산업현장의 자율 제조를 위한 연합 학습에 관한 연구

정우성, 윤태현, 황윤숙, 유대승

한국전자통신연구원

woosung@etri.re.kr, thyoon0820@etri.re.kr, hanulai403@etri.re.kr, ooseyds@etri.re.kr

A Study on Federated Learning for Autonomous Manufacturing in Industrial Fields

Woo-Sung Jung, Tae Hyun Yoon, Yoonsook Hwang, Dae Seung Yoo

Electronics and Telecommunications Research Institute

요 약

제조 산업에서 자율 제조를 위한 인공지능(AI) 기반 시스템을 구축하는데 가장 큰 이슈는 현장에서 수집되는 데이터의 보안에 관한 것이다. 본 논문에서는 이와 같은 이슈를 해결하는데 적용 가능한 연합 학습(Federated Learning) 기술 동향을 살펴보고, 제조 현장의 특수성(이기종 설비, 시계열 데이터, 보안 요구 등)을 고려한 아키텍처와 구성 기술을 분석하였다. 또한, 이를 기반으로 주요 연구 이슈를 도출하여 이슈별 연합 학습의 필요성과 현장에 특화된 연합 학습 모델 개발을 위한 기술적 과제를 제안하고자 한다.

Ⅰ. 서론

디지털 전환 기술의 확산으로 제조 산업도 빠르게 디지털화되는 흐름에서 특히 자율 제조(Autonomous Manufacturing)로의 전환이 가속화되고 있다. 이는 단순한 자동화뿐만 아니라, 데이터를 기반으로 한 실시간 의사결정, 예측, 최적화가 가능한 지능형 자율 제조시스템의 운영을 의미한다. 이러한 변화의 중심에는 인공지능 기술이 있으며, 인공지능은 생산성 향상, 품질 제어, 공정 최적화 등의 핵심 임무를 수행하고 있다.

인공지능 기반 자율 제조를 실현하기 위해서는 고품질의 대규모 데이터 수집과 이를 효율적으로 학습하는 과정이 필수적이다. 제조 현장은 각 설비나 공장 단위로 대규모 데이터가 생성되고 있으나, 기업은 이들 데이터를 기업의 핵심 자산으로 간주하기 때문에 데이터 전처리 및 학습 목적으로 외부로 보내거나 공유하는 것에 대해 기업 기밀 및 데이터 유출 등 보안에 대한 우려가 크다. 이는 자율 제조를 실현하는데 큰 제약사항이 될 수 있다. 이를 해결할 수 있는 방안으로 연합 학습(Federated Learning)의 적용을 고려할 수 있다. 연합 학습은 데이터를 로컬에 보관한 채, 각 설비 또는 공장에 설치된 클라이언트에서 개별적으로 학습한 모델 파라미터만을 중앙 서버로 전송하여 글로벌 모델을 구축하는 방식이다. 이에 따라 데이터 유출 없이 다양한 환경의 데이터를 활용한 학습이 가능하며, 최근 제조 산업을 포함한 다양한 분야에서 연합 학습에 관한 연구가 활발히 이루어지고 있다. 본 논문에서는 이러한 연합 학습을 통해서 산업현장에 적용할 수 있는 기술 구성을 소개하고 이를 완성하기 위한 연구 이슈에 대해서 알아본다.

Ⅱ. 본론

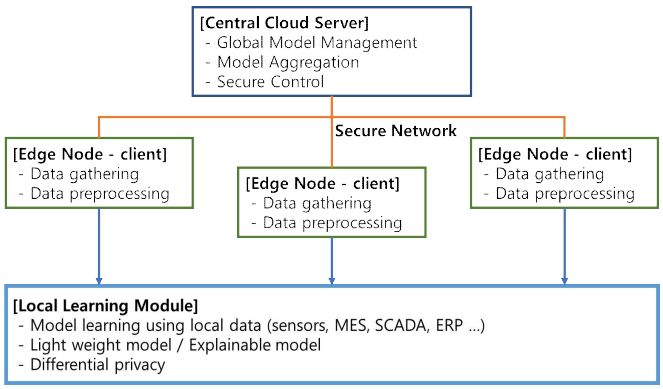
1) 연합 학습 관련 연구 동향

연합 학습은 2016년 Google의 발표[1] 이후로 급격히 발전해 왔으며, 의료, 금융, 스마트시티 등 다양한 민감 데이터 환경에서 실용화되고 있으며, 비동기 학습, 이질적 데이터 분포(Non-IID), 보안성 강화, 통신 효율화 등 다양한 측면에서 지속적인 기술 진보가 이루어지고 있다. 특히 제조 분야에서는 센서 기반의 시계열 데이터 처리, 고장 예측, 품질 분석, 공정관리 등에서 연합 학습의 적용 가능성이 크게 주목받고 있다.

