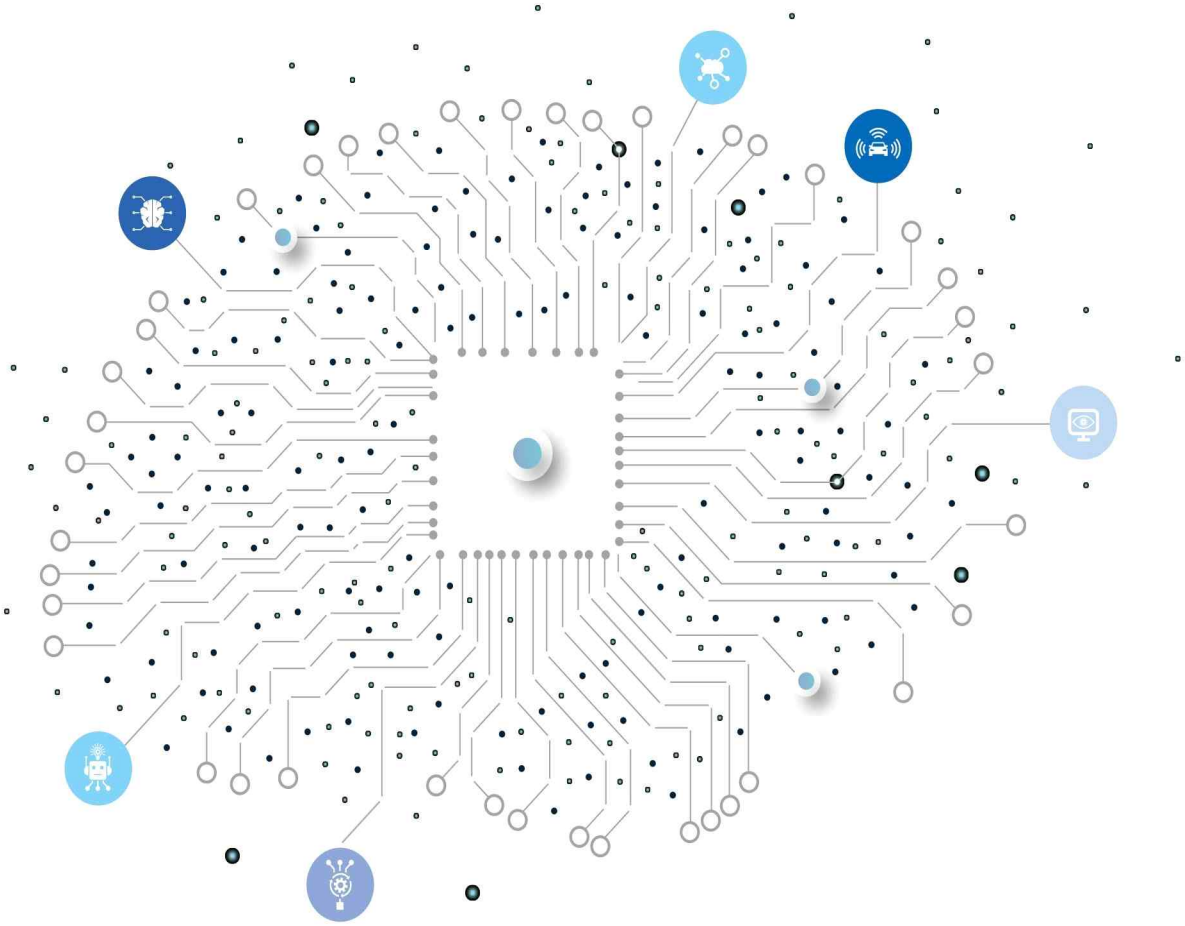
AI Network Lab
INSIGHT
Vol.4
(2021.04)



엣지 컴퓨팅을 위한 분산 AI학습 구조

: 연합 학습과 민주화 학습을 중심으로

| 작 성 | 경희대학교 홍 충 선 (cshong@khu.ac.kr)

NIA 한국지능정보사회진흥원
NATIONAL INFORMATION SOCIETY AGENCY

o 『AI Network Lab 인사이트』는 인공지능, 클라우드, 5G 등 4차 산업혁명의 핵심인 지능정보기술과 네트워크 신기술에 대한 동향을 간략하고 심도 있게 분석한 보고서입니다.

o 본 연구보고서는 과학기술정보통신부의 방송통신발전기금조성사업, 한국지능정보사회진흥원의 초연결지능형연구개발망 구축·운영사업의 연구과제 결과이며, 한국지능정보사회진흥원/한국능률협회와 공동 기획하였습니다.

발 행 처 한국지능정보사회진흥원

발 행 인 문용식

기 획 한국지능정보사회진흥원 지능형인프라본부 미래네트워크센터

보고서 온라인 서비스 www.nia.or.kr

Contents

보고서 주요 내용

Ⅰ. AI기술과 분산학습 소개

오늘날 인공 지능(AI)기술은 챗봇, 임상의사결정지원시스템, 자동화 시스템, 로봇제어, 자율자동차, 사이버 보안, 네트워크 최적제어, 비즈니스 처리 등 사회 전 분야에 걸쳐 해결하기 어려운 복잡한 문제들을 성공적으로 해결할 수 있을 만큼 성능의 우수성을 인정받고 있다. 인터넷서비스의 기반이 되는 네트워크 도메인에서는 폭증하는 데이터 서비스 수요를 충족시키기 위해 도입된 다양한 이종 네트워크(Heterogeneous Networks)가 도입되었으며 이 같은 네트워크의 대역폭, 채널상태, 에너지 등 자원을 효율적으로 관리하는 것이 주요한 이슈로 떠오르고 있다. 이에 기존의 모델 중심(Model-Driven) 접근 방식으로는 복잡한 네트워크의 자원을 최적으로 관리하는데 있어 한계에 부딪히게 되었고 이를 대처하기 위해 연구자들은 AI 기반 지능형 의사결정 솔루션이 좋은 대안이 될 것으로 여기고 이에 대한 연구개발에 몰두하고 있다.

기존 기계학습(machine learning: ML) 프레임워크는 모든 클라이언트 노드가 중앙 클라우드에 데이터를 전송하여 중앙에서 모델을 학습시키고 클라우드 서버로 부터의 모델 업데이트 결과를 클라이언트가 전송받는 중앙 집중형 구조로 되어 있다. 하지만, 최근 기존 기계학습 프레임워크에서 클라이언트의 데이터 프라이버시에 대한 우려가 높아지면서 연합 학습(federated learning) 프레임워크(FL) [1], [2], [3], [4], [5], [6]와 같은 분산 AI학습 구조(architecture)에 대한 관심이 높아지고 있다. 따라서 기존 중앙 집중형 학습을 수행하는 것이 아니라, 데이터 프라이버시 문제 해결 및 개인 맞춤형 서비스 제공을 위하여 각 디바이스에서 복잡한 학습을 공동으로 수행할 수 있는 대규모 분산 AI 학습 구조가 필요하다. 이러한 요구사항을 충족시키기 위해 고안한 연합학습의 핵심 아이디어는 클라이언트의 학습 데이터를 타 엔티티(클라우드, 학습에 참여하는 다른 디바이스)와 공유할 필요 없이 로컬 기계학습 모델을 활용하여 온-디바이스(On-Device) 학습을 수행하는 것이다.

