클러스터 헤드 기반 계층적 프롬프트 연합 학습 구조 설계 및 QKD 를 이용한 보안 강화 방안 논의

박지원, 이주형

가천대학교
pich7755@gachon.ac.kr, j17.lee@gachon.ac.kr

Design of Cluster Head-based Hierarchical Federated Prompt Learning and Discussion on Security Enhancement using Quantum Key Distribution

Jiwon Park, Joohyung Lee
Gachon Univ.

요 약

최근 파운데이션 모델의 발전과 함께, 연합 학습 환경에서 사전 학습된 모델의 프롬프트만을 학습하는 Federated Prompt Learning (FPL) 방식이 통신 효율성 측면에서 주목받고 있다. 하지만 클라이언트 수가 증가함에 따라 중앙 서버의 통신 및 연산 부하가 병목 현상을 야기하여 확장성에 한계를 가진다. 본 논문에서는 이러한 문제를 해결하기 위해 클러스터 헤드를 중간 계층으로 두는 계층적 FPL 구조를 제안한다. 제안된 구조는 클러스터 헤드에서 1 차적인 프롬프트 집계를 수행하고, 중앙 서버는 클러스터 헤드의 결과만을 집계하여 중앙 서버의 부하를 크게 줄이고 시스템 확장성을 향상시킨다. 또한 본 연구는 통신 효율성 개선 효과를 중심으로 분석하고, 향후 양자 키 분배(Quantum Key Distribution, QKD) 기술을 활용하여 계층 간 프롬프트 전송 보안을 강화할 수 있는 방안에 대해 논의한다.

Ⅰ. 서 론

통신 대역폭이 제한적인 모바일 및 엣지 환경에서 연합 학습(Federated Learning, FL)에서는 통신 효율성이 중요한 고려 사항이다. 이러한 연합 학습 환경에서 사전 학습된 대규모 파운데이션 모델의 프롬프트만을 학습하고 교환하는 Federated Prompt Learning (FPL) 방식은 통신 효율성 면에서 큰 장점을 보인다[1]. 하지만 참여 클라이언트 수가 증가할 경우, 모든 프롬프트 업데이트가 중앙 서버로 집중되어 통신 병목 및 연산 부하로 인한 확장성 한계에 직면하게 된다.

때문에, 본 논문에서는 FPL 의 확장성 한계 극복과 통신 효율성 향상을 위해 클러스터 헤드 또는 엣지 서버를 중간 집계 계층으로 도입하는 계층적 FPL 구조를 제안한다.

제안 구조는 클러스터 헤드가 자신의 클러스터에 속하는 클라이언트들의 프롬프트 업데이트를 1 차적으로 집계하고, 중앙 서버는 클러스터 헤드로부터 집계된 결과만을 받아 2 차 집계를 수행한다.

이러한 2 단계 분산 집계 방식을 통하여 중앙 서버의 부하를 효과적으로 줄여 시스템 전체의 확장성을 향상시키는 것을 목표로 한다.

본 연구는 제안하는 계층적 FPL 구조의 설계 및 구현 방안을 제시하고, 통신 효율성, 특히 중앙 서버 부하 감소 효과를 중심으로 분석한다. 더불어, 보안이 중요한 연합 학습 환경에서 양자 키 분배(Quantum Key Distribution, QKD) 기술을 활용하여 계층 간 프롬프트 전송의 보안을 강화할 수 있는 가능성에 대해 논의한다[2].

Ⅱ. 본론

그림 1 은 본 논문에서 제안하는 계층적 FPL 시스템의 전체 아키텍처를 보여준다. 본 시스템은 크게 클라이언트, 클러스터 헤드, 그리고 중앙 서버의 3 개 계층으로 구성되어, 프롬프트 집계 과정을 2 단계로 분산시켜 중앙 서버의 부하를 줄이고 시스템 확장성을 향상시키는 것을 목표로 한다.

