한국컴퓨터정보학회 하계학술대회 논문집 제31권 제2호 (2023. 7)

정규화 흐름 기반 시계열 이상 탐지 시스템 연구

전영훈*, 곽정환(교신저자)O
*한국교통대학교 소프트웨어학과,
O한국교통대학교 소프트웨어학과
e-mail: 0hoon.jeon@gmail.com*, jgwak@ut.ac.krO

Research on Normalizing Flow-Based Time Series Anomaly Detection System

Younghoon Jeon*, Jeonghwan Gwak(Corresponding Author)O
*Dept. of Software, Korea National University of Transportation, Chungju, Korea,
ODept. of Software, Korea National University of Transportation, Chungju, Korea

● 요 약 ●

이상 탐지는 데이터에서 일반적인 범주에서 크게 벗어나는 인스턴스 또는 패턴을 식별하는 중요한 작업이다. 본 연구에서는 시계열 데이터의 특징 추출을 위한 비지도 학습 기반 방법과 정규화 흐름의 결합을 통한 이상 탐지 프레임워크를 제안한다. 특징 추출기는 1차원 합성곱 신경망 기반의 오토인코더로 구성되며, 정상적인 시퀀스로만 구성된 훈련 데이터를 압축하고 복원하는 과정을 통해 최적화된다. 추출된 시계열 데이터의 특징 맵은 가능도를 최대화하도록 훈련된 정규화 흐름의 입력으로 사용된다. 이와 같은 방식으로 훈련된 이상 탐지 시스템은 테스트 샘플에 대한 이상치를 계산하며, 최종적으로 임계값과의 비교를 통해 이상 여부를 예측한다. 성능 평가를 위해 시계열 이상 탐지를 위한 공개 데이터셋을 이용하여 공정하게 이상 탐지 성능을 비교하였으며, 실험 결과는 제안하는 정규화 흐름 기법이 시계열 이상 탐지 시스템에 활용될수 있는 잠재성을 시사한다.

키워드: 이상 탐지(Anomaly Detection), 시계열 (Time Series),
정규화 흐름(Normalizing Flow), 딥러닝 (Deep Learning)

I. Introduction

이상 탐지는 데이터에서 보여지는 정상 범주에서 크게 벗어나는 인스턴스 또는 패턴을 식별하는 중요한 작업이다. 최근 인공지능을 이용한 이상 탐지 기법은 침입 탐지[1], 고장 진단[2] 등 다양한 응용 분야에서 잠재적인 위협을 식별하는 데 제안되어왔다. 기존의 이상 탐지 방법으로 사용되는 이진 분류 기법은 주로 정상과 비정상 인스턴스를 구분하는 데 초점을 맞추고 있다. 하지만 비정상 샘플의 부족, 이상 현상에 대한 정의의 모호성 및 복잡성으로 인해 정상과 이상을 구분하는 것은 여전히 매우 어려운 일이다.

최근 몇 년간 정상 데이터만을 이용하여 이상 탐지 모델을 최적화하기 위한 많은 연구가 진행되고 있다. 대부분의 연구에서 정상 데이터만으로 테스크를 수행하도록 인공신경망을 학습시키면, 학습하지 않은 비정상 샘플에 대한 테스크 수행 성능이 저하된다는 가설에 근거한다. 대표적인 방법으로 오토인코더 기반 인공신경망의 복원 오류를 기반으로 이미지와 비디오 데이터의 이상을 탐지하는 모델이 제안되었다.

정규화 흐름(Normalizing Flow)은 역변환이 가능한 연속적인 함수를 이용하여 기존의 복잡한 데이터 분포를 가우시안 분포와 같은 간단한 분포로 변환하는 알고리즘이며, 최근 이상 탐지 시스템을 위한 확률 분포 모델링 기법으로 주목받고 있다. 하지만, 정규화 흐름을 기반으로 시계열 데이터의 이상 탐지에 대한 연구는 아직 초기 단계에 있으며, 이미지 데이터와는 달리 시계열 데이터는 잘 알려진 특징 추출기가 없기 때문에 이상 탐지 작업이 더욱 어려운 경향이 존재한다.