Android의 Gboard 모바일 키보드, QuickType 키보드, iOS의 Siri용 음성 분류기, 자동 음성 인식(ASR)과 같은 기존 온-디바이스(on-device) 애플리케이션들은 개인 데이터를 통해 AI 기반 맞춤 서비스를 제공하고 있다. 일반적으로 서

비스 제공자는 사용자의 연락처 정보, 인터넷 검색 기록, 자주 방문한 주소, 키보드 입력 기록을 통한 사용 문장 패턴, 방문 웹 페이지 및 열람 뉴스기사 목록 등과 같은 민감한 개인 정보를 수집해야 한다. 따라서 이러한 온-디바이스 ML 애플리케이션은 주로 사용자 경험을 높여 줄 뿐만 사용자 별 특화된 맞춤형 서비스를 제공할 수 있게 해준다. 이와 관련하여 본 보고서에서는 대규모 분산 및 민주화 학습 시스템을 구축하기 위한 기본 원칙과 함께 우리 사회의 의견 수렴 모델에 기반한 민주화 학습 (Democratized AI: Dem-AI) 구조 [7], [8]를 제시한다. 이 같은 Dem-AI의 기본 원리와 추구하는 방향성에서 영향을 받아, 병합 군집 (Agglomerative Clustering), 계층적 일반화(Hierachical Generalization) 및 개인화(Personalized)된 학습 메커니즘을 기반으로 하는 자율 조직화 계층구조 메커니즘으로 구성된 새로운 분산 학습 접근 방식을 설명하고자 한다. 이 같은 AI구조는 네트워크 자원관리를 위한 최적 학습모델 도출 및 적용에 활용이 가능하다.

네트워크 산업은 그동안 지속적으로 사용자에게 향상된 통신 속도와 향상된 네트워킹서비스를 제공하며 발전해 오고 있다. 6세대 이동 통신 (6G)는 5세대 이동 통신 (5G)이 제공하는 빠른 "연결(connectivity)"의 개념에서 "연결된 지능"의 개념으로의 전환을 약속하는 5G의 후속 모델이다 [9]. 실제로 6G는 언제 어디서나 데이터를 효율적으로 수집·통신·분석해 혁신적이고 지능적인 서비스를 구축하기 위해 첨단화된 인공지능 기반 기능을 포함할 것으로 예상된다. 이와 같은 방향으로 발전하기 위해서는 6G를 유비쿼터스 AI의 개념과 결합함으로 데이터, 디바이스 또는 애플리케이션 중심에서 네트워킹의 다양한 측면을 인간 중심적으로 바꾸어 갈 수 있다. 하지만 중앙 클라우드 기반 서버 아키텍처를 기반으로 하는 전통적인 기계학습 설계로는 유비쿼터스 AI서비스의 꿈을 이루기가 용이하지 않다. 따라서 학계와 연구소, 그리고 각 AI기업의 학습모델 생성 관련 연구방향은 로컬 데이터를 전송할 필요 없는 분산형 기계학습 프레임워크로 점차적으로 이동하고 있다.

본 이슈보고서에서는 AI학습구조로서의 분산학습 시스템 기반 네트워킹을 위해 적용 가능한 연합학습, 민주화학습에 대해 상세히 소개한다. 또한 엣지 컴퓨팅에 활용 가능한 AI구조를 제시하고 이와 관련된 연구 토픽들에 대해서도 다룬다.

Ⅱ. 분산 학습 구조 개요

그림1의 기존의 분산기계학습(distributed machine learning) 또는 파라미터 서버 프레임워크(parameter server framework)[3]는 학습 성능을 개선하고 입력 데이터크기를 확장하기 위한 다중 노드 기계학습 접근 방식이다. 분산학습과 연합학습의 주요 차이점에 대해 논하면, 분산 접근 방식은 로컬 데이터를 수집하고 로컬에서 학습 모델을 훈련하고 학습 매개변수를 서버로 전송하고 파라미터 서버는 서버가 수신한 각 클라이언트 노드의 학습 매개변수를 이용하여 글로벌 모델을 도출한다. 이 글로벌 모델이 각 클라이언트에 전송되지 않는다는 측면에서 연합학습 모델과 다르다.

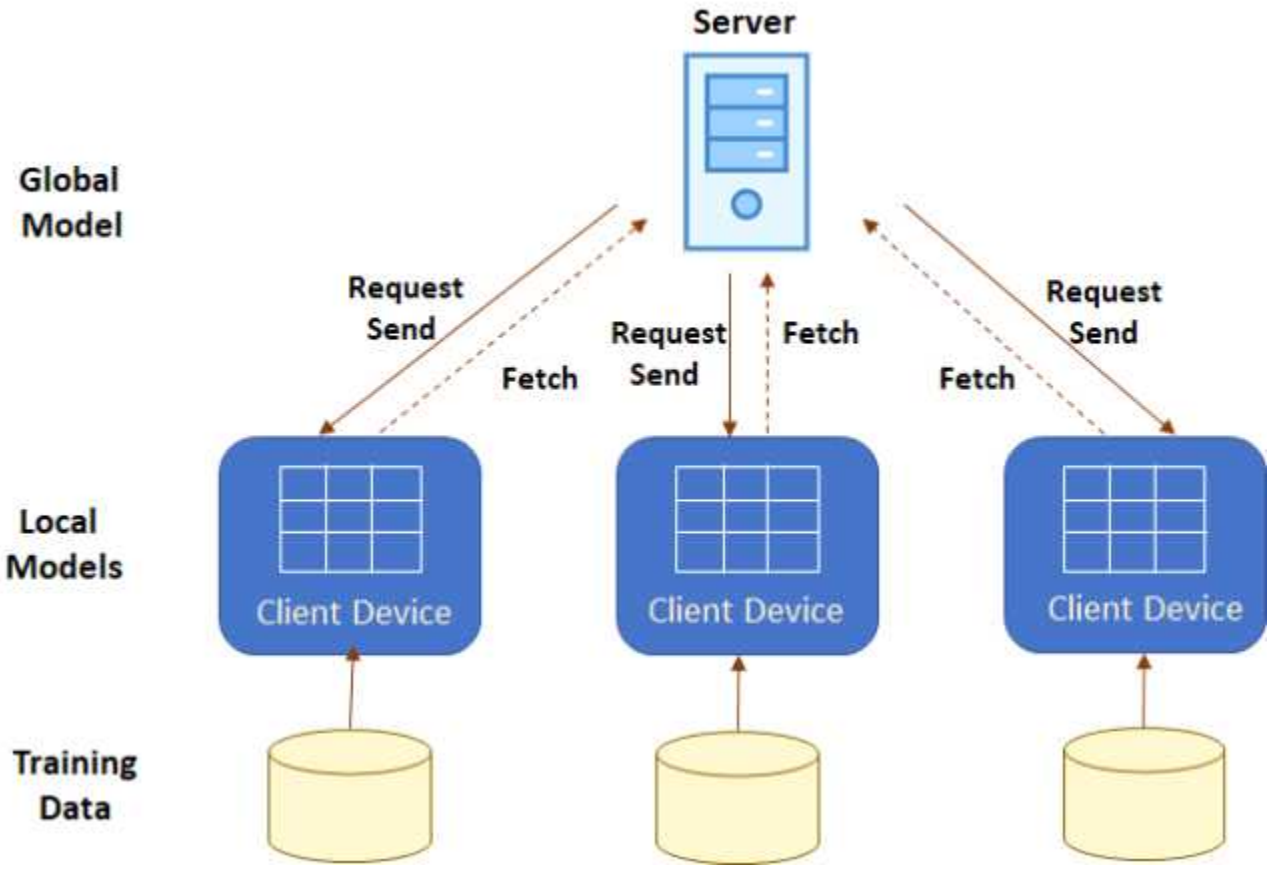


그림 1. 기존 분산 학습 구조

2.1 연합 학습 (federated learning)

