TKAD: 트랜스포머 구조와 칼만 필터 결합을 통한 클라우드 시스템 시계열 로그 이상 탐지 기법

허용석 [1], 유헌창 [2]
[1] 고려대학교 SW · AI 융합대학원 석사과정
[2] 고려대학교 정보대학 컴퓨터학과 교수

ys_heo@korea.ac.kr, yuhc@korea.ac.kr

TKAD: Transformer Networks and Kalman Filter-based Approach for Anomaly Detection in Cloud System Time-Series Logs

Yongseok Heo[1], Heonchang Yu[2]
[1]Dept. of Applied Artificial Intelligence, Graduate School of SW · AI Convergence, Korea University
[2]Dept. of Computer Science & Engineering, Korea University

요 약

서비스 고도화와 퍼블릭 클라우드 확산으로 인해 시스템 복잡성과 규모가 증가하면서 시계열 로그 데이터의 양과 유형이 증가하고 있다. 안정적인 시스템 운영을 위해 시계열 로그 모니터링은 필수적이며 이상 탐지에는 높은 정확도가 요구된다. 본 연구에서는 트랜스포머 구조와 칼만 필터를 결합해 시스템 장애와 무관한 로그 데이터의 노이즈를 제거하고, 시계열 데이터의 패턴을 주기적으로 학습하여 임계치를 자동으로 조정함으로써 이상 탐지의 정확도를 높이고자 한다. 제안된 방법의 성능을 검증하기 위해 운영 중인 클라우드 환경에서 발생된 시계열 로그를 기반으로 실험을 수행한 결과, 연구에 사용된 다른 4 가지 딥러닝 기반 이상 탐지 모델보다 우수한 성능을 보였다.

1. 서론

최근 생성형 AI 와 탄소 정책은 기업의 IT 전략에 큰 변화를 가져오고 있다. 이 변화의 중심에는 퍼블릭 클라우드가 있으며 기업들이 운영하는 시스템에 대한 클라우드 환경의 수요가 증가하고 있다. 퍼블릭 클라우드 시장은 향후 5 년간 연평균 16.9% 성장할 것으로 예상된다[1].

클라우드 환경에서 생성되는 방대한 양의 시계열 로그 데이터는 시스템 상태를 모니터링하고 이상 탐지하는 데 중요한 역할을 한다. 이를 효과적으로 관리하는 것은 시스템의 안정성과 성능을 유지하는 데 필수적이다. 개발 및 운영 담당자들은 시스템의 장애를 예방하기위해 CPU, 메모리, 네트워크, DB 등의 다양한 성능 지표들을 모니터링한다. 시스템 장애를 판단하는 임계치는 초기 검증 단계에서 기존 운영 경험을 바탕으로 설정하며 이후 운영 상황에 따라서 지속적으로 조정해야 한다.

서비스의 복잡성과 규모가 증가함에 따라 시스템 구조도 변화하면서 부정확한 장애 알람이 발생하거나 실제 장애를 사전에 감지하지 못하는 문제가 발생할 수 있다. 특히 이러한 문제는 두 가지 주요 원인으로 나눌 수 있다. 첫째, 시스템 상태 체크나 단순 에러 로그와 같은 시스템 장애와 무관한 노이즈이다. 둘째, 시스템 구조의 변화에 따라 장애 기준이 변동되면서 적정한 임계치를 수동으로 조정하기 어렵기 때문이다.

본 연구에서는 시스템 장애와 무관한 노이즈를 효과적으로 제거하고 주기적 학습을 통해 최적의 임계치를 자동으로 반영하는 이상 탐지 시스템을 제안한다. 시스템의 핵심 요소인 TKAD(Transformer networks and Kalman filter-based Anomaly Detection)는 트랜스포머 구조와 칼만 필터를 결합한 시계열 로그에서의 이상 탐지 모델이다. 실제 클라우드 환경에서 운영 중인 데이터에 다른 4 개의 딥러닝 기반 이상 탐지 모델(LSTM-AE, USAD, TadGAN, TranAD)을 적용하여 성능 지표(F1-Score, AUC)를 비교했을 때 TKAD 모델이 가장 높은 점수를 기록하며 우수한 성능을 보여주었다.

2. 관련 연구

2.1 이상 데이터 유형

이상 데이터는 데이터의 특성과 발생 맥락에 따라 여러 유형으로 나눌 수 있으며 대표적으로 점 이상(Point Anomaly), 맥락적 이상(Contextual Anomaly), 집합적 이상(Collective Anomaly)로 분류할 수 있다[2].

