거리기반 이상치 탐지를 통한 개선된 연합학습 기법

고은서, 김효원, 도인실*
이화여자대학교
rhdmstjrjdi@ewhain.net, haze_by@ewhain.net, *isdoh1@ewha.ac.kr

Improved Federated Learning techniques through distance-based outliers detection

Eunseo Ko, Hyowon Kim, Inshil Doh*
Ewha Womans University

요 약

IoT와 같은 인터넷에 연결되는 장치의 수가 증가함에 따라, 다양한 디바이스로부터 기하급수적인 양의 데이터가 생성되고 있다. 이러한 데이터는 중앙 서버에 업로드하는 과정에서 개인정보가 유출되는 문제를 야기할 수 있다. 이에 연합학습 기술이 도입되었지만, 연합학습 과정에서 불균형한 분포로 인한 성능 저하 문제가 발생할 수 있다. 이러한 문제를 해결하기 위해 편향된 데이터셋을 가지는 노드들을 제거하여 학습시키면 글로벌 모델의 성능이 향상될 수 있지만, 이러한 노드를 완전히 제거하는 경우 다양성을 학습할 수 없어 여러 가지 환경에 대한 적용이 불가능하다. 본 논문에서는 모니터링 라운드-업데이트 라운드로 구성된 개선된 연합학습 기법을 제안하여 모든 노드가 학습에 참여할 수 있도록 하면서 각 라운드에서 이질적인 분포를 보이는 노드의 가중치에 대한 영향력을 임시로 낮춰 불균형한 데이터셋 분포에서의 학습 취약점을 개선하고자 한다.

Ⅰ. 서 론

오늘날에는 다양한 디바이스로부터 기하급수적인 양의 데이터가 생성되고 있다. 이러한 데이터로부터 유의미한 작업을 하기 위해서는 각 로컬 디바이스의 원본 데이터를 중앙 서버에 업로드해야 한다. 하지만 데이터를 중앙 서버로 업로드하는 과정에서 개인정보가 유출될 가능성이 있다. 이러한 문제는 연합학습을 도입함으로써 해결할 수 있다. 연합학습은 여러 디바이스에서 데이터를 로컬로 유지하면서 글로벌 모델을 공동으로 학습할 수 있도록 하는 머신 러닝 기술이다[1]. 일반적으로 연합학습은 모든 로컬 디바이스에 글로벌 모델을 배포하여 작동한다. 각 디바이스에서 로컬 데이터를 사용하여 글로벌 모델을 학습하고 추출된 가중치를 중앙 서버로 보낸다. 서버는 가중치를 집계하여 글로벌 모델을 업데이트한다.

거리 기반 탐지 기술은 데이터 지점 간의 거리 또는 유사성을 계산하고 이 측정을 사용하여 패턴 또는 관계를 식별하는 것을 의미한다[2]. 이 과정에서 유클리드 거리, 맨해튼 거리, 코사인 유사성과 같은 다양한 거리 측정을 사용할 수 있다. 이러한 기술은 종종 나머지 데이터셋과 크게 다른 데이터를 식별하는 데 사용된다. 본 논문에서는 유클리드 거리 측정법을 사용하여 편향된 데이터셋을 가진 노드를 감지한다.

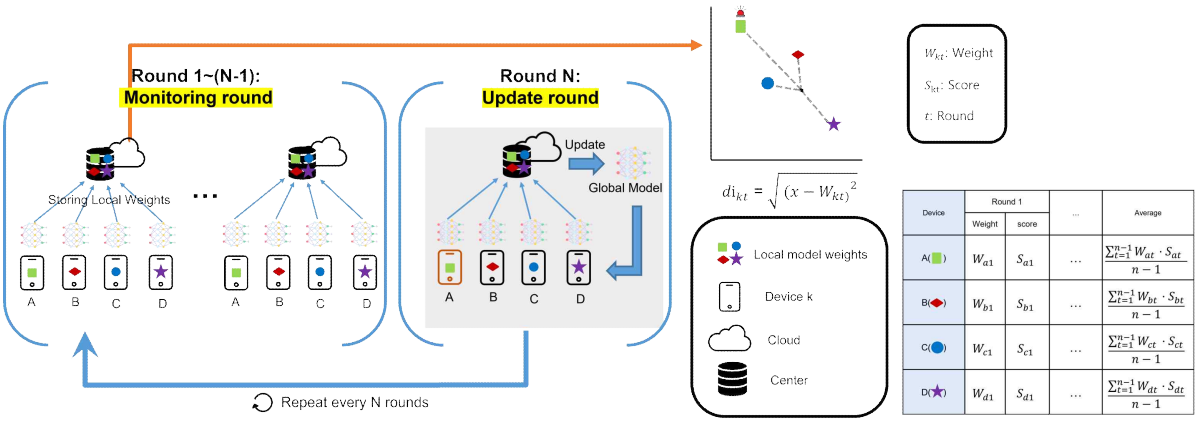
특히, 본 연구에서는 사용되는 데이터를 실시간으로 수집되는 데이터로 가정하며, 편향된 데이터셋을 가지는 노드를 배제하는 것이 아니라 그 영향력을 낮추는 것을 목표로 한다. 이를 위해 score를 기록하는 모니터링 라운드와 score가 적용된 가중치를 기반으로 글로벌 모델을 개선하는 업데이트 라운드로 구성되는 개선된 방식의 연합학습 구조를 제안한다. score는 편향된 데이터셋을 가지는 노드의 영향력을 줄이기 위해 설정한 변수로 0과 1 사이의 값을 가진다. 본 논문에서 제안한 기법은 다양한 상황에서의 일반화 능력 향상과 글로벌 모델의 업데이트 횟수의 감소로 인해 오버헤드를 줄일 수 있다는 장점이 있다.

