집중형 학습(Centralized Learning)을 통해 학습을 진행하였다. 이러한 중앙집중형 학습은 많은 양의 데이터를 직접적으로 전송하기 때문에 통신 효율이 좋지 않다는 문제점과, 데이터 보안에 더욱 취약해진다는 문제점을 가지고 있다. 따라서, 연합 학습 방법에서는 직접적으로 데이터를 전송하지 않는 대신, 각 단말에서 개별 데이터를 이용하여 학습한 개별 모델의 정보를 전송하여 기존 중앙집중형 학습의 두가지 문제점을 해결하였다[1,2].

그러나 모델의 모든 정보를 공유하는 연합 학습 방법은 각 단말이 보유하고 있는 개별 데이터의 특성과 무관하게, 일관된 하나의 모델을 공유한다는 문제점이 존재한다. 이러한 연합 학습 방법의 문제점을 해결하기 위해, 개별 데이터의 최적화된 모델의 생성이 가능한 부분 공유 연합 학습이 제안되었다[3,4,5].

본 논문에서는 부분 공유 연합 학습을 위한 기존의 학습 알고리즘의 방법에 대하여 서술한 뒤, 각 알고리즘의 성능 비교를 진행한다.

## Ⅱ. 부분 공유 연합 학습

본 장에서는 부분 공유 연합 학습의 전체적인 방법과 기존 학습 알고리즘인 FedSim 과 FedAlt 알고리즘의 학습 방법에 대하여 서술한다[3].

부분 공유 연합 학습은 통신 라운드(Communication Round) $1 < r < R$ 마다 중앙 서버에서 $C$ 개의 단말 기기를 선택하여 통신 참여 집합을 생성한다. 통신 참여 집합 $D^r$에 포함되는 $d$번째 단말 기기는 개별 데이터를 이용하여 개별 모델의 학습을 진행하며, 학습 후의 모델 정보 $W_d$를 공유 부분 $S_d$와 개인 부분 $P_d$로 구분한다. 이렇게 구분된 공유 부분 $S_d$는 중앙 서버로 전송하여 다른 단말 기기와 연합 학습을 진행할 수 있으며, 개인 부분 $P_d$ 을 이용하여 개별 데이터에 최적화된 모델을 생성할 수 있다.

중앙 서버에서는 전송 받은 $d$번째 단말 기기의 공유 부분 $S_d$를 취합하여 갱신된 공유 부분 $\bar{S}$를 다음과 같은 방법으로 생성한다.

$$\bar{S} = \frac{1}{C}\sum_{d \in D^r} S_d$$

중앙 서버는 각 단말 기기의 공유부분에 대하여 평균값을 가지도록 갱신된 공유 부분 $\bar{S}$를 생성한 후, 해당 정보를 각 단말 기기에게 전송한다. 각 단말 기기에서는 갱신된 공유 부분 $\bar{S}$를 이용하여 개인 부분 $P_d$를 학습을 진행하며, 갱신된 공유 부분 $\bar{S}$를 이용하는 방법에 따라 FedSim과 FedAlt 방법의 알고리즘 차이가

*교신저자(Corresponding Author)

존재한다. 본 논문에서는 각 알고리즘의 학습 결과를 $(P_d^*, S_d^*)$로 표현하여 그 차이를 설명한다.

### Ⅱ.1. FedSim 알고리즘

FedSim 은 각 단말 기기에서 공유 부분 $S_d$ 를 서버에서 전송 받은 $\bar{S}$ 로 갱신한 뒤, 개별 데이터를 이용하여 개인 부분 $P_d$ 와 공유 부분 $\bar{S}$ 전체에 대하여 동시에 학습을 진행하는 방법이다[3].

$$(P_d^*, S_d^*) \leftarrow (P_d, \bar{S})$$

그러나 FedSim 은 $\bar{S}$로 갱신하였을 때, 개인 부분 $P_d$와 공유 부분 $\bar{S}$ 사이의 호환성이 떨어지는 상태로 바로 학습을 진행한다는 문제점이 존재한다. 따라서 $\bar{S}$와 $P_d$ 사이의 호환성을 높이는 방향으로 학습이 진행되며, 이 과정에서 $\bar{S}$가 포함하고 있는 연합 학습에 대한 정보의 보존이 어렵다는 문제가 존재한다.