점 이상은 다른 데이터와 비교하여 단일 데이터 포인트가 이상한 경우이다.

맥락적 이상은 특정 상황에서는 이상하지만 다른 상황에는 그렇지 않은 경우이다.

집합적 이상은 여러 데이터 포인트가 집합적으로 이상한 패턴을 보이는 경우이다.

점 이상과 맥락적 이상은 시스템 운영 중 일시적인 외부 요인이나 오류로 인해 발생하는 경우가 많아 서버 재기동 등의 단기적인 조치로 해결되는 경우가 많다. 반면, 집합적 이상은 여러 데이터 포인트가 함께 나타내는 패턴으로 서서히 증가하거나 하락하며 누적될 때 사전에 파악하지 못하면 실제 장애로 이어질 가능성이 크다. 따라서 집합적 이상은 근본적인 원인 파악과 해결이 필요하며 간과할 경우 심각한 문제로 발전할 수 있다. 본 연구에서 사용한 데이터셋은 기존 데이터의 불균형을 해소하고 집합적 이상 탐지의 성능을 높이기 위해 집합적 이상 데이터를 추가로 생성했다.

2.2 칼만 필터

데이터에서 신호를 예측하고 잡음을 제거하며 최적의 상태 추정을 수행하는 데 널리 사용되는 방법론이다. 확률론적 접근 방식을 기반으로 시스템의 동적인 상태를 추정하며 통신 및 제어 시스템에서의 예측 문제를 해결하기 위해 개발되었다[3].

2.3 트랜스포머

기존 순환 신경망(RNN) 기반 모델을 대체할 수 있는 아키텍처로 Self-attention 메커니즘을 사용하여 시퀀스 데이터의 의존성을 학습한다. Self-attention 메커니즘은 시퀀스 내의 각 위치가 다른 모든 위치와 상호작용할 수 있도록 하여 시퀀스 길이에 관계없이 전체적인 의존성을 효율적으로 학습할 수 있다[4].

2.4 딥러닝 모델 기반 이상 탐지

이 절에서는 시계열 데이터에서 이상 탐지 분야에서 활용되는 딥러닝 모델들을 살펴본다.

LSTM-AE 모델은 LSTM 기반의 인코더와 디코더 구조로 구성되어 있다. 주어진 입력 시퀀스를 고차원 벡터로 인코딩한 후 원래 시퀀스로 디코딩하여 재구성 오류를 계산한다. 재구성 오류를 기반으로 이상 탐지하며 재구성 오류가 클수록 이상 가능성이 높다고 판단한다[5].

USAD 모델은 두 개의 AE 구조를 활용하여 적대적 학습을 적용한 모델이다. 첫 번째 AE 는 입력 데이터를 재구성하고 두 번째 AE 는 첫 번째 AE 의 출력을 재구성한다. 이 과정에서 재구성 오류가 이상 입력에 대해 증폭되며 이상 탐지 성능을 향상시킨다[6].

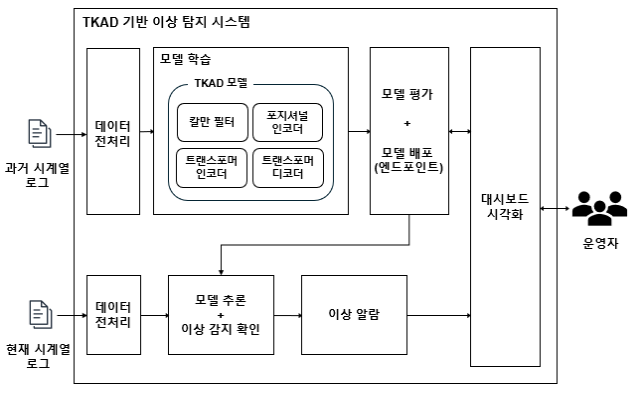
TadGAN 모델은 생성적 적대 신경망(GAN)을 활용하여 시계열 데이터의 이상 탐지하는 모델이다. LSTM 기반의 Generator 와 Critic 으로 구성되어 Generator 는 정상적인 시계열 데이터를 학습하고 데이터를 재구성한다. Critic 은 Generator 가 생성한 데이터와 실제 데이터를 비교하여 생성된 데이터가 실제 데이터와 유사한지 평가하고 재구성 오류와 Critic 의 출력을 결합하여 이상 탐지한다[7].