연합학습(federated learning)은 클라이언트라고 하는 다수의 디바이스에 의해 기계학습모델을 반복훈련 시켜 훈련 결과를 협력적으로 통합하는 분산기계학습

접근법이다. 연합학습[1]은 글로벌 학습모델을 구축하기 위해 로컬 모델을 통합하는 역할을 하는 중앙 서버로 학습에 참여하는 다수의 모바일 기기가 온-디바이스 학습을 통해 학습된 로컬모델을 공유하는 분산 학습 프레임워크이다. 또한 연합학습에는 중앙 서버가 반복적으로 학습된 모델의 평균을 사용하여 각 디바이스의 확률적 경사값(stocasitc gradient)을 통합하는 Federated Averaging (FedAvg) 학습 알고리즘이 사용된다. 연합학습 구조는 하나의 중앙 서버(파라미터 서버)와 클라이언트 집합으로 구성되며, 각 클라이언트는 고유한 로컬 데이터셋을 가지고 있다. 연합학습이 시작되면 학습에 참여하기 위한 클라이언트 집합이 선택되고 로컬 학습을 위하여 중앙 서버로부터 글로벌 모델의 가중치(Weight) 정보가 공유된다. 글로벌 모델의 가중치가 공유되면 각 클라이언트는 자체 CPU 및 에너지 자원을 사용하여 공유 매개변수를 기반으로 로컬 데이터셋에서 로컬 모델 학습을 수행한다. 그 다음 각 클라이언트는 로컬 데이터셋으로 학습된 로컬 모델의 가중치를 파라미터 서버로 전송하고, 파라미터 서버는 현재 글로벌 모델과 로컬 모델 업데이트를 통합하여 새로운 글로벌 모델를 생성한다. 이 프로세스는 글로벌 모델이 특정 정확도 수준에 도달할 때까지 파라미터 서버와 클라이언트들 간 몇 번의 반복(communications rounds 라고 함) 작업이 수행된다. 요약하면 연합 학습 시나리오는 로컬 모델 업데이트와 글로벌 모델 통합이라는 두 가지 주요 단계로 구성된다. 로컬 모델 업데이트 단계는 로컬 데이터에 대한 기본 손실 함수(loss function)를 최소화하기 위해 클라이언트 장치에 의한 경사하강(gradient descent)을 계산하는 과정을 말한다. 글로벌 통합(global aggregation)은 서버가 서로 다른 클라이언트 장치로 부터 업데이트된 모델 매개 변수를 수집한다. 이러한 매개 변수를 통합한 다음 클라이언트로 다시 보내는 단계를 수행한다. 최근 머신러닝 연구자들은 학습 성능개선, 차등 개인정보보호(differential privacy), FedAvg 알고리즘의 보안을 강화시키기 위해 새로운 학습 알고리즘개발에 많은 노력을 기울이고 있다. 그림2는 엣지 컴퓨팅 분야에 적용 가능한 연합학습 시나리오와 연합학습 애플리케이션의 예를 나타내고 있다.

그림 3은 연합학습과 관련된 주요 여섯 가지 도전과제를 나타낸다. 이 같은 주요 도전과제를 주제로 하여 발표된 논문조사 결과 통계 관련 이슈 해결과 통신