Ⅱ. 관련연구

연합 학습은 원본 데이터가 로컬에 있기 때문에 사용자의 개인 정보를 보호할 수 있지만, 장치 간 사용 패턴과 환경의 차이로 인해 데이터의 불균형 분포를 유발하여 글로벌 모델에 부정적인 영향을 미칠 수도 있다[3]. 기존 연구에서는 이러한 통계적 이질성 문제를 해결하기 위해 불균형한 분포를 유발하는 장치들을 배제하여 학습을 진행하였다[4]. 이는 기존 연합학습에 비해 향상된 성능을 보였으나 불균형한 분포를 유발하는 노드들을 완전히 제거하면 훈련 데이터셋의 전반적인 다양성이 감소할 수 있다. 또한, 학습 중에 광범위한 데이터에 노출되지 않기 때문에 새로운 상황에 대처하기 어렵다[3].

또 다른 방법은 그라디언트 압축[5]으로 네트워크 통해 전송해야 하는 기울기의 크기를 줄임으로써 이질성 문제를 해결하는 데 도움이 될 수 있다. 그라디언트 압축을 통해 장치는 더 적은 데이터로 모델을 업데이트할 수 있지만, 과도한 그라디언트 압축은 정보 손실을 유발하여 학습 품질에 부정적인 영향을 미칠 수 있기 때문에 통신 효율성과 정확성 사이에서 균형을 맞추기 위해 압축 정도를 신중하게 선택해야 한다.

기존에 가중치의 영향력을 조절하는 방법으로는 학습률[6]와 가중치 감쇠[7]가 있다. 학습률은 주로 로컬에서 중앙 서버로 가중치를 전송할 때 속도를 조절하기 위해 사용되고, 가중치 감소는 일반적으로 과적합을 막기 위해 사용되며 중앙 서버에서 가중치에 규제를 가함으로써 가중치를 정규화하는 기술이다. 해당 기술들을 통해 가중치에 영향을 줄 수 있지만 이질성을 해결하기 위해 고안된 방법이 아니기 때문에 근본적인 문제를 해결하기에는 충분하지 않다. 이러한 이유로 해당 기술들은 편향된 분포를 유발하는 노드들을 신중하게 탐지하여 영향력을 줄이기는 어렵다.



(a) 모니터링 라운드-업데이트 라운드 (b) 거리 계산 (c) 매개변수 축적 및 Average

[그림 1] 제안하는 모니터링 라운드-업데이트 라운드를 통한 개선된 연합학습의 전체 구조

Ⅲ. 모니터링 라운드-업데이트 라운드로 구성된 연합학습 개선방안

제안 기법에서는 [그림 1]에서와 같이 모니터링 라운드-업데이트 라운드를 제안하여 글로벌 모델의 일반화 능력 향상과 절감된 커뮤니케이션 오버헤드를 달성하고자 한다.