대표적인 연구 사례인 Federated Averaging (FedAvg) 알고리즘[2]은 연합 학습의 기본개념을 제안하여 각 클라이언트에서 학습한 모델을 효과적으로 통합하는 방법을 제시하였다. FedProx[3]는 이기종 클라이언트 환경에서 각 클라이언트의 데이터 편향 및 계산 자원의 차이를 보정하는 방식을 제안하였다. 산업현장에서는 고장과 관련된 예측에 주로 연합 학습이 많이 사용되었다. 고장 진단의 신뢰성을 높이는 방법으로 데이터의 이질성 문제를 해결하고 모델 검증의 정확도를 향상하는 방식[4]이 제안되었으며, 분산된 공장 환경에서 예지보전 목적의 연합 학습 기반 고장 진단 기술[5]도 연구되었다. FedCPG[6]는 클래스 프로토타입을 활용하여 모델의 일반화 성능을 향상시켰으며, 이를 통해 각 공장의 고유한 데이터 특성을 반영하면서도 효율적인 고장 감지 기능이 연구되었다.

2) 자율 제조를 위한 연합 학습 아키텍처

제조 환경에서의 연합 학습 아키텍처는 크게 중앙 서버, 다수의 엣지 클라이언트, 통신 보안 계층으로 구성할 수 있다. 중앙 서버는 글로벌 모델의 집계를 담당한다. 엣지 클라이언트는 자율적으로 로컬 데이터를 학습하여 파라미터를 생성하여 글로벌 모델 구성에 사용된다. 각 클라이언트는 센서, MES, PLC 등과 연결되어 데이터 수집 및 전처리를 수행하며, 경량화된 학습모델을 활용하여 실시간 처리 성능을 확보한다. 또한, 보안 강화를 위해 이들 사이에 암호화 통신과 위변조 방지 기술을 적용한다.



〔그림 1〕 제조산업현장에서의 연합 학습을 위한 구성도

〔표 1〕 제조 산업 분야의 연합 학습 적용을 위한 연구 이슈

연구 이슈	필요성	기술적 과제
제조 공정 특화 연합 학습 모델 개발	- 제조 데이터는 자연어 및 이미지 중심의 모델과 함께 대부분 시계열 센서 기반으로 구성된 데이터 처리가 중요하며, 정적 모델로는 시간 흐름에 따른 이상 탐지나 고장 예측에 한계가 발생 - 이미지 및 시계열 기반 제조 데이터를 효과적으로 학습할 수 있는 공정 특화 연합 학습 모델 설계 등의 연구가 필요	- 시계열 특화 RNN, LSTM, Transformer 기반의 연합 학습 모델 구조 설계 - 데이터 정렬, 윈도잉, 결측치 처리 등 시계열 전처리 전략 - 이벤트 기반 공정에 적합한 알고리즘 개발 - 멀티모달을 지원하는 제조 특화 모델 구조 설계
비동기 및 이기종 연합 학습 기술 개발	- 제조 공정은 각각 설비의 가동 시간, 데이터 양, 주기 등이 다르므로 동기식 학습 방식에 한계가 존재 - 설비 간 데이터 형식 및 품질이 상이하여 일관된 모델 학습이 어려우므로 클라이언트 특성을 반영한 유연한 학습 구조가 필요	- 클라이언트별 모델 클러스터링, Personalized 연합 학습, 구조적 적응형 모델 아키텍처 설계 기술 - 서로 다른 데이터 분포 환경을 위한 성능 최적화 - 이기종 모델의 학습 방법론 개발
엣지 환경의 모델 경량화 및 통신 최적화 기술 개발	- 제조 설비에 탑재된 엣지 디바이스는 연산과 통신 자원이 제한적이기 때문에 리소스 부족, 실시간성 저하, 통신 병목 현상 문제가 발생 - 효율적인 로컬 학습을 위해 모델 경량화 및 전송량을 최소화하기 위한 노력이 필요	- 통신 자원의 효율적 활용을 위한 데이터 압축 및 전송빈도 조절, 컴퓨팅 오프로딩 등 통신 및 자원의 최적화 기술 연구 - 로컬 모델의 경량화 프레임워크 개발 - 연산 부하를 줄이기 위한 경량 학습 스케줄러에 대한 연구
보안 및 프라이버시 강화 기술 개발	- 제조 데이터는 기업 경쟁력과 직결되는 경우가 많아 기업의 핵심 자산으로 취급되며 학습 중 유출 시 막대한 경제적 피해와 신뢰 저하 초래 - 데이터 기밀성을 보장하면서도 안정적인 협력 학습 환경 제공이 필요	- 경량화된 보안 네트워크 적용 기술 개발 - 제조 데이터 특화 차등 프라이버시 적용 방식 - 위변조 방지 및 공격 탐지 메커니즘 개발
설명 가능한 연합 학습 모델 설계	- 제조 현장에서 고장, 품질 문제 발생 시 인공지능의 판단 근거가 불분명하면 인공지능에 신뢰도 하락 및 실무 적용이 어려움 - 제조 엔지니어와 관리자에게 모델 판단 근거를 제시함으로써 제조 현장의 신뢰성 확보 및 결과 검증이 중요	- 해석 가능한 AI 기법을 분산 환경에 적용하는 기술 - 모델의 판단 근거를 사용자 친화적 시각화 도구를 이용하여 제공하여 설명할 수 있는 기술 - 설명 가능한 연합 학습 구조의 개발
디지털 트윈 및 강화학습과의 융합 기술 개발	- 실제 설비에서 반복적 실험이나 테스트는 비용 및 위험이 크기 때문에 가상 시뮬레이션 기반 학습과 제어가 필수적	- 연합 학습 기반 디지털 트윈 시뮬레이션에 적용 연구 - 강화학습과 연계된 공정 최적화 및 의사결정 구조 설계 - 물리 모델/데이터 모델의 융합 구조 등의 연구

