RAG-LLM을 활용한 고위험 환경 시계열 이상 감지: 프롬프트 최적화와 의사 이상 데이터 생성

최하진, 박지원, 김민석*
상명대학교 휴먼지능로봇공학과

pid9534@naver.com, dev_parkjiwon@naver.com, *minsuk.kim@smu.ac.kr

Time-Series Anomaly Detection in High-Risk Domains based on RAG-LLM: Prompt Optimization and Pseudo-Anomaly Data Generation

Ha Jin Choi, Ji Won Park, Min-Suk Kim*
Dept. of Human Intelligence & Robot Engineering, Sangmyung University

요 약

고위험 플랜트 시설에서의 시계열 데이터 기반 이상 감지는 데이터 수집의 제약, 센서의 다양성, 상이한 데이터 분포 환경, 그리고 시계열 전용 파운데이션 모델의 부재 등으로 해결하기 어려운 도전 과제로 남아 있다. 본 논문은 고위험 환경에서의 시계열 이상 감지 한계를 극복하기 위해, Large Language Model(LLM) 기반 시계열 데이터 이상 감지 구조에 Retrieval-Augmented Generation(RAG) 구조를 결합하여 환경 적응성을 강화하는 새로운 접근 방식을 제안한다. 또한, 시계열 이상 상태에 대한 프롬프트 전략 및 해당 프롬프트와 LLM을 이용하여 의사 이상 데이터를 생성하고, 생성한 이상 데이터와 입력 데이터와의 유사도 비교를 통해 LLM 기반 이상 추론 과정의 불투명한 결과 분석 문제를 보완하고 이상감지 성능을 높인다. 실험 결과, 제안한 방식은 다양한 환경에서 일관되게 높은 정확도를 나타내고 있으며, 데이터가 제한적인 환경에서도 효과적인 적용 가능성을 보여주고 있다.

Ⅰ. 서 론

고위험 산업 환경의 시계열 데이터 이상 감지는 데이터 수집의 어려움과 다수의 센서별 데이터 분포 차이로 추가 모델이 요구되지만 시간과 비용이 많이 필요하다. 더불어 시계열 전용 파운데이션 모델의 부재로 인해 도메인 간 전이 학습을 적용하기도 매우 어렵다. 이러한 한계를 극복하기 위해, 최근에는 사전 학습된 Large Language Model(LLM)을 시계열 분석에 적용하려는 연구가 활발히 진행되고 있지만, 이상 감지 분야에서는 여전히 시계열 데이터의 도메인별 특수성을 반영하지 못해 도메인 적응력이 제한되고 있다.

본 논문에서는 이러한 문제를 해결하기 위해 프롬프트 설계에 기반한 LLM 시계열 이상 감지 구조인 AAD-LLM[1]을 바탕으로 Retrieval-Augmented Generation(RAG)을 결합한 프레임워크를 제안하며, 이를 통해 적용 도메인에 대한 적응성을 향상시키고자 한다. 더하여 이상을 잘 감지할 수 있도록 보조기법을 더한 프롬프트를 설계했다. 또한, LLM 을 이용해 의사 이상 데이터를 생성하고, 이를 입력 데이터와 비교하여 유사도를 산출함으로써, LLM 의 추론 과정에서 발생하는 결과 해석의 모호성을 완화하고 이상 감지 성능을 향상시킨다.

Ⅱ. 시스템 구조

Ⅱ.1. RAG 기반 도메인 적응

RAG 는 retriever 를 통해 외부 지식을 검색하여 LLM 의 응답 생성 과정에 반영함으로써, 출력의 품질과 신뢰성을 향상시키는 기법이다. 일반적으로 Retriever 은 벡터 데이터베이스나 문서 집합에서 유사도 기반으로 관련 정보를 검색하고, 이를 LLM 의 입력 프롬프트에 포함시켜 응답을 생성한다. 본 연구에서는 적용 도메인에 특화된 데이터를 csv 파일 형태로 벡터 데이터베이스에 저장하고, 입력 데이터가 새롭게 들어오면 이를 참조하도록 하여 환경 적응력을 향상시키는데 목적이 있다.

