

Non-IID 데이터를 활용한 개인화 연합학습 기반 실내 측위

김택윤, 박준하, 김효원, 김선우
한양대학교 융합전자공학과

{kty0264, eric0725, khw870511, remero}@hanyang.ac.kr

Personalized Cross-silo Federated Learning on Non-IID data for Indoor Localization

Taekyoon Kim, Junha Park, Hyowon Kim, and Sunwoo Kim
Department of Electronic Engineering, Hanyang University

요약

본 논문에서는 서로 다른 분포를 지닌 non-IID 데이터를 활용한 개인화 연합학습(personalized federated learning) 기반 실내 측위 방법을 소개하고 그 결과를 분석한다. 분산 학습과 연합학습의 주요한 차이점 중 하나인 학습 데이터의 non-IID 특성은 모델의 최적화 및 수렴성에 큰 영향을 미친다. 이를 해결하기 위해 FedAMP (federated attentive message passing)라는 연합학습 기법을 활용한 측위 모델을 제안한다. FedAMP는 서로 다른 분포의 데이터를 지닌 클라이언트 간의 유사도를 고려하여 클라이언트마다 개인화된 모델을 최적화하는 것을 목표로 한다. 시뮬레이션을 통해 서로 다른 위치에서 획득한 데이터로 최적화시킨 개인화 모델의 측위 성능을 평가하고 그 결과를 분석한다.

I. 서론

연합학습(federated learning)은 deep neural network (DNN)을 기반으로 여러 클라이언트가 함께 학습해 서버에 있는 글로벌 DNN 모델을 최적화하는 기계 학습 기법이다. 연합학습은 분산 학습과 다르게 개별 클라이언트들이 최적화를 진행하는 데이터가 서로 다른 분포를 지닌다(non-IID). 때문에, 연합학습으로 최적화되는 모델은 DNN보다 낮은 성능을 보이게 된다. 이를 해결하기 위해 본 논문에서는 서버에서 클라이언트마다 개인화된 글로벌 모델을 생성하는 FedAMP 기반 측위 모델을 제안한다. 시뮬레이션을 통해 classification 정확도를 평가하고 FedAMP가 기존의 연합학습과 어떤 차이를 보이는지 분석한다.

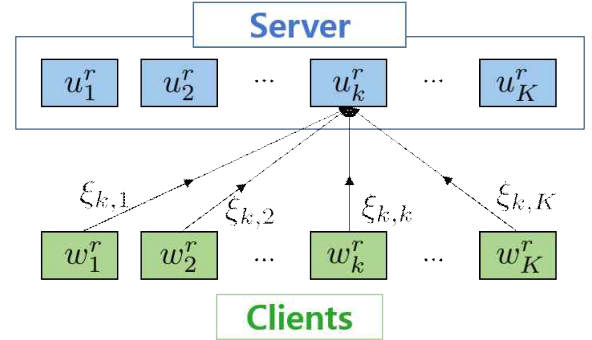


그림 1. FedAMP 학습 구조

σ 는 임의로 설정된 매개변수이다. 두 모델 w_i, w_j 가 완전히 같으면 1, 차이가 점차 커질수록 0에 가까운 값을 갖는다. FedAMP에서 클라이언트의 개인화 모델은 유사도가 낮은 모델에는 낮은 가중치를, 유사도가 높은 모델에는 높은 가중치를 주고 선형 결합으로 통합한다.

글로벌 모델의 학습은 일반적인 DNN 모델과는 조금 다르다. 서버에서 생성되는 글로벌 모델의 학습은 여러 모델의 선형 결합으로 이루어지기 때문에, 모델 통합 반복 횟수인 round 단위로 학습이 진행된다. t 번째 round에서 i 번째 클라이언트를 위한 개인화 글로벌 모델의 가중치 통합은 다음과 같이 이루어진다.