### Ⅱ.2. FedAlt 알고리즘

FedAlt 는 알고리즘은 FedSim 과 달리 개별 데이터를 이용하여 개인 부분 $P_d$와 $\bar{S}$를 두 단계에 걸쳐 번갈아 학습을 진행하는 방법이다. 첫번째 단계에서는 서버로부터 $\bar{S}$를 전송 받아 갱신한 직후, $\bar{S}$가 포함하고 있는 연합 학습에 대한 정보를 보존하기 위해 $\bar{S}$ 의 파라미터를 고정한 후 개인 부분 $P_d$ 의 파라미터만 학습을 진행한다[3].

$$(P_d^*, \bar{S}) \leftarrow (P_d, \bar{S})$$

이 과정을 통해 학습된 개인 부분 $P_d^*$는 $\bar{S}$에 대한 높은 호환성을 가지게 된다. 두번째 단계에서는 학습된 개인 부분 $P_d^*$ 의 파라미터를 고정한 후 공유 부분 $\bar{S}$ 의 파라미터만 학습을 진행한다.

$$(P_d^*, S_d^*) \leftarrow (P_d^*, \bar{S})$$

이 과정을 통해서 공유 부분 $\bar{S}$를 $S_d^*$로 갱신해 주게 되며, 이렇게 갱신된 $S_d^*$는 개별 데이터에 대한 정보를 포함할 수 있도록 학습된다.

## Ⅲ. 성능 비교 실험

본 논문에서는 기존에 제안되었던 FedSim 과 FedAlt, 알고리즘의 성능 비교를 위한 실험을 진행하였다. 성능 비교 실험을 위한 데이터로 MNIST 데이터를 사용하였으며, 각 개별 단말 기기가 다른 데이터 분포 특성을 가지도록 데이터를 분배하였다. 또한 부분 공유 연합 학습 방법의 유효성을 검증하기 위해 연합 학습을 진행하지 않고 개별로 학습을 진행하는 방법인 No sharing 과 부분 공유 연합학습 방법인 FedSim 과 FedAlt 의 성능 비교를 진행하였다.

성능 비교 실험 결과, 연합 학습 방법을 사용하지 않고 개별적으로 학습을 진행한 No sharing 방법 대비 부분 공유 연합 학습 방법을 사용하였을 때 더 좋은 성능을 내는 것을 확인 할 수 있다. 이를 통해 개별적인 데이터의 분포가 다른 상황이라도, 연합 학습 방법이 유효함을 검증하였다. 또한 FedSim 방법과 FedAlt 방법을 비교하였을 때, 공유 부분의 연합 학습 정보를 보존하는 FedAlt 가 근소하게 개선된 성능을 보이는 것을 확인 가능하다.

**표 1. 학습 알고리즘에 따른 성능**

| | Accuracy |
|---|---|
| No sharing | 0.8641 |
| FedSim | 0.9066 |
| FedAlt | 0.9108 |

## Ⅲ. 결론

본 논문에서는 개인화 연합 학습을 위한 기존의 부분 공유 연합 학습 방법의 학습 알고리즘에 따른 성능 비교 실험을 진행하였다. FedAlt 알고리즘의 학습 방법은 FedSim 알고리즘이 가지고 있는 연합 학습 정보 보존 문제, 모델 호환성 문제를 해결한 방법으로 그 우수성을 실험을 통해 입증하였다. 따라서 분산된 데이터 환경에서 FedAlt 알고리즘의 학습 방법을 적용하여 개선된 성능의 연합 학습 방법을 기대할 수 있다.

ACKNOWLEDGEMENT

이 논문은 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원(No. 2021-0-00739, 분산/협력 AI 기반 5G+ 네트워크 데이터 분석 기능 및 제어 기술 개발)과 한국연구재단의 지원(No. NRF-2020R1F1A1069182)을 받아 수행된 연구임

## 참 고 문 헌

[1] B. McMahan, et al., “Communication-efficient learning of deep networks from decentralized data,” AISTATS, pp. 1273-1282, 2017.

[2] Li, Tian, et al., "Federated learning: Challenges, methods, and future directions," IEEE signal processing magazine vol.37, no.3, pp. 50-60, 2020.

[3] K. Pillutla, et al., “Federated learning with partial model personalization,” ICML, pp. 17716-17758, 2022.

[4] H. Kye, and M. Kwon, “Partial federated learning based network intrusion system for mobile devices,” ACM MobiHoc, pp. 283-284, 2022.

[5] P. P. Liang, et al. "Think locally, act globally: Federated learning with local and global representations," NeurIPS 2019 Workshop on Federated Learning, 2019.