Ⅱ.2. 프롬프트 설계

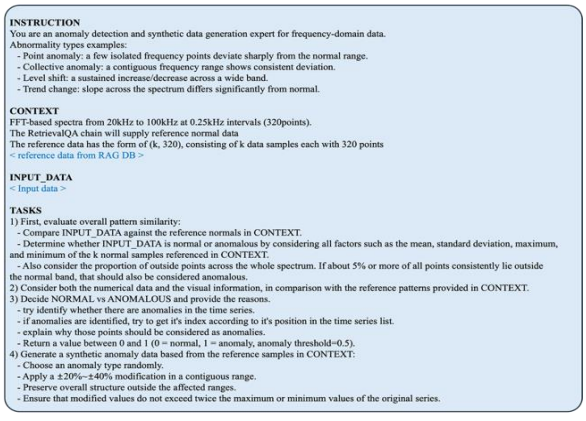

그림 1. 프롬프트 템플릿 구성

위 그림과 같이 프롬프트는 INSTRUCTION, CONTEXT, INPUT_DATA, TASKS 네 부분으로 구성되며 규칙 및 이상 상태에 대한 정의가 포함된다. 또한, 이상 탐지 성능 향상을 위해 프롬프트에 기존의 세 가지 보조 기법[2]을 적용하였다. 첫째, multi-modal instruction 을 활용하여 LLM 이 시계열 데이터를 단순한 수치정보 뿐만 아니라 시각적 패턴으로도 해석할 수 있도록 하였으며, 이를 통해

이상 패턴 인식의 정확도를 향상시켰다. 둘째, In-context learning 을 통해 RAG retriever 에서 참조한 정상 데이터 예시를 포함시켜 데이터가 제한된 환경에서도 높은 적응성을 확보할 수 있게 하였다. 셋째, Chain-of-Thought(CoT) 프롬프트 튜닝을 적용하여 모델이 이상 판단 과정과 근거를 단계적으로 서술하게 함으로써 LLM 기반 이상 탐지 정확도를 향상시켰다.

Ⅱ.3. 시스템 구조

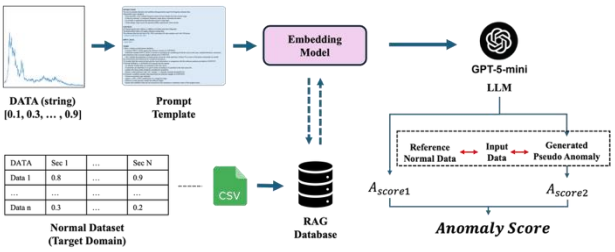

그림 2. RAG-LLM 기반 이상감지 작업흐름도

그림 2 는 본 논문에서 제안하는 RAG-LLM 기반 이상 감지의 전체 작업흐름도를 나타내고 있다. 시계열 입력 데이터 x_{in}이 시스템에 제공되면, 해당 데이터는 전처리 과정을 거친 후 앞서 언급한 바와 같이 프롬프트 템플릿에 입력된다. 프롬프트는 임베딩 모델을 통해 벡터화되고 이 벡터는 retriever 를 통해 도메인 관련 데이터셋에서 유사도가 높은 정상 데이터들을 검색하는데 사용된다. 또한, 검색된 관련 정상 데이터와 원본 프롬프트는 LLM 에 입력되고 두 가지 방식으로 이상 감지 과정을 거친다. 첫 번째 방식은 입력 데이터와 RAG 를 통해 검색된 유사 데이터 간의 비교 및 분석을 LLM 이 자체 판단을 하여 A_{score_1} 이 산출된다. 두 번째 방식에서는 LLM 이 프롬프트를 기반으로 n개의 의사 이상 데이터(pseudo anomaly data)를 생성한다. 이에 대한 평균 점인 P_a 와, RAG retriever 를 통해 뽑은 n개의 정상 데이터에 대한 평균 점인 P_n을 수식(1)과 같이 구한다. 이후 수식(2)와 같이 입력 데이터와 각 평균점과의 코사인 유사도 $\cos(\,)$ 에 대한 Softmax 기반의 두번째 이상점수인 A_{score_2}를 계산한다.