$$\begin{aligned} u_i^t &= \left(1 - \alpha \sum_{j \neq i}^K A'(\|w_i^t - w_j^t\|^2)\right) w_i^t \\ &\quad + \alpha \sum_{j \neq i}^K A'(\|w_i^t - w_j^t\|^2) w_j^t \\ &= \xi_{i,1} w_1^t + \xi_{i,2} w_2^t + \dots + \xi_{i,K} w_K^t. \end{aligned} \quad (4)$$

α 는 학습률, K 는 전체 클라이언트 수, A' 은 attention-inducing function A 의 미분, ξ 는 클라이언트의 attention 가중치를 의미한다. Self-attention 가중치는 $\xi_{i,i} = 1 - \sum_{j \neq i}^K \xi_{i,j}$ 로 정의된다. 모델 w_1^t, \dots, w_K^t 는 t 번째 round에서 모델 통합 메시지(model-aggregation message)로 정의할 수 있고, 서버에서는 전달받은 모델 통합 메시지와 attention 가중치를 이용해 i 번째 클라이언트를 위한 모델 u_i^t 를 생성한다. $t+1$ 번째 round에서 i 번째 클라이언트는 초기 모델 가중치로 u_i^t 를 설정하고, adam과 같은 기울기 기반 학습을 통해 w_i^{t+1} 을 학습한다. 연합학습은 최종적으로 글로벌 모델의 성능이 수렴할 때까지 round를 반복한다.

II. FedAMP 기반 측위 학습 모델

연합학습의 서버에 있는 글로벌 DNN 모델은 로컬 클라이언트들이 각자 획득한 정보로만 DNN 모델을 학습하고, 서버에서 모든 모델을 통합해 글로벌 DNN 모델을 생성한다. 서버는 글로벌 모델의 구조를 미리 설정해놓고, 학습에 참여하는 클라이언트가 결정되면 각 클라이언트들에게 미리 설정된 구조의 글로벌 모델을 전달해 학습을 진행한다.

로컬 클라이언트들의 학습 레이블은 기준 위치의 ID이고, 학습 입력 데이터는 기준 위치에서 측정한 주변에 있는 AP (access point) RSSI (received signal strength indicator)로 이루어진다. 학습 레이블은 각각 미리 설정된 기준 위치를 나타내고 있고, 기준 위치마다 학습 레이블 번호 y 가 설정되어 있다. i 번째 단말이 획득한 n 번째 데이터는 다음과 같다.

$$\mathbf{x}_{i,n} = [r_{i,1}, \dots, r_{i,M}] \quad (1)$$

$r_{i,m}$ 은 m 번째 AP로부터 획득한 RSSI 값이다. 모든 단말은 다음과 같이 손실함수를 최소화하는 방법으로 자신들의 DNN 모델을 학습한다.

$$w_i = \arg \min_w \frac{1}{N} \sum_{n=1}^N f(w, \mathbf{x}_{i,n}, \mathbf{y}_{i,n}) \quad (2)$$

w 는 모델의 가중치, f 는 손실함수를 의미한다. 모든 클라이언트는 동일한 구조로 학습하기 때문에, 서버에서는 각 모델 가중치 w 의 정규화된 선형 결합(normalized linear combination)으로 통합할 수 있다.

일반적인 연합학습[2] 방법과 다르게, FedAMP[1]는 클라이언트마다 개인화된 모델을 제공한다. 그림 1과 같이, 클라이언트들이 최적화시킨 모델의 선형 결합을 통해 각각 클라이언트의 모델로 통합한다. 선형 결합에는 유사도(similarity)를 활용하는데, 유사도는 다음과 같은 attention-inducing function A 를 통해 계산된다.

