FedWPSO: Federated Learning using PSO with added Weighted Aggregation

박성환[1] · 장예슬[1] · 이재우[2]

[1] 중앙대학교 융합보안학과 [2] 중앙대학교 산업보안학과

한국정보과학회 컴퓨터시스템 소사이어티
KIISE Computer System Society

INTRODUCTION

Federated learning

- 분산형 장치 또는 서버 전반에 걸쳐 기계 학습 model을 훈련하는 접근 방식으로, communication cost를 절감하고 프라이버시와 보안성을 강화하는 방법으로 최근 활발히 연구되고 있음. [1-4]
- 데이터의 중앙 집중화 없이 다양한 로컬 장치에서 model을 training하여, 데이터의 프라이버시를 유지하고 데이터 전송량을 최소화하는 장점을 제공함.
- 프라이버시 침해 우려 없이 사용자 데이터를 효과적으로 보호하며, 중앙 서버에 대한 과도한 의존성을 줄임으로써 보안 위험을 감소시킴.
- Model의 training은 로컬에서 이루어지며, 중앙 서버로는 개선된 model parameter(or weight)만을 전송하여, 개인 데이터의 외부 노출 없이 모델을 최적화할 수 있음.
- 스마트폰이나 IoT 기기 등의 다양한 개인 장치를 활용하여, 실생활 데이터를 바탕으로 한 모델의 정밀도를 향상시키는 데 기여함.

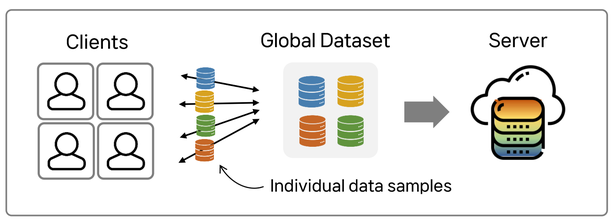

Figure 1. Centralized machine learning

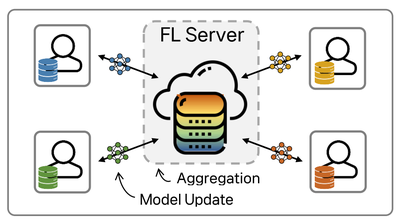

Figure 2. Federated learning

Non-IID 데이터의 특징과 문제점

- Non-IID(Non-independent and identically distributed) 데이터는 장치 간에 데이터가 동일하게 분포되지 않은 상태를 지칭하며, 분산 학습 네트워크에서 자주 발생하는 현상임. [1, 5, 6]
- Non-IID 환경에서는 사용자별 데이터의 다양성이 model training에 영향을 미쳐, model의 일반화 및 예측 성능에 부정적인 영향을 줄 수 있음.
- 다양한 사용자 행동과 맥락에 따라 수집되는 데이터의 차이는 model의 편향을 초래하고, 일부 클라이언트에 대해 overfitting 되는 경향을 나타낼 수 있음.
- 클라이언트 간의 데이터 분포 차이는 model의 training 과정을 복잡하게 하며, 이는 특히 FL에서 모델의 성능을 저하시키는 주요 요소로 작용함.
- Non-IID 데이터로 인해 FL 모델의 학습이 어려워지며, 이는 최종 모델이 실제 사용 환경에 적합하지 않을 가능성을 높임.

Personalized federated learning의 특징과 문제점

- FL에서 개인화는 사용자 개별 데이터에 최적화된 model을 생성하여 사용자 만족도를 높이고 장치 별 성능을 향상시키고자 하는 프로세스. [3, 4]
- 개별 사용자의 독특한 데이터 패턴을 반영하는 개인화된 model은 FL에서 중요한 목표이며, 사용자 경험에 맞춘 model을 생성 하는데 중요한 역할을 함.
- Model이 전역적으로 유용하면서도 로컬 장치의 특성에 맞춰 조정될 수 있도록 하는 것은 personalized FL의 중요한 고려 사항임.
- 개인화는 집단의 이익과 개별 사용자의 효과 사이의 균형을 찾는 복잡한 과정이며, 이는 사용자 중심의 model 설계에 있어 핵심적인 요소임.

EXPERIMENTS

Experimental setup

- **Client setup:** 총 20개의 학습 클라이언트를 배치. 모든 클라이언트의 학습 능력이 동일하고 최초 시작점이 동일한 homogeneous 환경을 고려하여 실험을 진행함.
- **Dataset:** CIFAR-10 [7]을 Training set 80% Test set 20% 로 분리. IID 와 Non-IID[5] 환경에서 각각 실험. 각 클라이언트에 분배된 IID와 Non-IID 데이터 분포는 Figure 5. 와 같음.
- **Training setup:** 총 50회의 communication을 진행하며, 각 round마다 전체 클라이언트의 50%만 communication에 참여함. 각 클라이언트는 communication 전 각자가 보유한 데이터로 총 5회의 local 학습을 수행함. 이 때 각 클라이언트는 LeNet5 모델을 이용하여 학습을 수행함. 이외 자세한 hyperparameter는 아래 Table 1. 참고.