TranAD 모델은 트랜스포머 구조를 활용하여 데이터를 인코딩하는 시점에 패턴과 정보를 학습하고 디코딩하는 시점에 재구성 오류를 기반을 이상 탐지한다. 한 개의 인코더와 두 개의 디코더를 사용하고 Self-conditioning 과 적대적 학습을 적용하여 높은 성능의 이상 탐지를 보여준다[8].

3. TKAD 기반 이상 탐지 제안

3.1 시스템 구성도

시스템의 전체 구성은 (그림 1)과 같이 데이터 전처리, 모델 학습, 모델 평가, 모델 배포, 모델 추론의 단계로 이루어진다. 모델 학습 단계에서는 TKAD 모델을 사용하며 평가 단계에서는 기간별로 학습된 여러 버전의 성능을 비교하고 이상 탐지 임계치를 갱신한다. 배포 단계에서는 평가 결과를 바탕으로 선정된 모델과 임계치를 적용해 시스템에 배포한다. 추론 단계에서는 신규로 발생한 시계열 로그를 배포된 모델과 API 통신을 통해 감지하여 이상 여부를 판단하고 운영자에게 알람과 모니터링 대시보드를 제공한다.



(그림 1) TKAD 기반 이상 탐지 시스템 구성도

3.2 TKAD 모델

TKAD 모델은 시계열 데이터에서 발생하는 노이즈를 제거하고 이상 탐지의 정확도를 높이기 위해 칼만 필터와 트랜스포머 구조를 결합한 모델이며 작동 알고리즘은 아래 Algorithm1 에 요약되어 있다. 노이즈가 많은 환경에서 우수한 성능을 발휘하며 다음과 같이 4 개의 모듈로 구성된다.

칼만 필터(Kalman Filter): 시계열 데이터의 노이즈를 제거하는 첫 단계로 상태 전이 행렬(A)과 관측 행렬(H)을 사용해 현재 상태를 예측하고 과정 노이즈(Q)와 관측 노이즈(R)를 고려하여 상태를 업데이트한다. 이를 통해 트랜스포머 입력으로 사용될 정제된 저차원 벡터를 생성한다.

포지셔널 인코더(Positional Encoder): 칼만 필터로 정제된 데이터와 원본 데이터를 결합해 시간적 위치 정보를 반영한다. 트랜스포머 구조가 시계열 데이터의 시간 의존성을 학습할 수 있도록 돕는다.

트랜스포머 인코더(Transformer Encoder): 포지셔널 인코더가 반영된 데이터를 받아 Self-attention 메커니즘을 통해 복잡한 시간적 패턴과 데이터 간 관계를 학습한다. 이 단계에서 중요한 패턴이 추출된다.

트랜스포머 디코더(Transformer Decoder): 트랜스포머 인코더 출력을 바탕으로 시계열 데이터의 미래 상태를 예측하며 손실을 계산해 모델 성능을 지속적으로 개선한다.

Algorithm1. TKAD Training Algorithm

Requirements:
Kalman Filter K, Positional Encoder E_p, Transformer Encoder E_t, Transformer Decoder D_t
Time-series Dataset W
Learning rate α
Maximum iterations N
1. Initialize weights for K, E_p, E_t, D_t
2. Set $n \leftarrow 0$
3. **do**
4. for each time step t in the dataset W:
5. Apply Kalman Filter K to remove noise: $K(W_t)$
6. Encode filtered data and original data using Positional Encoder: $E_p(K(W_t)+W_t)$
7. Learn patterns using Transformer Encoder: $H_t = E_t(E_p(K(W_t)+W_t))$
8. Predict future states using Transformer Decoder: $O_t = D_t(H_t)$
9. Compute loss between prediction and actual data: $L = \|O_t - W_t\|^2$
10. Update weights of K, E_p, E_t, D_t using the loss L and learning rate α
11. $n \leftarrow n + 1$
12. **While** $n < N$

3.3 학습 기간 설정에 따른 최적 임계치 갱신

서비스 고도화에 따른 시스템 구조의 변화에 유연하게 대응하기 위해 다양한 학습 기간을 설정하여 주기적으로 모델을 재학습하고 성능을 비교하여 가장 높은 정확도를 보이는 모델을 선정해 임계치를 업데이트한다. 예를 들어 데이터 패턴이 급변할 경우 짧은 학습 기간의 모델이 정확도가 높을 수 있으며 데이터 패턴이 안정적일 경우 긴 학습 기간의 모델이 더 신뢰성 있는 결과를 제공할 수 있다.