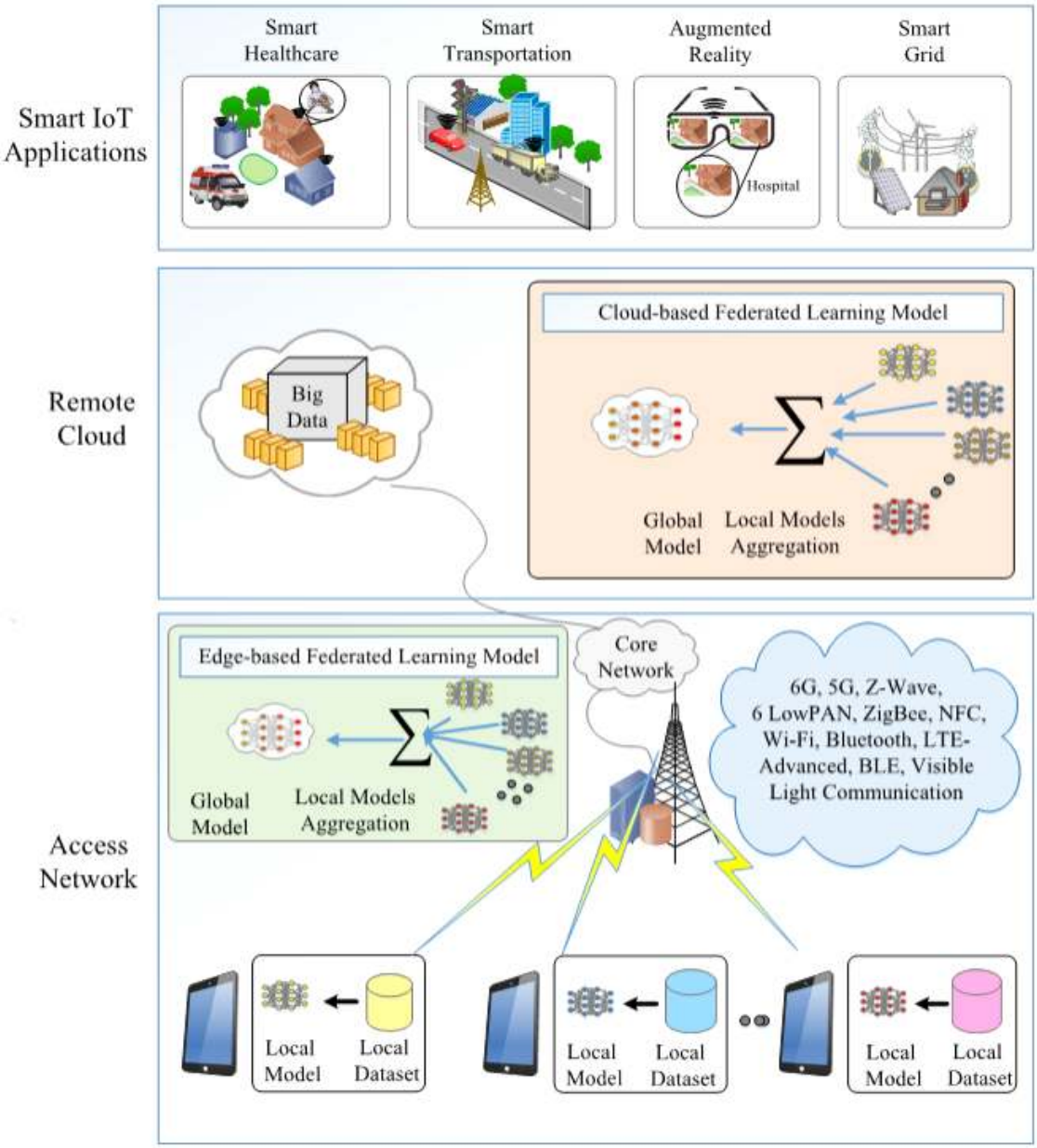


그림 2. 엣지 컴퓨팅에서의 연합학습과 응용 예

효율성을 높이기 위한 연구가 가장 많이 수행되었음을 알 수 있다 통계관련 연구는 사용자 데이터의 Non-IID(Non-Independent and Identically Distributed) 특성, 즉 훈련집합과 시험집합이 동일한 확률분포구조가 아닌 특성 때문에 발생하는 문제를 해결하기 위한 많은 연구가 이루어졌음을 알 수 있다. 이 같은 문제는 각 로컬 디바이스가 서로 다른 클라이언트의 데이터를 수집함으로써 데이터의 크기, 특징 및 목표 등급 분포가 서로 다르기 때문에 발생한다. 연합학습에서 Non-IID 데이터의 세 가지 특성인 클래스 불균형, 데이터 분포 불균형, 데이터 크기 불균형에 의해 학습 효율이 저하될 수 있다. 클래스 불균형은 한 클

래스에 속한 인스턴스 수가 다른 클래스에 속하도록 분류된 인스턴스 수보다 훨씬 높을 때 발생한다. 분포 불균형은 수집되는 데이터의 특징(Feature) 분포가 클라이언트마다 다르기 때문에 발생한다. 연합학습에서는 클라이언트의 훈련 데이터 크기의 상이 때문에 발생하는 크기 불균형의 경우가 일반적으로 발생한다. 데이터 증강(dada augmentation), 능동 학습(active learning), 멀티 태스크 학습, 전이 학습, 클라이언트 클러스터링과 같은 최신 머신러닝기술은 이러한 다양한 유형의 불균형 환경에서의 학습에 도움이 될 수 있는 기술이다. 또한 모델 이질성 연구는 각 클라이언트에서 공통 학습모델을 사용하기보다 클라이언트별 서로 다른 학습모델을 적용하는 시도이다. 이러한 이질적 특성 환경에 대처하기 위해 연합학습에 지식증류(knowledge distillation) 및 메타학습(meta learning) 기술이 적용될 수 있다.

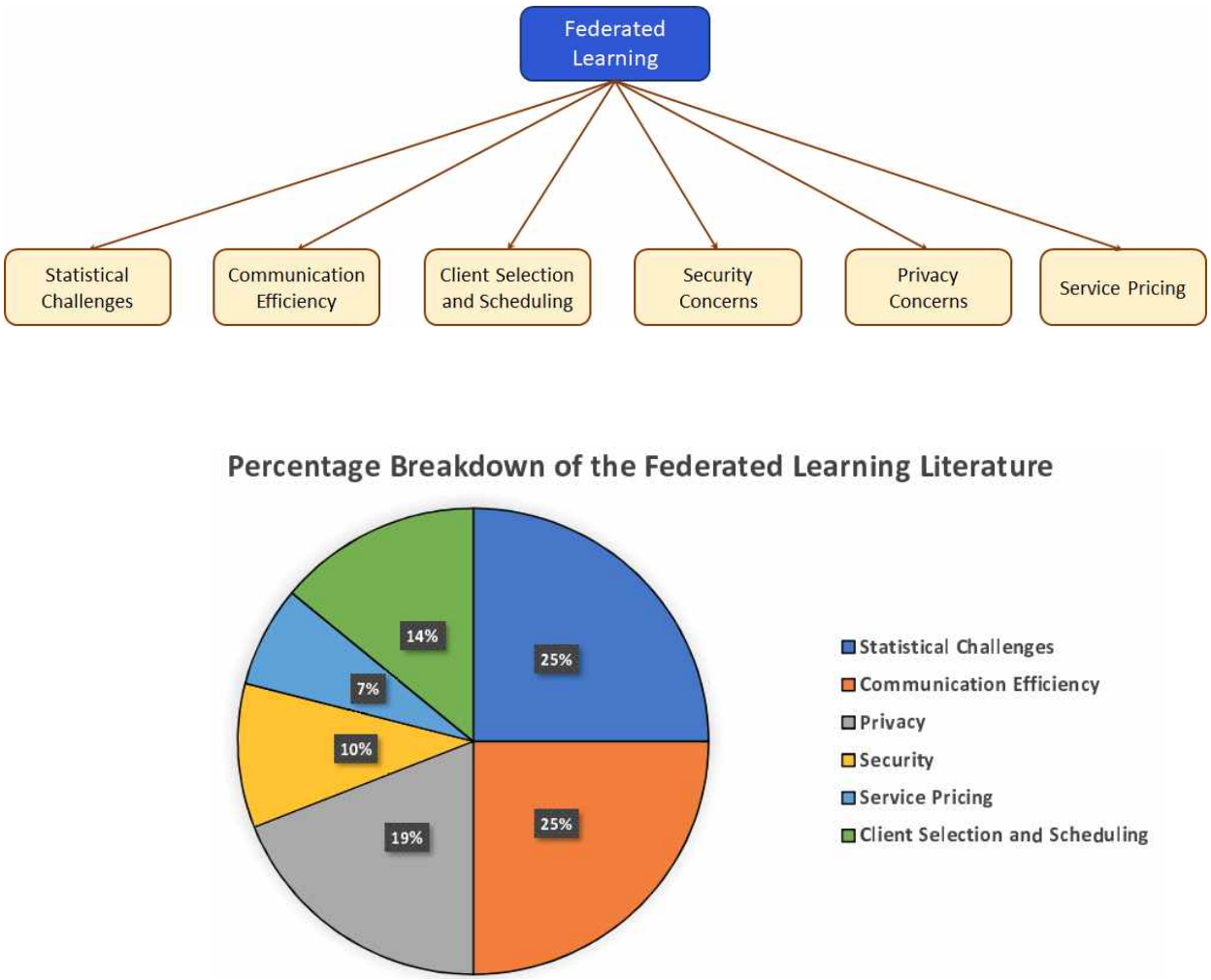


그림 3. 연합학습의 연구주제 분류

2.2 민주화 학습(democratized learning) 구조

연합학습과는 달리, 제안된 민주화 학습(democratized learning)의 철학[7]은 생물학적 지능의 일반화(generalization) 및 전문화(specialization)능력, 대규모 학습 시스템에서 복잡한 과제를 해결하기 위한 사회 및 집단 지성 시스템의 계층 구조를 갖는 분산학습 프레임워크를 말한다. 즉, **민주화 머신러닝 구조(architecture)는 계층구조를 갖는 분산학습시스템으로 보다 많은 클라이언트가 참여하여 채택한 학습모델이 상대적으로 적은 수의 클라이언트가 참여하여 도출된 학습모델보다 더 좋은 학습 성능을 갖는다는 민주화 사회에서 채택하고 있는 다수결의 원칙을 준용하여 계층적으로 구성한 구조를 말한다.**

민주화 AI 학습(Democritized AI: Dem-AI)은 대규모 분산학습 시스템의 자율적으로 구성되는 계층 구조를 갖는 전문화-일반화된(specialized-generalized) 프로세스들로 구성된다. 전문화되고 일반화된 프로세스는 각 에이전트(클라이언트)의 제한된 학습 역량을 이용하여 자신의 데이터를 이용하여 로컬학습을 수행하고 각 계층에서 일반화 모델을 만드는 학습을 수행하는 공통의 목표위해 협력적으로 동작한다. 각 계층학습모델은 로컬 에이전트로 전이(transfer)되어 로컬 모델이 되는 과정을 갖게 된다.