3) 자율 제조 적용을 위한 연합 학습 연구 이슈

연합 학습 기술은 자율 제조 분야에서 데이터 보안과 협력적 모델 학습이라는 두 가지 요구를 모두 충족시키며 제조 AI의 기술 개발에 새로운 접근 방식으로 주목받고 있다. 그러나 연합 학습 기술을 실제 산업현장에 안정적으로 적용하기 위해 해결해야 할 기술적 과제는 여전히 남아 있다. 예를 들어, 고장이나 설비 교체 등 환경 변화에 대응하는 적응형 연합 학습 기술, 클라이언트의 학습 실패를 보완할 수 있는 재학습 메커니즘, 공정별 연합 모델의 설명 가능성 및 해석력 향상을 위한 기술 등이 연합 학습 기술에 포함되어야 필요가 있다. 또한, 연합 학습과 디지털 트윈의 연동 등 다른 기술과의 융합도 중요한 연구 주제로 제시될 수 있다. 연합 학습 기술의 제조 분야 적용에 관한 주요 연구 이슈는 [표1]과 같이 정리할 수 있다.

Ⅲ. 결론

제조 산업 분야에서 디지털 전환과 함께 자율 제조에 대한 요구는 지속적으로 증가하고 있으며, 이러한 지능형 시스템의 기반 기술로 인공지능과 데이터 기반 학습은 핵심적인 역할을 하고 있다. 그러나 현장에서는 기업이 보안, 기밀성 등을 이유로 데이터를 보호하고자 하며, 이기종 설비의 데이터 수집 등 여러 제약으로 인해 데이터 공유 및 중앙 집중형 학습에는 한계가 존재한다. 이러한 문제를 해결할 수 있는 대안으로 연합 학습이 제시되고 있으며, 실제 제조 현장에서도 이를 활용하기 위한 구조를 확인하고 실제 고장 진단 등에 적용을 위한 한 시도 및 연구를 살펴보았다.

본 논문에서는 제조 산업에서의 연합 학습 적용 가능성을 기반으로, 이를 위한 핵심 아키텍처를 소개하고, 효과적인 적용을 위한 연구 이슈와 필요성, 기술적 과제를 도출하였다. 각 연구 이슈는 제조 환경의 현실적인 요구와 기술적 한계를 동시에 반영하고 있으며, 연합 학습 기반 제조 인공지능의 실효성을 높이기 위한 중요한 연구 방향임을 확인하였다. 향후에는 제안된 기술적 과제들에 대한 실증 기반의 평가, 산업현장 적용성 검증, 모듈화된 아키텍처 설계 및 표준화 작업이 병행되어야 할 것이다.

ACKNOWLEDGMENT

본 논문은 울산시-ETRI 2차 공동협력사업(25AB1600, 제조 혁신을 위한 주력산업 지능화 기술 개발 및 산업현장에서의 사람-이동체-공간 자율협업지능 기술 개발)의 지원을 받아 수행되었음

참 고 문 헌

[1] Brendan McMahan and Daniel Ramage. “Federated learning: Collaborative machine learning without centralized training data.” Google Research Blog 3, 2017.

[2] Brendan McMahan, Eider Moore, Daniel Ramage, Seth Hampson, Blaise Aguera y Arcas Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, PMLR 54:1273-1282, 2017.

[3] Tian Li, Anit Kumar Sahu, Manzil Zaheer, Maziar Sanjabi, Ameet Talwalkar, Virginia Smith, “Federated optimization in heterogeneous networks.” Proceedings of Machine learning and systems, 2, pp. 429-450., 2020

[4] Y. Li, Y. Chen, K. Zhu, C. Bai and J. Zhang, "An Effective Federated Learning Verification Strategy and Its Applications for Fault Diagnosis in Industrial IoT Systems," in IEEE Internet of Things Journal, vol. 9, no. 18, pp. 16835-16849, 15 Sept.15, 2022

[5] Dinh C. Nguyen, Ming Ding. Pubudu N. Pathirana, Aruna Seneviratne. Jun Li. Dusit Niyato, "Federated Learning for Industrial Internet of Things in Future Industries," in IEEE Wireless Communications, vol. 28, no. 6, pp. 192-199, Dec. 2021

[6] Haodong Li, Xingwei Wang, Peng Cao, Ying Li, Bo Yi, Min Huang, "FedCPG: A class prototype guided personalized lightweight federated learning framework for cross-factory fault detection," Computers in Industry, Volume 164, 2025, 104180