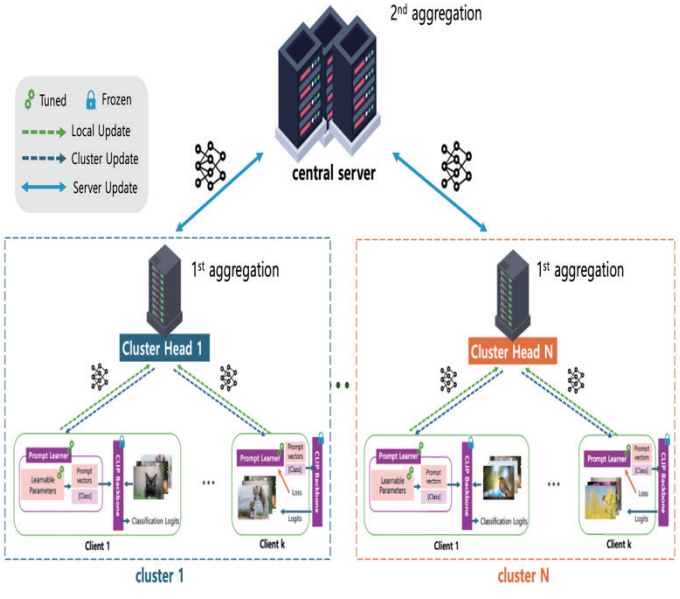

그림 1. 클러스터 기반 계층적 FPL 의 프레임워크

가. 프롬프트 학습

파운데이션 모델을 특정 작업에 적용하기 위한 주요 기법 중 하나는 프롬프트 학습이며, 이는 파라미터 효율적 미세조정 방식에 속한다. 이 접근법은 거대한 사전 학습 모델의 가중치는 대부분 변경하지 않고 고정시킨 상태에서, 모델의 입력 임베딩 공간에 학습 가능한 소수의 연속적인 벡터를 추가하여 이를 목적작업에 맞게 최적화한다. 이러한 프롬프트 학습은 모델 전체를 미세조정하는 것에 비해 학습해야 할 파라미터 수가 현저히 적어 학습 시간과 메모리 요구량을 크게 줄일 수 있으며, 특히 본 제안 기법과 같이 학습된 프롬프트만을 교환하는 연합 학습 환경에서 통신 효율성을 극대화하는 핵심적인 역할을 수행한다.

나. 클러스터 헤드 기반 계층적 집계

기존 FPL 방식의 중앙집중식 집계로 인한 확장성 한계를 극복하기 위해, 본 논문은 클라이언트와 중앙 서버 사이에 클러스터 헤드라는 중간 집계 계층을 도입하는 클러스터 기반의 계층적 구조를 도입하였다. 이 구조에서 클라이언트는 로컬 학습 후 업데이트된 프롬프트 벡터를 중앙 서버가 아닌 자신이 소속된 특정 클러스터 헤드로 전송한다. 각 클러스터 헤드는 담당 클라이언트 그룹으로부터 수신한 프롬프트 벡터들의 1 차 평균 집계를 수행하여 클러스터 레벨 대표 프롬프트를 생성한다.

이후, 중앙 서버는 모든 클라이언트가 아닌, 훨씬 적은 수의 클러스터 헤드로부터 이 집계된 대표 프롬프트들만을 수신하여 최종적인 2 차 글로벌 집계를 수행한다. 이러한 2 단계 분산 집계 방식은 중앙 서버로 집중되는 통신 트래픽과 연산 부하를 클러스터 헤드 수(M)에 비례하는 수준으로 크게 감소시켜(기존 N 대비, M << N), 시스템 전체의 병목 현상을 완화하고 대규모 클라이언트 환경에서의 확장성을 획기적으로 향상시킨다.

이러한 계층적 구조에서 다중 계층 간 프롬프트 전송 과정에서의 보안은 반드시 고려되어야 한다. 학습된 프롬프트 정보의 유출 및 변조를 방지하기 위해, 본 연구는 향후 양자 키 분배(QKD) 기술의 적용 가능성을 탐색한다. QKD 는 통신 당사자 간에 정보이론적으로 안전한 비밀 키를 분배하는 기술로, 제안된 구조에서는 QKD 를 활용하여 (1) 클라이언트-클러스터 헤드 간, (2) 클러스터 헤드-중앙 서버 간의 안전한 통신 채널을 구축할 수 있다. 각 링크에서 QKD 로 생성된 세션 키를 공유하고, 이를 대칭키 암호화와 결합하여 프롬프트 관련 데이터를 암호화하여 전송함으로써, 통신 과정에서의 기밀성과 무결성을 크게 향상시킬 수 있다.