민주화 AI의 메타법칙(Dem-AI Meta-Law)는 Dem-AI 시스템의 전문화-일반화된 프로세스 간의 천이를 조정하는 데 사용할 수 있는 메커니즘으로 정의된다. 이 메타 법칙은 1)안정성(stability) 힘과 2)가소성(plasticity) 힘의 두 가지 균형 축에 따라 작동된다. 학습 시간 내내 천이 메커니즘은 이러한 힘 사이의 중요도 가중치를 조정하여 Dem-AI 시스템의 계층구조뿐만 아니라 전문화된 학습과 일반화된 학습의 가소성 또는 안정성을 강화한다. 또한 Dem-AI Meta-Law는 자율계층구조 메커니즘을 조정하는 데 필요한 레벨의 수, 측정된 유사성 거리와 같은 정보들을 제공한다.

전문화된 프로세스는 그림 4에 설명된 대로 수집된 데이터를 활용하여 개별 에이전트 또는 전문화된 그룹에서 전문화된 학습능력을 활용하기 위해 사용된다. 따라서 개인화 학습 목표는 1) 전문화된 학습을 수행하는 것과 2) 각 계층에서 일반화된 지식을 재사용하는 두 가지 목표를 가지고 있다. 또한, 일반화된 지식

은 개인화된 학습 목표를 위해 레귤러라이저(regularizer)에 의해 조정될 수 있다.

일반화된 프로세스(generalized process)는 기존의 모든 전문화된 그룹들에 대한 일반화와 모든 일반화 그룹의 가소성 수준을 조절하는 데 사용된다. 지식 공유는 유사하고 연관성이 있는 학습 작업으로부터 일반화된 지식을 구성하는 메커니즘이다. 이는 연합학습에서의 모델 평균화, 멀티 태스크 학습에서의 지식 공유, 지식 증류 등과 유사하다. 과도하게 간극이 있는 전문 그룹 간의 차이를 해결하기 위해, 일치를 위한 선거(election) 메커니즘을 채택할 수 있다. 또한 잠재적 그룹의 다양성을 유지하기 위해 집합(union) 메커니즘을 적용할 수 있다. 이 프로세스는 그림4에 설명되어 있다. 이 경우 집합에 속해 있는 학습모델 중 어떤 것을 선택할 것인가에 대한 기법은 별도로 연구해야 한다.

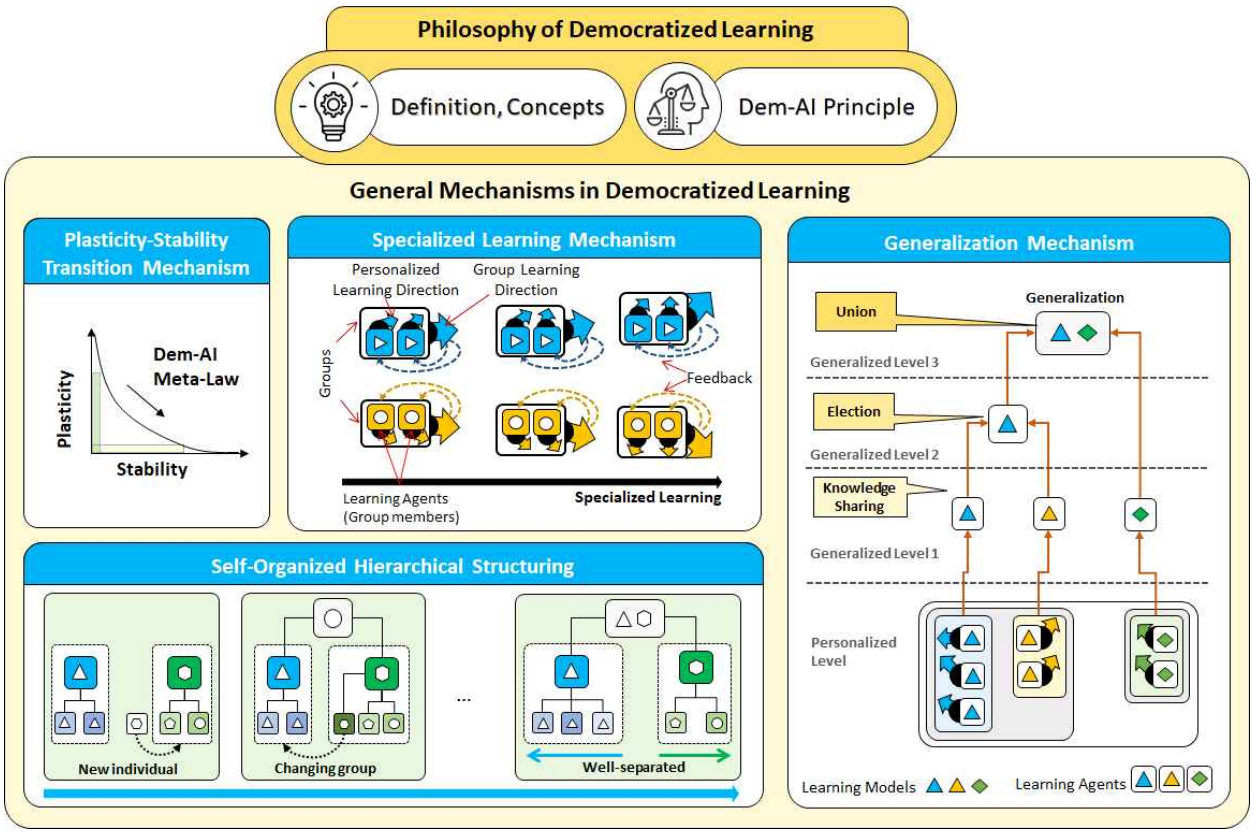


그림 4. 민주화 학습 메커니즘

자율구조 구성 원리: 전문화된 그룹의 계층구조와 관련 일반화된 지식은 학습 에이전트의 유사성에 기초한 자율구조 구성 원칙에 따라 만들어 진다. 이 프로세스는 다음의 세 단계로 이루어진다.

• **초기 단계(계층구조 구성):** 가장 낮은 레벨의 그룹은 공통 학습 작업을 수행하고 학습 모델에서 유사한 특성을 가진 에이전트를 그룹화 함으로써 생성된다. 현재 그룹 간의 거리 측정값이 각 레벨과 관련하여 미리 정의된 임계값보다 클 때 새로운 레벨을 생성할 수 있다.