$$P = \frac{1}{n}\sum_{k=1}^{n} x_k \tag{1}$$

$$A_{score\_2} = \frac{\exp(\cos(x_{in}, P_a))}{\exp(\cos(x_{in}, P_a)) + \exp(\cos(x_{in}, P_n))} \tag{2}$$

최종 이상 점수는 수식(3)과 같이 α 와 β 를 통해 기여도를 조절하여 두 방식의 이상 점수를 가중 합산하여 결정된다.

$$Anomaly\ Score = \alpha \cdot A_{score\_1} + \beta \cdot A_{score\_2} \tag{3}$$

Ⅱ.4. 데이터 분석 및 처리

본 연구에서는 실험을 위해 발전소의 이차계통에서 배관의 누출 상황을 가정한 실험 장비에서 수집한 시계열 데이터를 활용하였다. 초음파 신호로 수집된 데이터는 고속 푸리에 변환을 통해 전처리 하였으며, 20~100 kHz 범위를 0.25 Hz 간격으로 측정한 평균 스펙트럼 값 320 길이로 구성된다. 서로 다른 환경에서 수집한 A, B, C 클래스가 있으며 구성은 표 1 과 같다.

	A	B	C
Normal	250	250	250
Anomaly	200	200	200

표 1. 데이터셋 구조

Ⅲ. 실험

본 실험에서 LLM 은 OpenAI 의 GPT-5-mini 를 사용하였으며, RAG 모듈에서 참조할 전용 CSV 파일에는 각 환경별로 정상 데이터를 무작위로 50 개씩 저장했다. 나머지 데이터는 실험의 입력데이터로 사용하여 제안한 구조의 성능을 평가했다. 또한, 제안한 RAG-LLM 기반 이상 감지 기법(RAG-AD)을 기존 LSTM 기반 이상 감지 모델과 비교하여 실험을 진행하였다. 실험 결과, 모든 환경에서 RAG-AD-2, RAG-AD-1, LSTM 순으로 성능이 우수하게 나타났다. 특히, RAG-AD-2 는 의사 이상 데이터를 사용한 이중 평균 점수 기반 이상 감지 방식인 $Anomaly\ Score$ 를 적용함으로써, A_{score_1} 만을 사용한 RAG-AD-1 대비 모든 환경에서 성능이 향상되었다. 이는 의사 이상 데이터 생성을 통해 정상 데이터와의 차이가 더욱 명확히 하여, LLM 의 이상 판단 정확도를 향상시킴을 보여주고 있다.

	A	B	C
LSTM Autoencoder	0.5325	0.4528	0.5401
RAG-AD -1	0.8041	0.6869	0.7693
RAG-AD-2	**0.8292**	**0.7692**	**0.8182**

표 2. F1-score 측정 결과

Ⅳ. 결론

본 논문에서는 데이터 제약이 존재하는 고위험 환경에서의 이상 감지를 위해 RAG-AD 구조를 제안하였으며, 프롬프트 전략과 의사 이상 데이터 생성을 통해 LLM 의 도메인 적응성과 이상 감지 성능을 향상시켰다. 또한, 고위험군 배관 누출을 재현한 테스트베드에서 수집한 데이터기반의 제안한 모델 성능은 기존 LSTM 모델 대비 높은 성능을 달성하였다. 특히, 의사 이상 데이터 기반 이중 평균 점수 방식은 모든 환경에서 성능 향상을 보였으며, 이는 데이터가 제한된 고위험 환경에서의 실질적인 활용 가능성을 시사하고 있다.

ACKNOWLEDGMENT

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korean government. (MIST) (No. RS-2022-00144000)

참 고 문 헌

[1] Russell-Gilbert, A., Sommers, A., Thompson, A., Cummins, L., Mittal, S., Rahimi, S., ... & Church, J. (2024, December). Aad-llm: Adaptive anomaly detection using large language models. In *2024 IEEE International Conference on Big Data (BigData)* (pp. 4194-4203). IEEE.

[2] Dong, M., Huang, H., & Cao, L. (2024). Can LLMs Serve As Time Series Anomaly Detectors?, *arXiv preprint arXiv:2408.03475*.