# 불확실성 기반 베이지안 연합학습: 통신 효율성과 학습 강인성 관점에서의 고찰

홍용상, 홍준표
홍익대학교

anftkwhrltke@g.hongik.ac.kr, jp_hong@hongik.ac.kr

# Uncertainty-Aware Bayesian Federated Learning: A Perspective on Communication Efficiency and Learning Robustness

Yongsang Hong, Jun-Pyo Hong
Hongik Univ.

## 요 약

연합학습(federated learning, FL)은 분산학습을 통해 개인정보 유출 위험을 줄이고, 중앙 서버의 연산 부담을 완화하며, 학습의 확장성과 통신 효율성을 동시에 달성할 수 있는 기술로 주목받고 있다. 하지만 현재까지 대부분의 연합학습 연구들은 빈도주의적(frequentist) 접근에 기반하고 있어, 비동질(Non-IID) 환경에서의 성능 저하, 모델 파라미터 및 예측에 대한 불확실성(uncertainty) 평가 불가 등 근본적인 제약을 가진다. 이러한 문제들을 보완하기 위해 확률론적 추론을 결합한 베이지안(Bayesian) FL 이 제안되었다. 본 논문에서는 BFL 의 기본 개념과 발전 과정을 정리하고, 주요 연구들의 흐름을 통해 그 장점과 한계를 분석하며, 향후 연구 방향성을 제시한다.

## Ⅰ. 서 론

최근 모바일 기기와 웨어러블 장치들을 통해 사용자들이 방대한 양의 데이터를 생성해 내고 있으며, 이러한 데이터에 기반한 지능형 서비스들에 대한 관심과 수요가 높아지고 있다. 그러나 이러한 데이터는 대개 개인정보와 밀접하게 연관되어 있기 때문에 중앙 서버에서 데이터를 수집해 학습할 시, 데이터 프라이버시 문제가 발생할 수 있다. 학습 과정에서 이와 같은 문제와 중앙 서버의 부하를 완화하기 위한 효과적인 방법으로 최근 연합학습(Federated learning, FL)이 각광을 받고 있다 [1], [2].

FL 은 지역 데이터셋의 분포가 크게 상이한 환경에서 각 클라이언트가 지역 학습을 통해 본인이 보유한 데이터에 적합한 단일 모델을 도출할 경우, 해당 모델이 클라이언트마다 크게 달라 이들의 통합에서 의미 있는 전역 모델이 도출되지 않는 client drift 현상으로 인해 학습 성능이 저하되는 문제를 갖고 있다. 또한 기존 대부분의 FL 기법이 채용하고 있는 빈도주의(frequentist) 접근법은 학습 상황에 대한 해석이 어려워 모델 공유를 위한 통신 자원이 제한적인 환경에서 통신 상황에 맞게 자원을 효율적으로 활용하기 어렵다는 한계가 존재한다.

이러한 기존 FL 기법들에 대한 한계점의 근원적 해결을 위해 최근 베이지안(Bayesian) 접근을 FL 에 도입하는 연구가 이루어지고 있다. 베이지안 접근법의 도입은 FL 에서 지역 모델의 파라미터에 대한 신뢰도 혹은 불확실도를 정량화함으로써, 이러한 신뢰도를 기반으로 파라미터의 중요성을 판단해 보다 효과적인 모델 합계와 통신 자원 환경에 적응적인 학습을 가능하게 한다.

## Ⅱ. 본 론

빈도주의 접근 기반의 학습 방식은 데이터를 기반으로 likelihood 를 최대화하는 단일 모델 파라미터 도출을 목표로 한다.

$$\boldsymbol{\theta}^* = arg\max_{\theta} p(D|\boldsymbol{\theta}) \quad (1)$$

반면, 베이지안 학습 방식은 모델 파라미터에 대한 사후분포(posterior distribution) $p(\boldsymbol{\theta}|D)$ 도출을 목표로 한다. 이러한 사후분포는 다양한 모델 파라미터에 대한 신뢰도 혹은 불확실도에 대한 정보를 내포하며, 이를 기반으로 (1) 예측 불확실성을 정량화하고, (2) 제한된 데이터 환경에서도 사전정보를 활용해 성능을 개선할 수 있다는 장점을 가진다 [3], [4].