• **적응 단계:** 적응 단계에서는 학습 에이전트가 그룹을 변경할 수 있다.

• **고도의 전문화 단계:** Dem-AI 시스템의 낮은 레벨에서는 에이전트 그룹들이 잘 분류되어 있고 안정화된 전문화 그룹들로 구성되어 있으므로 클라이언트 이동, 새로운 클라이언트 조인(join) 등에 따른 미세조정만을 허용한다.

상기의 Dem-AI 구조 설계를 위해 재귀 형태의 계층적 일반화 학습 원리에 착안하여 공식을 만들었고, 분산되고 개인화된 학습 문제와 계층적 평균화 메커니즘을 사용하여 솔루션을 얻을 수 있다. 본 저자가 속한 연구팀에서는 민주화학습 시스템을 위한 분산 학습 알고리즘, 즉 DemLearn과 이의 변형인 DemLearn-P를 개발했다. 이와 관련된 상세 사항은 참고문헌 [8]을 참조하기 바란다.

개인화된 인텔리전스: 우리는 대규모 학습 시스템에서 유비쿼터스 인텔리전스를 사용자에게 제공하기 위한 미래의 인간 중심 애플리케이션 개발을 추구한다. Dem-AI는 웹서비스, 교육, 의료, 인포테인먼트와 같은 일상생활에서 개인에게 제공되는 서비스에 유익한 솔루션을 제공하는 것을 목표로 한다. 더욱이, Dem-AI 구조는 서비스 제공자들에게는 그들의 서비스를 확장하기 위해 사용자의 지식을 이용할 수 있게 하고 일반 사용자들은 지식 공유를 통해 개인화된 성능을 집단적으로 향상시킬 수 있게 한다. 따라서 Dem-AI는 최종 사용자와 서비스 제공자를 위한 윈-윈 솔루션의 도출이 가능한 프레임워크를 제공한다.

Ⅲ. 네트워킹 시스템에서의 분산 학습

네트워크 환경에서 연합학습은 주로 태스크 스케줄링과 리소스 할당을 위해 사용되어 왔다. 이 같은 기술을 활용하는 경우 각 네트워크 노드가 책임지는 결정 프로세스(decision process)의 분산화와 태스크의 모듈화가 가능해진다. 분산학

습은 5G/6G 네트워크에서 많은 문제들을 해결할 수 있는 유력한 후보 학습 메커니즘의 하나이다. 예를 들어, 연합강화학습 알고리즘은 리소스 관리, 네트워크 제어, 채널간섭조정 및 사용자그룹화 같은 중요한 문제들을 다루기 위해 복잡한 convex함수 및 non-convex함수 최적화 문제에 대한 효율적인 솔루션을 제공하는 데 사용될 수 있다. 또한 연합지도학습 알고리즘은 무선 환경 분석, 사용자 식별, 사용자 인증, 접근 제어관리, 행동예측, 침입 탐지 및 방지를 포함하지만 이에 국한되지 않고 네트워크에서 제기 될 수 있는 광범위한 분석 서비스를 제공하는 데 사용될 수 있다. 또한 5G/6G 네트워크를 활용하여 분산 학습 프레임워크의 적용 가능성을 확인 할 수 있으며 학습효율 제고에 활용할 수 있다. 특히 높은 대역폭과 낮은 대기시간을 갖는 5G/6G 네트워크에 IoT와 엣지 디바이스를 연결함으로써 컴퓨팅 리소스 공유를 통해 효율적 자원 사용이 가능하게 된다. 또한 더 나은 성능으로 갖는 로컬모델을 도출하기 위해 배포된 로컬모델을 훈련시킬 수 있을 것이다. 마찬가지로 클라이언트 디바이스와 파라미터 서버 간에 글로벌 모델 배포와 모델 업데이트 정보를 교환하는 프로세스는 5G/6G 네트워크 설계에 반영한 eMBB(enhanced Mobile Broadband)특성 덕분에 더욱 효율적으로 수행될 수 있을 것이다.

3.1 연합 학습을 위한 클라이언트 선택 및 스케줄링

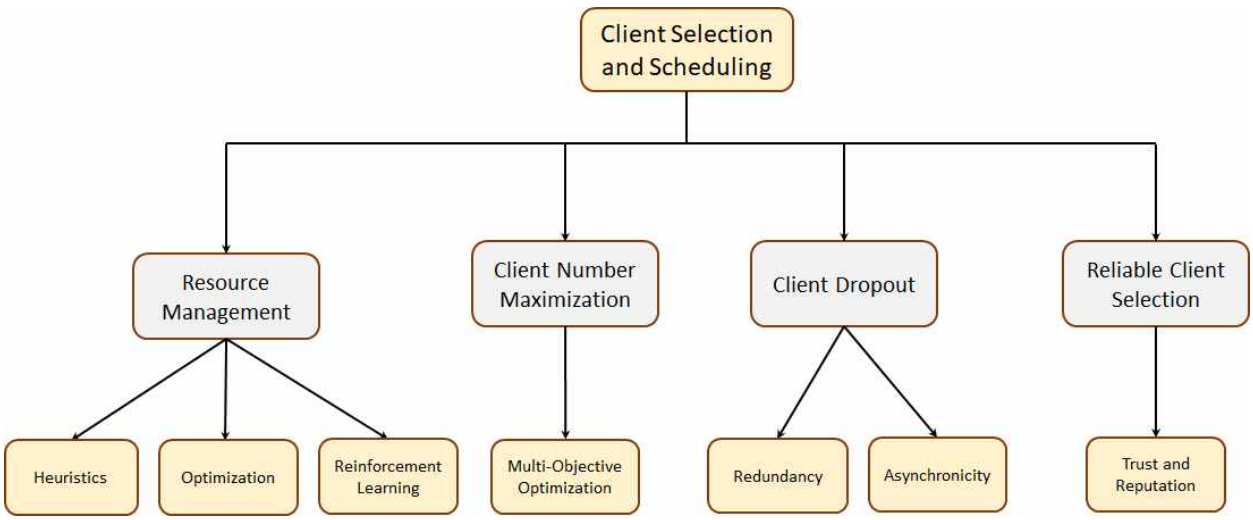


그림 5. 연합 학습에서의 클라이언트 선택 및 스케줄링의 접근 방법

클라이언트 선택 및 스케줄링 접근법[3]의 주요 목표는 연합학습 모델 소유자(즉, 파라미터 서버)가 협업 훈련의 성능을 개선하고 수렴 시간을 최소화하기 위해 어떤 클라이언트를 선택하고 훈련 태스크를 어떻게 분배할 것인지를 결정하는 것이다. 이러한 맥락에서, 1)리소스 관리 2)클라이언트 수의 최대화 3)클라이언트 누락에 대한 대응 4)신뢰할 수 있는 클라이언트 선택과 같은 해결해야 할 과제를 상정할 수 있다.