Hyperparameter			
# of Client	20	Optimizer	SGD
Dataset	CIFAR-10 (IID / Non-IID)	Batch size	16
Communication round	50	Local learning rate	0.01
local training epoch	5	Non-IID Dirichlet α	0.1
Training model	LeNet5 []	PSO α, c_1, c_2	0.4, 0.6, 1.0

Table 1. Hyperparameter

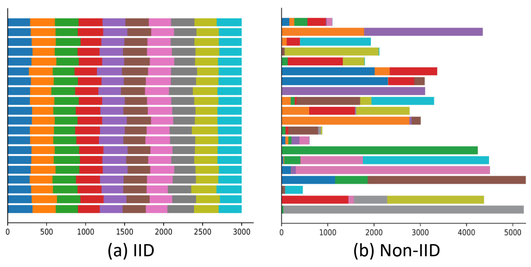

Figure 5. CiFAR-10 distribution of each client

Experimental result

- 제안하는 FedWPSO 알고리즘의 객관성을 평가하기 위해 유사한 기능을 수행하는 알고리즘 4개와 비교 평가를 수행. 그 결과는 Figure 6. 을 참고.
  FedAVG(IID/Non-IID) [1], FedPSO[2], FedPer [3], FedRep [4] 각 알고리즘에 대해 학습에 참여한 클라이언트들의 해당 라운드 test accuracy의 평균을 기반으로 학습 성능을 평가.
- FedAVG 알고리즘은 각 클라이언트가 local training을 마친 후 서버에서 학습에 참여한 클라이언트가 제공하는 학습 모델의 평균을 global model로 채택하는 전략.
  (FedAvg-iid) IID 환경에서는 비교적 안정적인 학습을 진행되지만 최대 test accuracy가 63.33%로 다른 알고리즘에 비해 낮음.
  (FedAvg) 다만 Non-IID 환경에서는 학습이 불안정한 모습을 보임.
- FedPer 알고리즘과 FedRep 알고리즘은 각 클라이언트에 맞게 개인화된 학습이 가능하도록 제안된 알고리즘으로 학습 모델 중 classifier 부분에 대해 fine tuning 하는 전략.
  (FedPer, FedRep) 두 알고리즘 모두 Non-IID 환경에서 높은 학습성능을 보여주며, 각각의 최대 test accuracy는 87.86%, 90.70%
- FedPSO 알고리즘은 각 클라이언트가 학습하기 전 PSO 알고리즘을 통해 local model을 업데이트하고, 서버에서는 학습에 참여한 클라이언트가 제공한 local best model 중 가장 성능이 좋은 모델을 global best model로 채택하고 다음 학습 시 각 클라이언트가 참고할 수 있게 배포하는 전략.
  (FedPSO) Non-IID 환경에서 각 클라이언트가 보유한 데이터의 분포가 다르나, 가장 성능이 좋은 하나의 모델을 목표로 최적화가 진행되다 보니 학습이 불안정한 모습을 보임. 다만 최대 test accuracy는 72.21%로 FedAVG에 비해 높은 성능을 보임.
- **(FedWPSO)** FedPSO 알고리즘에 비해 Non-IID 환경에서도 안정적으로 학습이 진행되며 다른 알고리즘에 비해 최대 test accuracy 91.01%로 가장 높은 성능을 보인다.

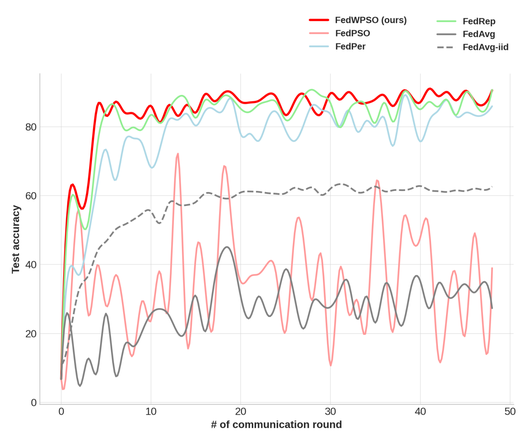

Figure 6. Test accuracy comparison

METHODS

입자군집최적화(PSO, Particle swarm optimization)