4. 실험 및 결과

4.1 데이터 구성

실험에 사용한 데이터는 IoT 운영 시스템의 CPU, 메모리, 네트워크, 디스크, 데이터베이스 영역에서 수집된 8 개의 메트릭으로 구성되며 1 분 간격으로 수집 서버에 적재되어 있다. 데이터셋은 <표 1>과 같이 Train, Validation, Test 세 가지로 분할했으며 Train 데이터셋은 기간별 학습을 위해 추가적으로 세 구간으로 나누었다. 각 구간에는 2.1 절에서 정의한 집합적 이상 데이터를 포함하여 최대 10% 비율로 생성하여 실험에 활용했다.

<표 1> IoT 운영 시스템의 데이터셋 설정

구분	기간	포인트 수	길이	차원 수	노이즈	이상치 비율
Train1	2023년 10 ~ 12월	1,059,840개	132,480분	8	O	5%
Train2	2023년 7 ~ 12월	2,119,680개	264,960분	8	O	5%
Train3	2023년 1 ~ 12월	4,204,800개	525,600분	8	O	5%
Validation	2024년 1월	357,120개	44,640분	8	O	10%
Test	2024년 2월	334,080개	41,760분	8	O	10%

4.2 학습 파라미터 설정

TKAD 모델의 학습 파라미터는 <표 2>와 같이 설정했다. Window Size 는 5 부터 30 까지 실험했으며 10 일 때 F1-Score 가 다른 크기보다 최대 10% 높았다. Window Size 가 크면 한 번에 학습하는 데이터 구간이 길어지지만 짧은 이상 패턴을 놓칠 수 있고 너무 작으면 데이터 포인트의 주변 상황을 충분히 반영하지 못해 성능이 떨어질 수 있다. 다른 비교 모델들은 원 논문에 제시된 설정값을 유지하여 성능 비교가 이루어지도록 했다.

<표 2> TKAD 모델의 학습 파라미터 설정

학습 파라미터	설정 값
Window Size	10
Encoder Layers	2
Hidden Units	128
Dropout Rate	0.1
Number of Epochs	50
Batch Size	128
Learning Rate	0.001
Optimizer	Adam

4.3 이상 탐지 성능 비교

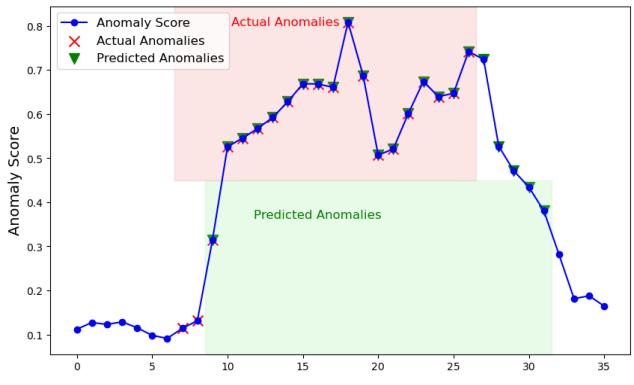
기간별로 누적된 데이터를 사용하여 학습된 모델들의 이상 탐지 성능을 비교했다. 성능 평가는 F1-Score, AUC, Precision, Recall 지표를 기준으로 수행하였다. F1-Score 는 정확도(Precision)와 재현율(Recall)의 조화평균이고 AUC 는 ROC 곡선 아래 면적으로 이진 분류 성능을 나타내며 값이 1 에 가까울수록 성능이 우수함을 의미한다. <표 3>은 전체 모델의 성능을 보여주며 TKAD 모델이 F1-Score, AUC 지표에서 다른 모

델보다 모두 우수한 성능을 보였다.

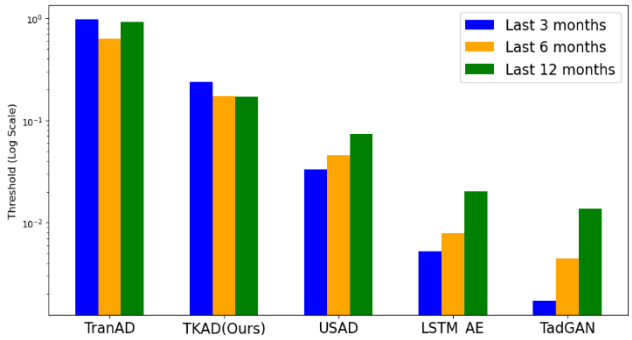
특히 최근 3 개월간의 데이터로 학습한 TKAD 모델이 가장 높은 F1-Score 성능을 보였는데 최신 데이터가 최근의 패턴과 변동성을 잘 반영했기 때문이다. F1-Score 가 0.6 으로 낮아 보일 수 있으나 집합적 이상을 개별 포인트 단위로 평가했기 때문이다. (그림 2)에서 볼 수 있듯이 TKAD 모델은 집합적 이상 구간을 포함한 대부분의 이상을 탐지하였다. (그림 3)은 학습 기간에 따라 각 모델의 최적 임계값 변화를 보여준다. TKAD 모델은 학습 기간에 따라 임계값이 비교적 안정적으로 유지되었으며 성능 변동성을 줄이는데 효과적이었다.