$$A(\|w_i - w_j\|^2) = 1 - \exp(-\|w_i - w_j\|^2 / \sigma). \quad (3)$$

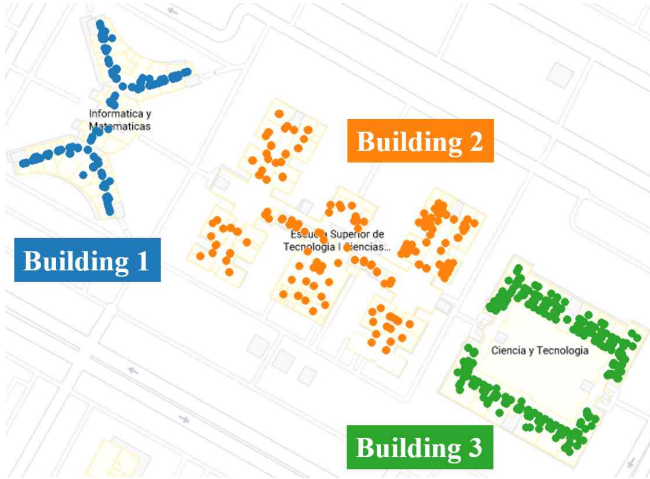


그림 2. 측위 학습 시뮬레이션에 사용된 참조 위치

III. 시뮬레이션 환경 및 결과

시뮬레이션은 classification 정확도를 통해 모델의 성능을 파악한다. 시뮬레이션을 위한 데이터베이스로 UJIIndoorLoc 데이터베이스를 사용하였다[3]. 시뮬레이션에 사용된 매개변수들은 표 1에 정리되어 있다. 전체 클라이언트 수는 3으로 설정했는데, 이는 학습을 위한 데이터베이스를 그림 2에서 보이는 건물 단위로 설정한 것과 같다. 전체 학습 데이터 개수 N_{train} 은 5,002개 데이터를 건물별로 1,356개, 1,484개, 2,162개로 설정했다. 서로 다른 건물에서 취득한 데이터는 다른 분포를 지니므로 non-IID의 특성을 띠게 된다.

성능 평가는 매 round 클라이언트가 속한 건물의 데이터 일부를 테스트 입력 데이터로 활용해 classification 정확도(accuracy)를 산출한다. 테스트 데이터 개수 N_{test} 는 건물별로 400개를 설정했다. 정확도 $p(c)$ 는 n 번째 테스트 출력 데이터의 예측된 위치를 \hat{y}_n , 실제 위치를 y_n 이라 할 때 다음과 같다.

$$p(c) = \frac{\sum_{n=1}^{N_{test}} c_n}{N_{test}}, c_n = \begin{cases} 1 & \text{if } \hat{y}_n = y_n \\ 0 & \text{otherwise} \end{cases} \quad (5)$$

Round는 총 100번을 수행했고 그 결과는 그림 3과 같다. 최초 모델 통합 이후에는 잠시 성능이 낮아지지만, 점차 높아지는 경향을 보여주는 것을 확인할 수 있었고 최소 정확도 91%에 도달했다. 정확도가 가장 낮은 건물은 가운데 위치한 건물로 양옆 건물에서 측정되는 AP의 정보가 측정되기 때문에 성능에 일부 영향을 주는 것으로 판단된다.

정확도만으로는 FedAMP가 다른 연합학습 기법이나 DNN에 비해 어느 정도 효용성이 있는지 알 수 없다. 다른 연합학습이나 DNN과 성능을 비교하기보다 모델 통합에 사용되는 attention 가중치를 확인해보면 FedAMP의 모델 통합이 어떻게 진행되는지 알 수 있다. 그림 4는 모델별 self-attention 가중치 $\xi_{i,i}$ 를 20 round까지 그린 그래프이다. $\xi_{3,3}$ 은 round 20회에서 이미 1에 가까운 수치를 보이고, $\xi_{1,1}, \xi_{2,2}$ 도 round에 따라 점차 1로 수렴한다. 즉, FedAMP의 개인화