따라서, 본 논문에서는 시계열 데이터의 이상 탐지에 대한 기존 연구의 한계를 해결하기 위한 목적으로 수행되었다. 본 연구의 기여는 시계열 데이터로부터 관련 특징을 추출하기 위한 비지도 학습 기반 특징 추출기의 설계이다. 또한, 시계열 데이터의 이상 탐지를 위한 딥러닝 프레임워크를 제안한다. 최종적으로, 시계열 데이터 이상 탐지를 위한 공개 데이터셋을 사용하여 제안하는 모델을 공정하고 철저하게 평가한다.

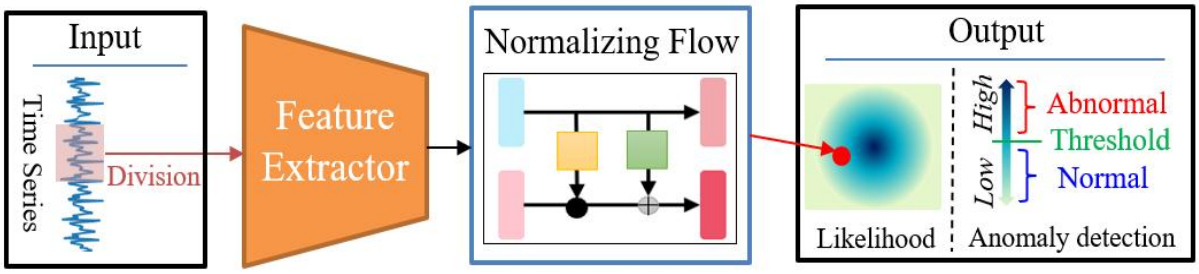

Fig. 1. Structure of Anomaly Detection System Based on Normalizing Flow

II. Related Works

심층 학습을 이용한 인공신경망을 기반으로 이상을 탐지하는 연구는 대부분 복원 기법, 표현 학습, 정규화 흐름을 기반으로 한다. 복원 기법 기반 이상 탐지는 입력된 정상 이미지에 대해 인코딩 및 디코딩을 수행하여 재구성을 목표로 신경망을 훈련시키는 방법이다. 이후, 재구성 전후의 이미지 차이를 분석하여 이상 징후를 탐지한다. 이 방법은 모델을 정상 이미지에 대해서만 훈련하면, 비정상 이미지를 올바르게 재구성할 수 없으며 이상 점수가 더 높아진다는 가정을 기반으로 한다. 이러한 방법을 통해 일반화 능력이 좋다는 장점이 있지만 이상 탐지 성능이 안정적이지 않다는 단점이 존재한다. 표현 학습 기반 이상 탐지는 전체 이미지를 설명하는 의미 있는 벡터를 추출하고, 정상 샘플들의 거리를 가능한 한 줄이는 것을 가정으로 한다. 이를 위해 심층 신경망을 특징 추출기로 훈련시켜 일반 이미지에서 추출된 특징 벡터의 분포를 가능한 한 컴팩트하게 만드는 것이 목표입니다. 이는 거리/메트릭 학습의 개념과 유사하게 작동한다. 하지만 특징 추출을 위한 백본은 일반적으로 이미지 분류를 위한 테스크에 편향되어 있기 때문에 일반화 성능이 좋지 않다. 정규화 흐름 기반 이상 탐지는 데이터 분포를 잘 정의된 밀도로 변환할 수 있는 신경망을 학습하는 방법이다. 정상 이미지의 특징을 가장 잘 추정하는 학습 가능한 프로세스를 통해 로그 우도를 최대화하여 분포를 추정한다. 그러나, 아직 이상 현상을 탐지하기 위한 확률 밀도의 적절한 추정기로서 흐름을 정규화하는 속성은 많은 관심을 받지 못하였기 때문에 아직 연구 초기 단계이다.

III. Proposed Method

Fig. 1은 본 논문에서 제안하는 정규화 흐름 기반 시계열 이상 탐지 시스템의 구조도이다. 제안하는 시스템은 단일 변수 시계열 데이터를 입력받아 비정상 여부를 출력하며, 구성요소는 특징 추출기와 정규화 흐름을 포함한다.