베이지안 FL 은 이러한 베이지안 접근을 연합학습에 도입한 방식으로, 각 클라이언트 $k$는 지역 데이터 $\mathcal{D}_k$를 기반으로 사후분포 $p(\boldsymbol{\theta}|\mathcal{D}_k)$를 학습하고, 서버가 이를 통합함으로써 전역 사후분포 $p(\boldsymbol{\theta}|\{\mathcal{D}_k\}_{k\in\mathcal{K}})$를 근사한다. 이후 업데이트된 전역 사후분포는 다시 각 클라이언트로 분배되어 분산 학습 후 통합을 반복하는 과정을 통해 학습이 수행된다. 이와 같이 베이지안 방식을 FL 에 적용하는 것은 사후분포 기반의 불확실성 정량화로 기존 베이지안 학습의 장점을 활용할 수 있을 뿐만 아니라 FL 의 주요 도전과제인 client drift 완화, 학습-통신 융합설계를 가능하게 한다

기존 FL 은 참여하는 클라이언트들이 보유한 데이터의 분포가 크게 상이한 환경에서 client drift 현상으로 인해 학습 성능이 저하하는 한계를 갖는다. 반면 베이지안 FL 은 각 클라이언트가 지역 학습을 통해 다양한 모델에 대한 신뢰도를 사후분포 형태로 표현하므로, 이를 바탕으로 여러 클라이언트들에서도 공통적으로 높은 신뢰도를 갖는 전역 모델을 도출할 수 있다. [5]에서 제안한 pFedBayes 는 지역 학습에서 변분 추론(variational inference)을 통해 사후분포를 KL divergence 를 최소화하는 정규분포로 근사하였으며, 지역 정규분포의 변분 파라

미터(variational parameter)의 평균으로 전역 모델을 도출하는 개인화 FL 을 연구하였다. 또한 도출된 전역 모델을 지역 모델의 사전분포로 설정하고 학습함으로써 일반화와 개인화 성능의 균형을 경험적으로 조절했다. 그 결과 제한된 데이터 환경에서도 CIFAR-10 및 FEMNIST 데이터셋에서 FedAvg 대비 5~8% 높은 정확도를 달성하며 개인화와 일반화 성능을 동시에 확보했다.

pFedBayes 가 경험적으로 균형을 유지한 반면, [6]에서는 이를 계층적(Hierarchical) 베이지안 구조로 일반화한 FedHB 를 제안했다. FedHB 는 각 클라이언트의 파라미터 $\theta_i$가 전역 하이퍼파라미터 $\phi$에 종속되도록 설계해, 모든 클라이언트가 전역 하이퍼-사전분포(Hyper-prior)를 공유한다. 이를 통해 클라이언트 간 데이터 편차가 큰 환경에서도 일관된 수렴을 달성하였으며, 개인화와 전역 일반화 간의 trade-off 를 명시적으로 제어할 수 있었다. 실험 결과, CIFAR-10 과 FEMNIST 에서 FedHB 는 FedAvg 대비 7~10% 높은 정확도를 보였고, 클라이언트 간 정확도 편차가 감소하였다.

개인화 FL 을 고려한 앞선 논문과 달리, [7]에서는 모든 클라이언트들에게 적용할 수 있는 일반화된 사후분포 도출을 목표로 하는 federated online Laplace approximation(FOLA)를 제안하였다. FOLA 에서는 각 클라이언트가 라플라스 근사(Laplace approximation)을 통해 사후분포와 동일한 mode 를 갖는 정규분포로 사후분포를 근사하고, 서버는 지역 사후분포 간 곱연산으로 전역 사후분포를 갱신한다. 이와 같은 곱연산은 다수의 분포를 대표하는 하나의 분포를 도출할 때, 정보 손실을 최소화할 수 있는 방법이다. 그 결과, 단순 평균 기반 BFL 대비 집계 오차가 약 23% 감소하였고, 학습 라운드당 연산 시간도 감소하여 연산 효율성과 학습 안정성을 동시에 개선되었다.