다. 성능 분석

본 절에서는 제안하는 클러스터 기반 계층적 FPL 구조의 실질적인 효과와 타당성을 검증하기 위해 수행한 시뮬레이션 결과를 심층적으로 분석한다. 주요 평가 지표는 두 가지로 구성된다. 첫 번째는 통신 효율성으로, 클라이언트 수가 증가하는 다양한 시나리오에서 제안된 계층적 구조가 기존 2 계층 FPL 방식 대비 중앙 서버의 통신 부하를 얼마나 효과적으로 감소시키는지를 정량적으로 측정한다. 이때, 기준으로 감소율을 산출하여 시스템의 확장성을 평가한다. 두 번째는 모델 학습 성능으로, 이는 클라이언트 수와 클러스터 헤드의 수(C)를 변화시켜가며 각 구성에서의 최종 글로벌 테스트 정확도를 비교 분석함으로써 이루어진다.

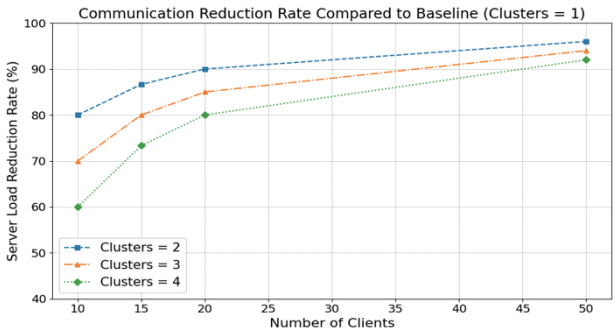

그림 2. 클라이언트 수 증가에 따른 중앙 서버 통신 부하 감소율 변화

#클라이언트 수	글로벌 테스트 정확도			
	c = 1	c = 2	c = 3	c = 4
20	80.5	83.6	83.3	81.7
50	89.6	89.5	88.5	88.7

표 1. 클라이언트와 클러스터 수에 따른 모델 성능 비교

그림 2 에서 제안된 계층적 구조가 모든 클러스터 구성에서 높은 통신 부하 감소 효과를 나타냈으며, 50 명으로 증가 시 클러스터 2 개 구성은 약 95%까지 통신 부하를 절감하여 뛰어난 확장성을 입증했다.

표 1 은 모델 성능을 비교한 결과이다. 클라이언트 20 명 환경에서는 클러스터 2 개 구성이 베이스라인보다 우수한 성능을 보였으며, 클러스터 수와 클라이언트 수가 증가한 상황에서도, 제안된 계층 구조는 베이스라인 대비 정확도 차이가 1%p 내외로 작아 거의 동등한 수준의 성능을 보여준다. 이는 앞서 분석한 통신 부하의 획기적인 감소 효과를 고려할 때, 제안 방식이 성능 손실 없이 뛰어난 효율성을 달성할 수 있음을 시사한다.

Ⅲ. 결론

본 논문은 기존 FPL 의 확장성 한계를 개선하고자 클러스터 헤드를 도입한 계층적 구조를 제안했다. 실험 결과, 제안된 2 단계 분산 집계 방식은 중앙 서버의 통신 부하를 베이스라인 대비 최대 95%까지 획기적으로 감소시키면서도, 모델의 최종 정확도는 유사한 수준으로 유지함을 확인했다. 이는 제안 구조가 대규모 환경에서의 통신 효율성 및 시스템 확장성을 크게 향상시킬 수 있음을 시사한다. 향후 QKD 기술을 접목하여 보안성을 강화한다면, 제안 구조의 실용성은 더욱 높아질 것으로 기대된다.

ACKNOWLEDGMENT

본 연구는 한국과학기술정보연구원(KISTI)의
위탁연구개발과제로 수행한 것입니다.
(과제번호 K25L5M2C2/P25030)

참 고 문 헌

[1] Guo, Tao, et al. "Promptfl: Let federated participants cooperatively learn prompts instead of models- federated learning in age of foundation model." *IEEE Transactions on Mobile Computing* 23.5 (2023): 5179-5194.

[2] Gisin, Nicolas, et al. "Quantum cryptography." *Reviews of modern physics* 74.1 (2002): 145.