- PSO[8]는 자연계의 집단 행동을 모방한 계산 기법으로, 최적화 문제를 해결하기 위해 개발됨.
- 입자(클라이언트) 집단이 문제 해결 공간을 탐색하며 각 입자는 자신의 위치와 속도를 갖고 이동함.
- 각 입자의 움직임은 자신의 최적 위치(개인적 최고 성과)와 전체 집단의 최적 위치(전역 최고 성과)에 영향을 받음.
- PSO는 최적화를 위해 gradient가 필요하지 않으며, 매우 다양한 후보 해결책의 공간을 탐색할 수 있는 메타휴리스틱으로, 최적화 문제를 미분할 필요가 없는 고전적 최적화 방법과 대조됨.

$$W_i^{t+1} = W_i^t + V_i^{t+1}$$

$$V_i^{t+1} = \alpha V_i^t + c_1 r_1 (W_i^{pbest} - W_i^t) + c_2 r_2 (W_i^{gbest} - W_i^t)$$

α, c_1, c_2 : Hyperparameter for PSO
r_1, r_2 : Random floats between 0 to 1
$pbest, gbest$: Particle best, Global best

Figure 3. Particle swarm optimization algorithm

FedPSO: PSO를 활용한 Federated learning

- FedPSO [2]는 FL에 PSO의 개념을 융합하여 FL의 통신 효율성 및 학습 성능을 개선함.
- FL 클라이언트들은 종종 제한된 통신 대역폭을 가지며, 서버와 클라이언트 간의 통신은 성능 향상을 위해 최적화 되어야 함.
- 기존 FL 알고리즘들은 global model 집계를 위해 많은 양의 학습 가중치를 전송 및 수신하기 때문에 불안정한 네트워크 환경에서 정확도가 크게 저하될 수 있음.
- FedPSO는 불안정한 네트워크 환경에서의 견고성을 향상시키기 위해 대량의 가중치 대신 점수 값을 전송함.
- FedPSO를 적용하면 네트워크 통신에서 사용되는 데이터의 양이 크게 감소하면서도 글로벌 모델의 정확도가 9.47% 향상됨.

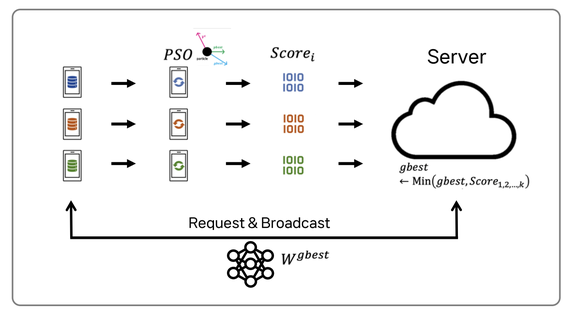

Figure 4. FedPSO algorithm

Proposed method: FedWPSO

- 본 연구에서 제안하는 알고리즘으로 FedPSO에 개인화 및 집계 가중치 개념을 융합함.

  Algorithm pseudocode:

  1. 서버에서 초기 global model 가중치 W^0 초기화
  2. 각 라운드 t에서 모든 클라이언트 k가 병렬로 ClientUpdate 함수를 수행하도록 명령
  3. ClientUpdate 함수 내에서, 클라이언트는 로컬 데이터 D_k를 사용하여 local model을 업데이트
  4. Local training이 완료된 후 PSO 알고리즘을 통해 local model을 개인화하며, local model 중 가장 높은 성능을 보였던 모델 W_{pbest}를 서버로 반환
  5. 모든 클라이언트의 학습이 완료된 이후 서버에서는 WeightedAggregation 함수를 수행하여 $t+1$ 시점의 W_{gbest}^{t+1}을 생성
  6. WeightedAggregation 함수는 각 클라이언트의 데이터 크기 D_k에 비례하여 수집된 W_k^{t+1}에 가중치를 부여

- 이러한 방식을 통해 FedWPSO는 각 클라이언트의 데이터에 대해 개인화된 model을 유지하면서도, 전체 네트워크를 통해 학습된 지식을 공유하고, 각 클라이언트의 데이터 크기에 기반한 가중치를 통해 더 정확하고 공정한 model 집계를 달성함.