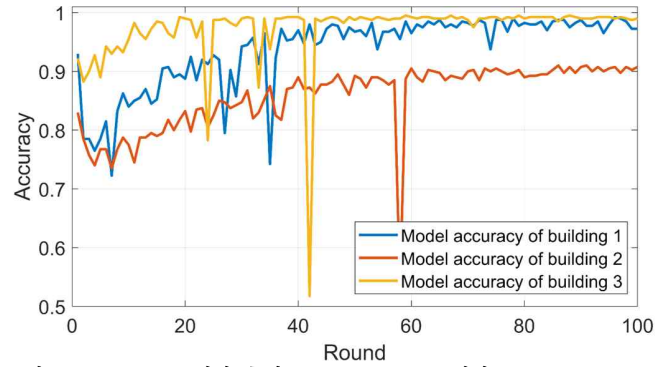


그림 3. FedAMP 기반 측위 classification 정확도

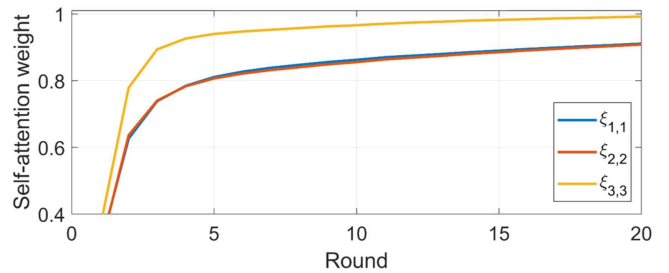


그림 4. 20 round까지의 self-attention 가중치

모델은 연합학습이 아닌 DNN으로 학습되는 것과 동일했다.

각 모델이 DNN으로 수렴하는 이유는 데이터베이스가 수집하는 RSSI 데이터 간에 correlation이 매우 작기 때문으로 추측된다. 학습 레이블이 건물에 따라 명확하게 나뉘고, 따라서 다른 건물의 데이터를 학습하기 위한 충분한 가중치를 부여하지 못하는 상황이 된다. 따라서 FedAMP는 non-IID 데이터라도 correlation이 매우 낮은 경우에는 활용할 수 없는 연합학습 방법을 확인할 수 있었다.

IV. 결론

본 논문에서는 non-IID 데이터를 사용한 FedAMP 기반 측위 방법을 제안한다. 건물 단위로 구축한 non-IID 데이터베이스에서 클라이언트별 연합학습 기반 측위 모델을 생성한다. 개별 모델 측위 정확도는 확보했지만 설정된 시나리오에서 DNN 학습과의 차이를 보이지 못했다. FedAMP의 장점을 잘 활용하기 위해선, 같은 non-IID 데이터베이스라도 데이터 사이에 correlation을 높인다면 (e. g. 한 건물 내의 겹친 구역 또는 다른 층에서 학습) 유의미한 결과를 보일 수 있을 것이다.

ACKNOWLEDGMENT

본 연구는 2021년도 정부(소방청)의 재원으로 정보통신기획평가원 (No.2019-0-01325, 재난현장 무선통신 추적기반 요구조사 및 소방관 위치정보시스템 개발), 과학기술정보통신부 및 정보통신기술진흥센터의 대학ICT연구센터 육성 지원사업(IITP-2021-2017-0-01637)의 연구 결과로 수행되었음.

참 고 문 헌

- [1] Y. Huang, *et. al.*, "Personalized cross-silo federated learning on non-IID data," in *Proc. AAAI Conf. Artif. Intell.*, 2021.
- [2] H. B. McMahan, *et. al.*, "Communication efficient learning of deep networks from decentralized data," in *Proc. Int. Conf. Artif. Intell. Statist. (AISTATS)*, PMLR, 2017.
- [3] J. Torres-Sospedra, *et. al.*, "UJIIndoorLoc: A new multi-building and multi-floor database for WLAN fingerprinting-based indoor localization problems," in *Proc. 2014 Int. Conf. Indoor Positioning Indoor Navi. (IPIN)*, 2014.

표 1. 모델 및 학습 매개변수

매개변수	값
전체 클라이언트 수, K	3
전체 access point 수, M	520
서버 학습 반복 횟수(round)	100
은닉층 구성(hidden layer format)	$1024 \times 2048 \times 1024$
최적화기(optimizer)	Adam
학습률(learning rate), α	0.0001
클라이언트 학습 반복 횟수(epoch)	20
활성 함수(activation function)	ReLU, softmax (last)
손실 함수(loss function)	Cross-entropy