특징 추출기는 컴퓨터 비전 연구에서 널리 채용되고 있는 ResNet[]에서 2차원 합성곱 신경망을 1차원으로 변환한 네트워크가 사용되었다. 특징 추출기의 최적화를 위해 역합성곱 신경망으로 구성된 디코더와 결합하고, 시계열 데이터의 압축/복원을 훈련하는 비지도 학습 기반 방법론이 사용되었다,

가능도 측정을 위한 정규화 흐름 모듈로는 이상 탐지 모델로 활용되고 있는 대표적인 모델인 FastFlow[3]를 기반으로 설계되었다. 하지만, 본 연구에서 제안하는 시계열 데이터의 특징 맵은 1차원이기 때문에 2차원 합성곱 신경망을 1차원으로 교체하였다. 본 연구에서 Normalzing Flow block의 수는 6개로 설정하였다.

본 연구에서 제안하는 이상 탐지 시스템을 최적화하는 방법은 Fig. 2에서 보여진다. 최적화 프로세스는 2단계로 구성되며, 1단계는 특징 추출기 최적화를 위한 인코더-디코더의 복원 오류 최소화 학습, 2단계는 정상 샘플에 대한 가능도 최대화이다.

본 연구의 구체적인 실험환경으로 Epoch는 500, Batch size는 32, 옵티마이저는 Adam(learning rate : 0.0001)이며 모든 실험은 NVIDIA Geforce RTX 3090이 장착된 1대의 PC와 Python Library를 이용하였다.

Table 1. Comparison of Anomaly Detection Performance (AUROC) According to TSB-UAD Dataset [4]

Model	Sub-Dataset Name			
	Dodgers	MGAB	NASA-MSL	Genesis
IForest	0.79	0.57	0.57	0.78
IForest1	0.64	0.58	0.69	0.66
LOF	0.54	**0.96**	0.52	0.68
MP	0.52	0.91	0.52	0.35
PCA	0.77	0.54	0.75	0.85
NormA	0.79	0.55	0.55	0.6
HBOS	0.3	0.54	0.77	0.59
POLY	0.69	0.51	0.81	0.87
OCSVM	0.64	0.52	0.64	0.7
AE	0.73	0.71	0.7	0.72
CNN	0.68	0.58	0.57	0.73
LSTM	0.39	0.56	0.57	0.53
Proposed	**0.81**	0.92	**0.82**	**0.97**

Table 1은 시계열 이상 탐지 데이터셋인 TSB-UAD[4]을 이용하여 이상 탐지 성능인 Area Under the Receiver Operating Characteristic Curve(AUROC)를 비교한 결과이다. 이상 탐지 방법론들의 성능 비교를 위해 Isolation Forest (IForest), Local Outlier Factor (LOF), Matrix Profile (MP), Principal Component Analysis (PCA), NormA, Histogram-based Outlier Score (HBOS), Polynomial Approximation (POLY), One-Class Support Vector Machine (OCSVM), Autoencoder (AE), Convolutional Nerual Network (CNN), Long-Short Term Memory (LSTM)이 사용되었다.제안하는 시스템은 이상 탐지 시스템은 대부분의 실험에서 가장 높은 성능을 보였으며, 특히 Genesis 데이터셋에서 제안하는 시스템은 기존 방법론에 비해 약 0.10의 성능 향상을 보였다. MGAB 데이터셋을 이용한