베이지안 FL 에서 클라이언트는 정규분포로 근사된 지역 사후분포에 대한 정보를 전달할 때, 모델의 각 파라미터에 대한 평균과 분산을 전송하므로 기존 FL 보다 통신 부하가 약 두 배 높다. 이에 따라, 베이지안적 접근과 함께 가중된 통신 부하 문제를 완화하기 위해 무선 채널의 중첩 현상을 활용한 Over-the-Air Computation (AirComp)를 베이지안 FL 에 적용한 기법이 [8]에서 제안되었다. 무선 채널에서의 전송 중 지역 사후분포 간의 곱연산이 이루어질 수 있도록 하는 사전/사후 처리 기법이 개발되었으며, 수렴 분석을 통해 학습 가속화를 위한 최적 전력제어 기법이 개발되었다. 이를 통해 AirComp 기반의 기존 FL 방식 대비 약 35% 낮은 통신 지연과 3~5% 높은 모델 정확도를 달성함으로써 데이터 희소성과 이질성이 공존하는 환경에서도 안정적으로 수렴함을 보였다.

## Ⅲ. 결 론

베이지안 FL 은 비동질 데이터 환경에서의 강건성, 예측 불확실성 정량화, 전역-개인화 모델 간 균형 조절, 통신 효율성 향상 등 다양한 장점을 지닌다. 그러나 posterior 근사를 위한 높은 계산 복잡도와 확률분포 파라미터 전송으로 인한 통신 부담, 모델 구조의 복잡성은 여전히 해결해야 할 과제이다. 이러한 맥락에서 적응형 모델 경량화(lightweight approximation) 와 효율적 확률 근사 기법에 대한 연구의 필요성이 높아지고 있다. 특히 저차원 확률 근사, 샘플 효율적 변분추론, 파라미터 공유 및 압축 전송 기법의 융합을 통해 연산과 통신 효율을 동시에 개선하는 방향으로 연구가 진행될 것으로 전망된다.

## ACKNOWLEDGMENT

이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (RS-2024-00464570)

## 참 고 문 헌

[1] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, “Communication-efficient learning of deep networks from decentralized data,” in *Proc. Int. Conf. Artif. Intell. Statist. (AISTATS)*, PMLR, 2017, pp. 1273-1282.

[2] T. Li, A. K. Sahu, M. Zaheer, M. Sanjabi, A. Talwalkar, and V. Smith, “Federated learning: Challenges, methods, and future directions,” *IEEE Signal Process. Mag.*, vol. 37, no. 3, pp. 50-60, May 2020.

[3] C. Blundell, J. Cornebise, K. Kavukcuoglu, and D. Wierstra, “Weight uncertainty in neural network,” in *Proc. Int. Conf. Mach. Learn. (ICML)*, PMLR, 2015, pp. 1613-1622.

[4] S. Sun, G. Zhang, J. Shi, and R. Grosse, “Functional variational Bayesian neural networks,” in *Proc. Int. Conf. Learn. Represent. (ICLR)*, 2019.

[5] X. Zhang, M. Hong, S. Dhakal, S. P. Karimireddy, and T. Li, “Personalized federated learning via variational Bayesian inference,” in *Proc. Int. Conf. Mach. Learn. (ICML)*, PMLR, 2022, pp. 26697-26716.

[6] M. Kim and T. Hospedales, “FedHB: Hierarchical Bayesian federated learning,” *arXiv preprint* arXiv:2305.04979, 2023.

[7] L. Liu, M. Chen, W. Saad, and C. Yin, “A Bayesian federated learning framework with online Laplace approximation,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 46, no. 1, pp. 1-16, Jan. 2024.

[8] J.-P. Hong, H. Seo, and K. Lee, “Distribution-level AirComp for wireless federated learning under data scarcity and heterogeneity,” *arXiv preprint* arXiv:2506.06090, 2025.