자원 관리: 클라이언트 선택 및 스케줄링 프로세스에서 해결해야할 주요 과제는 제한된 자원을 클라이언트 장치에서 효율적으로 관리하여 연합훈련 성능을 극대화하는 방법이다. 특히 클라이언트 디바이스에서 사용할 수 있는 리소스의 양은 선택되는 클라이언트와 각 클라이언트에 할당해야 하는 작업량을 결정하는 데 중요한 요소이다. 여기서 중요 고려사항은 모델 매개변수의 크기와 증가하는 매개변수 숫자, 그리고 클라이언트 디바이스의 이질성 및 대역폭 제한 등이다. 계산용량과 무선링크 품질은 클라이언트별로 다를 수 있으며, 학습정확도를 향상시키는 동시에 클라이언트의 리소스 소비를 최소화하는 적절한 방안을 도출하기 위한 최적의 리소스 관리방식을 설계하는 것이 중요하다. 본 연구팀에서 수행한 연구결과로 [4], [5], [6]에서 제시한 것과 같이 연합학습 알고리즘의 수렴과정을 분석한 다음, 연합학습 수렴 임계 클럭 시간과 이질적인 컴퓨팅자원과 전력자원을 갖는 클라이언트 디바이스의 에너지소비 사이의 절충점을 찾는 리소스 할당 최적화 문제를 해결하기 위해 연합학습을 무선 네트워크 환경에서 적용하였다.

스케줄링 방안과 관련하여 본 연구팀에서는 무작위 스케줄링(random scheduling: RS), 라운드 로빈방식(round robin: RR) 및 비례페어(proportional fair: PF) 스케줄링 전략이 대규모 무선 네트워크 환경에서 연합학습 성능에 미치는 영향에 대한 심층적 연구를 수행하였다. 액세스 포인트 및 무선 사용자 디바이스 위치는 독립적인 포아송 프로세스에 따라 배치된다. 분석 결과, 네트워크가 높은 신호 대 간섭 잡음비(SINR) 임계값으로 운용되는 경우 PF와 함께 연합학습을 실행하면 RS 및 RR 방식보다 더 나은 성능을 달성할 수 있음을 확인하였다.

클라이언트의 수 최대화: 반복적 학습에 참여하는 클라이언트의 수를 늘리면 글로벌 모델이 목표 성능에 도달하는 데 필요한 시간을 줄이는 데 기여한다. 실제로 각 라운드에 참여하는 클라이언트가 많으면 파라미터 서버가 필요로 하는 정확도를 얻기 위해 실행해야 하는 라운드 수를 줄일 수 있다. 이 같은 아이디어를 활용하여 각 반복훈련에 참여하는 클라이언트 수를 최대화하는 문제를 연구하는 것이다. 그러나 이는 1)non-IID 데이터를 생성 클라이언트 수 증가, 2)클라이언트 수 증가에 따른 로컬모델 업데이트 지연, 3)운용 프로세스에 추가되는 클라이언트 증가에 따른 각 클라이언트 신뢰성 검사와 같은 몇 가지 고려사항들이 발생된다.

클라이언트 드롭아웃: 클라이언트 드롭아웃(Client dropout)은 연합학습훈련에서 누락되는 클라이언트 문제를 가리킨다. 드롭아웃은 훈련 중 어느 순간에 발생할 수 있으며 배터리 부족, 연결 불량, 전화통화로 인한 무선링크 자원 미할당 등으로 발생하는 연결단절 등 여러 가지 이유로 인해 발생할 수 있다. 학습완료 전에 연합학습 훈련에서 탈락하는 클라이언트를 낙오노드(straggler)고 하며, 서버와 나머지 클라이언트 모두에 상당한 대기시간을 갖게 함으로써 리소스 낭비를 초래할 수 있다. 클라이언트 드롭아웃에 대응하는 두 가지 일반적인 기술은 중복성(redundancy)과 비동기성(asynchronicity)이다. 중복성 접근법의 주요 아이디어는 일부 클라이언트 드롭아웃 사례가 발생할 경우 통합 모델을 재구성하기 위해 활용할 모델 업데이트에 클라이언트를 추가하는 것이다. 비동기성은 모델 집계 프로세스의 동기화 가정을 완화하여 일부 클라이언트가 서버와 비동기 상태를 유지하도록 허용함으로써 수행될 수 있다. 즉 서버는 클라이언트로부터의 반응이 임계값 이상으로 지연되는 경우 해당 클라이언트의 송부 데이터를 기다리지 않는다는 것을 의미한다.

신뢰할 수 있는 클라이언트 선택: 연합학습에서 훈련은 지리적으로 분산된 대규모 클라이언트 디바이스 셋에 대해 수행된다. 모델 소유자는 이 같은 디바이스에 대한 제어 권한이 없으므로, 머신러닝 패러다임에서 신뢰할 수 없는 클라이언트와 마주치는 것은 불가피한일 일이 것이다. 그러한 클라이언트는 연합학습 프로세스에 치명적 악영향을 미칠 수 있다. 예를 들어 신뢰할 수 없는 클라이언트는 신뢰할 수 없는 데이터를 활용하여 로컬모델을 훈련시켜 나쁜 학습모델의 출현을 야기시킬 수 있다. 연합훈련의 성공을 보장하기 위해 신뢰할 수 있는 클

라이언트를 선택하기 위한 솔루션을 도출해야 한다. 따라서 클라이언트의 신뢰도와 평판도 평가는 중요한 과제가 될 수 있을 것이다.