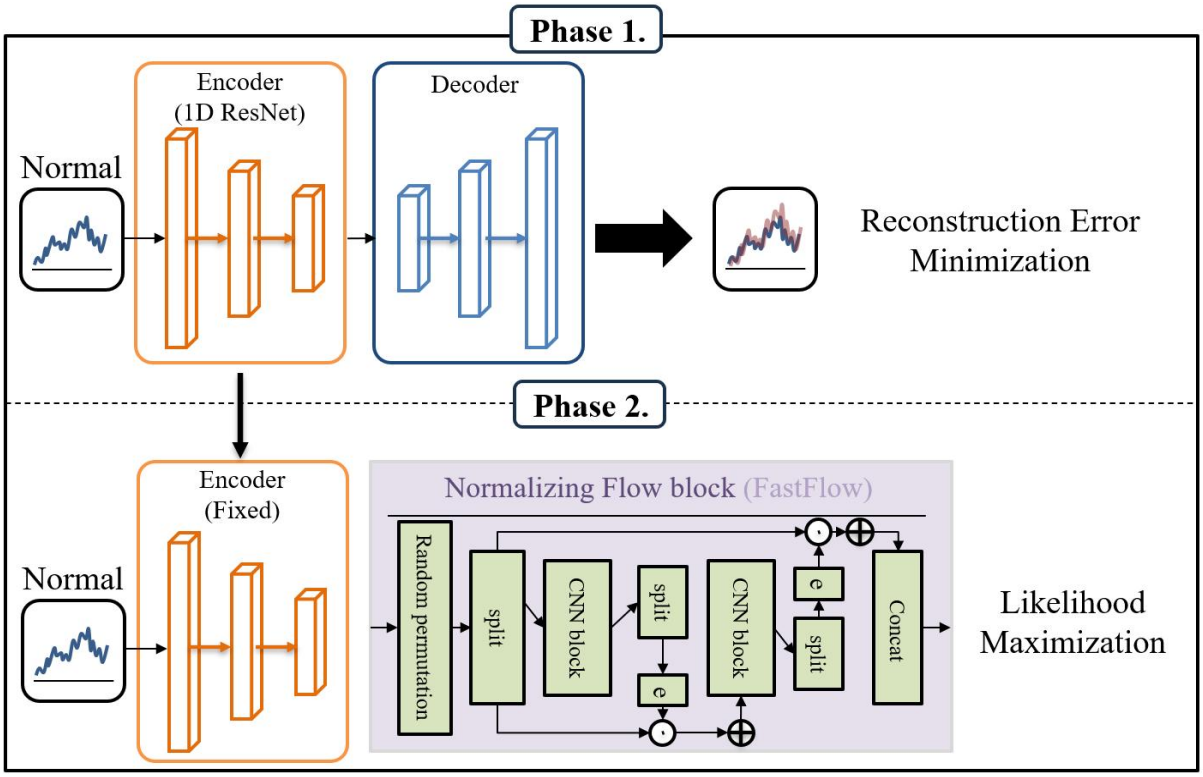

Fig. 2. Optimization Process of Anomaly Detection System Based on Normalizing Flow

실험에서는 기존 방법론에 비해 성능이 저하되었지만 그 차이는 0.04로 큰 차이를 보이지 않았다. 이는 본 연구에서 설정한 가설과 일치하며, 이를 통해 제안하는 정규화 흐름 기법이 이상 탐지를 위한 방법론으로 우수함을 시사한다.

IV. Conclusions

본 논문에서는 정규화 흐름 모듈을 기반으로 시계열 데이터의 이상을 탐지하는 모델을 설계하고, 시계열 이상 탐지를 위한 공개 데이터셋을 이용하여 성능을 비교 평가 실험을 수행하였다. 제안하는 시스템은 기존 방법론에 비해 높은 이상 탐지 성능을 보였으며, 정규화 흐름이 시계열 이상 탐지를 위한 방법론으로 활용될 잠재성을 시사한다. 향후 연구에서는 특징 추출기에 따른 정규화 흐름 기법의 비교와 정규화 흐름 모듈의 개선을 포함한다.

ACKNOWLEDGEMENT

This was supported by Korea National University of Transportation in 2023.

REFERENCES

[1] Yang, Zhen and Liu, Xiaodong and Li, Tong and Wu, Di and Wang, Jinjiang and Zhao, Yunwei and Han, Han, "A systematic literature review of methods and datasets for anomaly-based network intrusion detection," pp. 102675, 2022

[2] Soldani, Jacopo, and Antonio Brogi. "Anomaly detection and failure root cause analysis in (micro) service-based cloud applications: A survey." ACM Computing Surveys (CSUR), Vol. 55, No. 3, pp. 1-39, 2022.

[3] Yu, Jiawei, et al. "Fastflow: Unsupervised anomaly detection and localization via 2d normalizing flows." arXiv preprint arXiv:2111.07677, 2021.

[4] Paparrizos, John, et al. "TSB-UAD: an end-to-end benchmark suite for univariate time-series anomaly detection." Proceedings of the VLDB Endowment , Vol. 15, No. 8, pp. 1697-1711, 2022.