<표 3> 전체 모델의 이상 탐지 성능 비교

Train Period	Model	F1	AUC	Precision	Recall
Train1 (Last 3 Months)	**TKAD (Ours)**	**0.6009**	**0.9336**	**0.5995**	**0.6023**
	TranAD	0.5325	0.8791	0.5312	0.5337
	USAD	0.2239	0.6624	0.2234	0.2244
	LSTM-AE	0.2761	0.7549	0.2755	0.2767
	TadGAN	0.4698	0.8800	0.4688	0.4709
Train2 (Last 6 Months)	**TKAD (Ours)**	**0.5012**	**0.8602**	**0.5000**	**0.5023**
	TranAD	0.2552	0.6994	0.2546	0.2558
	USAD	0.2390	0.6681	0.2384	0.2395
	LSTM-AE	0.2378	0.7178	0.2373	0.2384
	TadGAN	0.2691	0.7322	0.2685	0.2698
Train3 (Last 12 Months)	**TKAD (Ours)**	**0.5081**	**0.8618**	**0.5069**	**0.5093**
	TranAD	0.2947	0.7124	0.2940	0.2953
	USAD	0.1624	0.5806	0.1620	0.1628
	LSTM-AE	0.1937	0.6669	0.1933	0.1942
	TadGAN	0.2529	0.7234	0.2523	0.2535



(그림 2) TKAD 모델의 집합적 이상 탐지



(그림 3) 학습 기간에 따른 모델별 최적 임계값

5. 결론

본 연구에서는 칼만 필터와 트랜스포머 구조를 결합하고 주기적 학습을 통해 최적의 임계치를 자동으로 반영하는 TKAD 기반 이상 탐지 시스템을 제안하였다. 운영 중인 클라우드 환경에서 다른 4 가지 딥러닝 모델들과 성능을 비교한 결과, TKAD 모델이 LSTM-AE, USAD, TadGAN, TranAD 모델에 비해 F1-Score, AUC 지표에서 높은 성능을 기록하며 가장 우수한 이상 탐지 능력을 보여주었다. 성능을 더욱 향상시키기 위해서는 다양한 도메인의 데이터를 적용해 모델의 일반화 성능을 평가하고 모델의 구조를 개선할 필요가 있다. TKAD 기반 이상 탐지 시스템은 클라우드 환경에서의 시계열 로그 분석과 시스템 모니터링의 효율성을 향상시킬 수 있는 잠재력을 가지고 있다. 향후 다양한 환경과 시나리오에서의 응용 가능성을 확인하는 연구를 진행하겠다.

참고문헌

[1] Sarah Park, “국내 퍼블릭 클라우드 서비스 시장 개요(2023-2027): 탄소 정책 및 생성형 AI 의 영향”, IDC Korea Ltd, 2023.

[2] Kukjin Choi, Jihun Yi, Changhwa Park, Sungroh Yoon, "Deep Learning for Anomaly Detection in Time-Series Data: Review, Analysis, and Guidelines", IEEE Access, Vol. 9, 2021, pp. 120043-120065.

[3] R. E. Kalman, "A New Approach to Linear Filtering and Prediction Problems", J. Basic Eng., Vol. 82(1), 1960, pp. 35-45.

[4] Ashish Vaswani et al., "Attention is All You Need," Proceedings of NeurIPS, 2017, pp. 6000-6010.

[5] Pankaj Malhotra et al., "LSTM-based Encoder-Decoder for Multi-sensor Anomaly Detection", ICML 2016 Anomaly Detection Workshop, 2016.

[6] Julien Audibert et al., "USAD: UnSupervised Anomaly Detection on Multivariate Time Series", KDD 2020, pp. 3395-3404.

[7] Alexander Geiger et al., "TadGAN: Time Series Anomaly Detection Using Generative Adversarial Networks", IEEE Big Data, 2020, pp. 4275-4282.

[8] Shreshth Tuli et al., "TranAD: Deep Transformer Networks for Anomaly Detection in Multivariate Time Series Data", VLDB Endowment, Vol. 15(6), 2022, pp. 1201-1214.