3.2 엣지 컴퓨팅을 지원하는 민주화 학습 구조

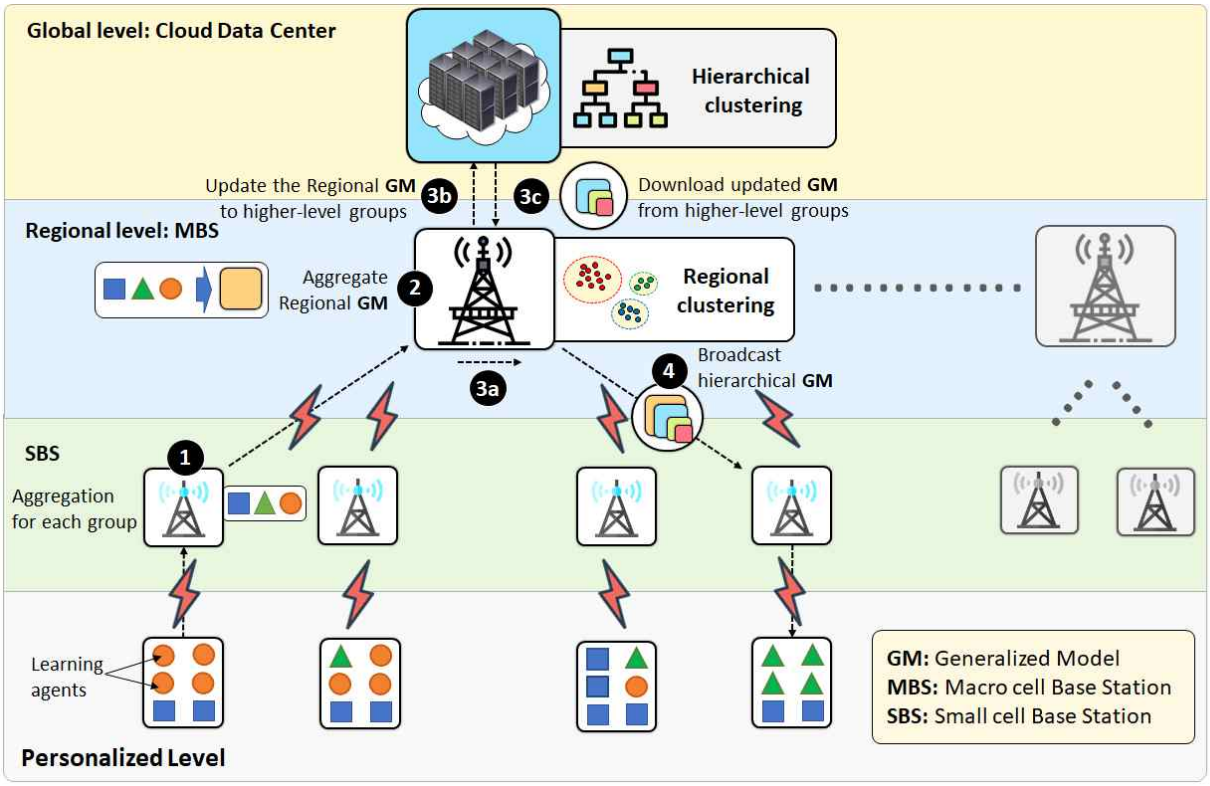


그림 6. 엣지 컴퓨팅 기반 민주화 학습 시스템 구조

Dem-AI의 활용에 대한 구조 [10]를 나타내는 그림 6은 자원할당 및 머신러닝 기법간 시너지 효과에 대해 설명 가능한 예를 보여주고 있다. SBS(small-cell base station)에서는 UE(user equipment)그룹 및 학습UE의 협업 학습프로세스와 지식통합(knowledge Integration)의 역할을 수행한다. MBS(macro-cell base station)에서는 전체 그룹 및 그룹 내 모델과 관련된 지역 수준의 학습 매개변수 집계를 수행한다. 또한, UE가 원시 데이터가 아닌 UE가 모델 매개변수만을 MEC(multi-access edge computing) 서버와 교환하는 것을 고려할 때, 이 같은 방식은 UE의 로컬 데이터를 중앙 엔티티(또는 원격 클라우드)에 전송하는 기존의 머신러닝 방식과 달리 프라이버시를 보장한다.

클라이언트 엣지-클라우드 계층적 연합학습[11]의 두 가지 통합(aggregation) 단계와는 달리 제안모델 업데이트는 SBS의 MEC 서버와 MBS에서 각각에서 수행될 수 있다. 본 보고서에서는 계층구조를 갖는 연합학습 구성모델을 제시하고 엣지 컴퓨팅 지원 Dem-AI 시스템의 실현을 위해 다음과 같은 이슈에 대한 추가적인 연구가 필요함을 언급하고자 한다.

- **보안 및 개인 정보 보호 강화**: 엣지 서버 및 클라우드 서버는 사용자 그룹핑을 통해 사용자의 비정상적인 학습 행태를 더 잘 관리하고 분류할 수 있으며, 연합학습에서 정보도용, 무단이용, 모델오염 및 데이터 오염공격을 완화하는 데 도움이 될 수 있다.
- **로컬 학습 및 효율적인 통신자원 관리 이슈에 대한 공통 설계**: 연합학습 프레임워크와 마찬가지로 Dem-AI 시스템도 제한된 통신 자원을 활용하기 위한 최적화 설계가 필요하다. 따라서 분산 학습 시스템의 효율성을 더욱 향상시키려면 엣지 영역에서 학습을 수행할 최적 사용자 선택은 매우 중요한 과제이다.

Ⅳ. 결론

본 보고서에서는 연합학습(federated learning) 및 민주화 학습(democratized learning)과 같은 분산 머신러닝 프레임워크의 핵심 구성 요소를 서술하고 제시하였다. 또한 주요 도전 과제와 해결해야 할 기술에 대해 논의했다. 주요 도전 이슈로서 데이터 확대, 능동학습, 멀티태스크 학습, 전이 학습, 매개변수 조정, 지식증류, 가중치 최적화, 데이터압축, 신뢰 및 평판, 다중 목적 최적화, 강화 학습 등이 포함된다. 따라서 본 이슈 보고서는 KOREN 연구 커뮤니티가 혁신적이고 효율적인 미래 인터넷 솔루션을 설계하도록 돕는 이정표가 되는 구조를 제시하였고, 분산학습 구조를 엣지 컴퓨팅 환경에 어떻게 내재화 할 수 있을 지에 대한 주요 방향을 제시한 리포트임을 밝혀둔다.

참 고 문 헌

[1] H. B. McMahan, E. Moore, D. Ramage, S. Hampson et al., “Communication-efficient learning of deep networks from decentralized data,” in *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS)*, 2017.

[2] L. U. Khan et al., “Federated learning for edge networks: Resource optimization and incentive mechanism,” *IEEE Commun. Mag.*, vol. 58, no. 10, pp. 88–93, Oct. 2020.

[3] Wahab, Omar Abdel, et al. "Federated Machine Learning: Survey, Multi-Level Classification, Desirable Criteria and Future Directions in Communication and Networking Systems." *IEEE Communications Surveys & Tutorials* (2021).

[4] N. H. Tran, W. Bao, A. Zomaya, M. N. H. Nguyen, and C. S. Hong, “Federated learning over wireless networks: Optimization model design and analysis,” in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Paris, France, April 29–May 2, 2019, pp. 1387–1395.

[5] C. T. Dinh, N. H. Tran, M. N. H. Nguyen, C. S. Hong, W. Bao, A. Y.Zomaya, and V. Gramoli, “Federated learning over wireless networks: Convergence analysis and resource allocation,” *IEEE/ACM Transactions on Networking*, vol. 29, no. 1, pp. 398–409, Feb. 2021.

[6] M. N. H. Nguyen, N. H. Tran, Y. K. Tun, Z. Han, & and C. S. Hong. “Toward Multiple Federated Learning Services Resource Sharing in Mobile Edge Networks,” arXiv preprint arXiv:2011.12469 (2020).

[7] M. N. H. Nguyen, S. R. Pandey, K. Thar, N. H. Tran, M. Chen, W. Saad, and C. S. Hong, “Distributed and democratized learning: Philosophy and research challenges,” *IEEE Computational Intelligence Magazine*, vol. 16, no. 1, pp. 49–62, 2021.

[8] M. N. H. Nguyen, S. R. Pandey, T. Nguyen D., E. N. Huh, C. S. Hong, N. H. Tran, and W. Saad, “Self-organizing democratized learning: Towards large-scale distributed learning systems,” 2020, *arXiv:2007.03278*.

[9] R. Shafin, L. Liu, V. Chandrasekhar, H. Chen, J. Reed, and J. C. Zhang, “Artificial intelligence-enabled cellular networks: A critical path to beyond-5g and 6g,” *IEEE Wireless Communications*, vol. 27, no. 2, pp. 212–217, 2020.

[10] S. R. Pandey, M. N. H. Nguyen, T. N. Dang, N. H. Tran, K. Thar, Z. Han, and C. S. Hong, "Edge-assisted Democratized Learning Towards Federated Analytics." arXiv preprint arXiv:2012.00425 (2020).

[11] L. Liu, J. Zhang, S. Song, and K. B. Letaief, “Client-edge-cloud hierarchical federated learning,” *IEEE International Conference on Communications (ICC)*, Dublin, Ireland, June 2020.