Algorithm 1 FedWPSO Algorithm

Server executes:
  initialize W^0

  for each round $t = 1, 2, \ldots$ **do**
    for each client k **in parallel do**
      $W_k^{t+1} \leftarrow$ **ClientUpdate**(W^{gbest})
    end for
    $W^{gbest} \leftarrow$ **WeightedAggregation**(W^{t+1})
  end for

Function: ClientUpdate(W^{gbest}) **//Run on client** k
  initialize $V^0, \alpha, c_1, c_2, r_1, r_2$
  $\beta \leftarrow$ (split D_k into batches of size B)
  $W_c^t \leftarrow$ (only *classifier* layers in W^t)

  for each client epoch i from 1 to E **do**
    for batch $b \in B$ **do**
      $W^{t+1} \leftarrow W^t - \eta \nabla l(W^t; b)$
    end for
  end for
  $V^{t+1} \leftarrow \alpha \cdot V^t + c_1 \cdot r_1 \cdot (W_c^{pbest} - W_c^t) + c_2 \cdot r_2 \cdot (W_c^{gbest} - W_c^t)$
  $W^{t+1} \leftarrow W_{\forall \setminus c}^{t+1} + W_c^{t+1} + V^{t+1}$
  if $S^{pbest} > \nabla l(W^t; D_k^{est})$ **then**
    $W^{pbest} \leftarrow W^{t+1}$
  end if

  return W^{pbest}

Function: WeightedAggregation(W^{t+1})
  initialized W_{agg}
  for each client $k = 1, 2, \ldots$ **do**
    $W^{agg} \mathrel{+}= \frac{D_k}{D} W_k^{t+1}$
  end for
  $W^{gbest} \leftarrow \frac{W^{agg}}{k}$
  return W^{gbest}

CONCLUSION

연구 요약

- 본 연구는 Non-IID 데이터 상황에서의 FL 학습 시 발생할 수 있는 문제를 해결하고자 수행됨.
- FL 학습 과정에 입자 군집 최적화(PSO)와 가중치 집계를 결합한 새로운 알고리즘 FedWPSO를 제안함.
- FedWPSO 알고리즘을 적용한 FedWPSO는 각 클라이언트 보유한 데이터의 분포가 서로 상이한 경우에도 안정적으로 학습을 수행할 수 있으며, 각 클라이언트가 갖고 있는 데이터의 특성을 반영한 개인 맞춤형 모델을 생성하는데도 좋은 성능을 보여줌.

실험 결과

- 실험에서 FedWPSO는 기존 FedAVG, FedPSO, FedPer, FedRep 등의 알고리즘과 비교했을 때 높은 정확도와 안정성을 달성.
- 특히 Non-IID 데이터 환경에서 이 알고리즘이 뛰어난 성능을 보여주었으며, 최대 91.01%의 test accuracy를 기록.
- 이러한 결과는 FL의 real-world 적용 가능성을 높임.

연구 한계

- 이 연구는 특정한 데이터 분포와 네트워크 조건에 초점을 맞추고 있어, 다양한 실제 환경에서의 적용성에 대한 한계 존재.
- 특히, 각 클라이언트 간의 학습 능력이 상이한 heterogeneous 환경이나 악의적인 참여자에 의한 공격이 발생하는 환경에서의 성능은 아직 충분히 검증되지 않았습니다.
- 또한, 충분히 많은 수의 클라이언트를 고려하지 못해 실제 학습 환경에 대한 고려가 부족함.

향후 발전 방향

- 이 연구의 결과를 바탕으로, heterogeneous 환경과 공격에 취약한 네트워크 환경을 고려한 추가적인 실험과 개선이 필요.
- 향후 연구는 FedWPSO의 범용성을 확장하고, 데이터 프라이버시 보호와 통신 효율성을 더욱 강화하는 방향으로 진행할 수 있음.
- 이러한 개선을 통해 FL의 적용 범위가 확장되고, real-world 데이터를 효과적으로 처리하는 능력이 향상될 것으로 기대.

REFERENCES

[1] McMahan, Brendan, et al. "Communication-efficient learning of deep networks from decentralized data." Artificial intelligence and statistics. PMLR, (2017).

[2] Park, Sunghwan, Yeryoung Suh, and Jaewoo Lee. "FedPSO: Federated learning using particle swarm optimization to reduce communication costs." Sensors 21.2 (2021): 600.

[3] Arivazhagan, Manoj Ghuhan, et al. "Federated learning with personalization layers." arXiv preprint arXiv:1912.00818 (2019).

[4] Collins, Liam, et al. "Exploiting shared representations for personalized federated learning." International conference on machine learning. PMLR, (2021).

[5] Hsu, Tzu-Ming Harry, Hang Qi, and Matthew Brown. "Measuring the effects of non-identical data distribution for federated visual classification." arXiv preprint arXiv:1909.06335 (2019).

[6] Yuan, Honglin, et al. "What do we mean by generalization in federated learning?." arXiv preprint arXiv:2110.14216 (2021).

[7] Krizhevsky, Alex, and Geoffrey Hinton. "Learning multiple layers of features from tiny images." (2009): 7.

[8] Kennedy, James, and Russell Eberhart. "Particle swarm optimization." Proceedings of ICNN'95-international conference on neural networks. Vol. 4. IEEE, 1995.