먼저 모니터링 라운드 과정이다. 학습을 진행하기 전에 중앙 서버는 모델을 랜덤하게 초기화한다. 이후 각 로컬 디바이스는 글로벌 모델을 받아 로컬의 데이터를 통해 학습을 진행한다. 학습이 완료되면 각 디바이스는 로컬 모델로부터 각자의 가중치를 추출하여 중앙 서버에 업로드한다. [그림 1]-(b)와 같이, 중앙 서버는 해당 라운드 내 가중치들의 평균을 계산한 뒤 평균값과 각 가중치의 거리를 산출한다.

$$di_{kt} = \sqrt{(x - W_{kt})^2} \quad (1)$$

x는 평균값, W_{kt}는 디바이스 k의 t번째 라운드에 해당하는 가중치를 의미한다. (1)의 연산을 수행하여 가중치 평균값과 각 가중치의 거리 di_{kt}를 얻을 수 있다. 이후 di_{kt}와 시스템 초기에 설정된 임계값을 비교하여 [그림 1]-(c)와 같이 score를 할당한다. 임계값이란 범위를 벗어나는지 여부를 판단할 수 있는 한계점에 대해서 나타낸 변수이다. di_{kt}와 임계값을 비교하여 di_{kt}가 더 크다면 편향된 데이터셋을 가지는 노드로 간주하여 낮은 S_{kt}를 부여한다. S_{kt}는 t 라운드 내 디바이스 k의 스코어를 의미한다.

모니터링 라운드가 끝나고 실행되는 업데이트 라운드는 글로벌 모델을 업데이트하고 업데이트된 글로벌 모델을 다시 로컬 디바이스로 전달한다. 업데이트 라운드에서는 그림의 Average 연산을 통해 얻은 값들을 집계한 후 글로벌 모델의 업데이트를 진행한다.

$$Avg = \frac{\sum_{k=1}^{n-1} W_{kt} S_{kt}}{n-1} \quad (2)$$

위의 식은 Average를 구하는 식으로, 모니터링 라운드를 통해 얻은 (n-1) 개의 가중치 W_{kt}와 스코어 S_{kt}를 각각 곱하여 편향된 데이터셋을 가지는 노드의 영향력을 줄이고, score가 반영된 가중치들의 평균을 계산하여 글로벌 모델의 업데이트를 수행할 값을 얻을 수 있다.

만약 극단적인 데이터가 다수를 차지하는 경우, 라운드의 가중치 평균값이 커지기 때문에 모든 노드가 임계치 이상의 값을 가지게 되어 모두 편향된 데이터셋을 가지는 노드로 여겨진다. 이런 경우에는 가장 거리가 먼 노드를 제외하고 다시 평균값을 계산하여 거리를 계산한다.

이 과정을 반복 후, 사전에 정의된 종료 조건이 만족되면 업데이트된 최종 글로벌 모델이 추출되고 연합학습은 종료된다.

Ⅳ. 결론

통계적 이질성 문제로 모델의 성능이 저하되는 문제를 해결하기 위해 본 연구에서는 모니터링 라운드-업데이트 라운드를 통해 연합학습의 성능을 개선하는 방안을 제안한다. 해당 방식을 통해 매번 업데이트하는 기존 연합학습의 커뮤니케이션 오버헤드 문제를 완화할 수 있다. 또한, 거리 기반 탐지기법을 이용하여 편향된 데이터셋을 가지는 노드의 영향력을 줄일 수 있다. 본 연구에서 제안하는 기법은 편향된 데이터셋을 가지는 노드들을 완전히 배제하지 않기 때문에 모델의 다양성을 유지하며 학습할 수 있다. 또한 새로운 데이터에 대해 정확하고 효과적으로 대응할 수 있는 모델을 훈련할 수 있다.

향후 연구에서는 편향된 데이터셋을 가지는 노드에 대한 시스템 초기 임계값 설정에 관한 연구를 진행할 예정이며, 시뮬레이션을 통해 제안하는 시스템의 효율성을 검증할 예정이다.

ACKNOWLEDGMENT

이 논문은 2020년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2020R1A2C1006497). (교신저자: 도인실)

참 고 문 헌

[1] Li, A. K. Sahu, et al. "Federated Learning: Challenges, Methods, and Future Directions," 2020.

[2] F. Angiulli, S. Basta and C. Pizzuti, "Distance-based detection and prediction of outliers," 2006.

[3] M. Aledhari, et al "Federated Learning: A Survey on Enabling Technologies, Protocols, and Applications," 2020.

[4] H. Wang, Z. Kaplan, D. Niu and B. Li, "Optimizing Federated Learning on Non-IID Data with Reinforcement Learning," 2020.

[5] XU, Chenhao, et al. "Asynchronous federated learning on heterogeneous devices: A survey.," 2021.

[6] SMITH, Samuel L., et al. "Don't decay the learning rate, increase the batch size.", 2017.

[7] LOSHCHILOV, Ilya; HUTTER, Frank. "Decoupled weight decay regularization.", 2017.