ISSN 2288-4866 (Print)
ISSN 2288-4882 (Online)
http://www.jiisonline.org
J Intell Inform Syst 2021 September: 27(3): 57~73 http://dx.doi.org/10.13088/jiis.2021.27.3.057

ICT 인프라 이상탐지를 위한 조건부 멀티모달 오토인코더에 관한 연구

신병진
모아데이타
(bjshin@moadata.co.kr)

이종훈
모아데이타
(jhlee@moadata.co.kr)

한상진
모아데이타
(sjhan@moadata.co.kr)

박충식
U1대학교
(leciel@u1.ac.kr)

ICT 인프라의 이상탐지를 통한 유지보수와 장애 예방이 중요해지고 있다. 장애 예방을 위해서 이상탐지에 대한 관심이 높아지고 있으며, 지금까지의 다양한 이상탐지 기법 중 최근 연구들에서는 딥러닝을 활용하고 있으며 오토인코더를 활용한 모델을 제안하고 있다. 이는 오토인코더가 다차원 다변량에 대해서도 효과적으로 처리가 가능하다는 것이다. 한편 학습 시에는 많은 컴퓨터 자원이 소모되지만 추론과정에서는 연산을 빠르게 수행할 수 있어 실시간 스트리밍 서비스가 가능하다.

본 연구에서는 기존 연구들과 달리 오토인코더에 2가지 요소를 가미하여 이상탐지의 성능을 높이고자 하였다. 먼저 다차원 데이터가 가지고 있는 속성별 특징을 최대한 부각하여 활용하기 위해 멀티모달 개념을 적용한 멀티모달 오토인코더를 적용하였다. CPU, Memory, network 등 서로 연관이 있는 지표들을 묶어 5개의 모달로 구성하여 학습 성능을 높이고자 하였다. 또한, 시계열 데이터의 특징을 데이터의 차원을 늘리지 않고 효과적으로 학습하기 위하여 조건부 오토인코더(conditional autoencoder) 구조를 활용하는 조건부 멀티모달 오토인코더(Conditional Multimodal Autoencoder, CMAE)를 제안하였다. 제안한 CAME 모델은 비교 실험을 통해 검증했으며, 기존 연구들에서 많이 활용된 오토인코더와 비교하여 AUC, Accuracy, Precision, Recall, F1-score의 성능 평가를 진행한 결과 유니모달 오토인코더(UAE)와 멀티모달 오토인코더(Multimodal Autoencoder, MAE)의 성능을 상회하는 결과를 얻어 이상탐지에 있어 효과적이라는 것을 확인하였다.

주제어 : 이상탐지, 멀티모달, 인공지능, 오토인코더, 시스템 모니터링

논문접수일 : 2021년 5월 21일 논문수정일 : 2021년 6월 24일 게재확정일 : 2021년 6월 30일
원고유형 : 학술대회 Fast-Track 교신저자 : 박충식

1. 개요

1.1. 연구의 배경 및 목적

코로나로 인하여 대외적인 활동의 제한으로 비대면 서비스와 활동이 점차 증가하는 추세이며, 많은 기업이 서비스와 애플리케이션을 융합한 플랫폼 형태로 비즈니스를 확장하고 있다. 이용자의 수 또한 폭발적으로 증가하였으며, 서비스 중단 시 피해액이 커지고 있다. 따라서, 시스템 가용성을 높이고, 서비스 품질을 높이는 것은 기업의 신뢰도와 수익 측면에서 중요한 요소이

다. 시스템 모니터링을 활용하여 장애에 대응하고 있으나, 운영자(operator)가 시스템의 모든 성능 지표(performance metric)를 직접 확인하고 관리하는 것에는 어려움이 있다(D. Lee, 2017). 이러한 문제를 해결하기 위해 기계학습을 고려하고 있으며, 특히 인공신경망을 활용하여 이상 탐지를 자동화하고자 하는 연구가 수행되었다.

이상 탐지는 확률적 모델과 선형 모델, 거리 및 근접 기반 모델, 기계 학습 기반 모델 등이 사용된다(Aggarwal, 2017). 확률적 모델에는 극한값 분석(extreme value analysis)(P. Billingsley, 1986; V. Barnett and T. Lewis., 1994; S. Roberts., 1999)과 깊이 기반(depth-based) 방법(T. Johnson, I. Kwok, and R. Ng., 1998; I. Ruts and P. Rousseeuw., 1996), 편차 기반(deviation-based) 방법(A. Arning, R. Agrawal, and P. Raghavan., 1996), 각도 기반(angle-based) 방법(H.-P. Kriegel, M. Schubert, and A. Zimek., 2008; M. Radovanovic, A. Nanopoulos, and M. Ivanovic., 2010; J. Laurikkala, M. Juholal, and E. Kentala., 2000; M.-L. Shyu, S.-C. Chen, K. Sarinnapakorn, and L., 2003), 거리 기반(distance-based) 방법(R. De Maesschalck, D. Jouan-Rimbaud, D.L. Massart, 2000; D. Pokrajac, A. Lazarevic, and L. Latecki., 2007; P. Rousseeuw and A. Leroy., 2003) 등이 있다. 선형 모델에는 주성분 분석(PCA, Principal Component Analysis), 선형 회귀 모델 등이 있다. 확률적 모델과 선형 모델은 모형을 간단하게 하여 적용이 간단하며, 해석하기 쉽다는 장점이 있다. 다만 이러한 모델들의 주요한 문제점은 로컬 특이치(Local outlier)를 감지하기 어려우며, 차원이 커질수록 성능이 떨어지는 한계가 있다(Y. Bengio and Y. LeCun, 2007). 또한 데이터의 증가에 따라 연산량이 크게 증가하여 실제 적용에는 한계가 존재한다(C. C. Aggarwal, 2017).

이러한 문제를 해결하기 위하여 인공 신경망 비지도 학습의 일종인 오토인코더(Autoencoder)를 활용할 수 있다. 오토인코더를 사용할 경우 잠재 공간(latent space)으로 차원을 축소하여 데이터의 특징을 효과적으로 나타낼 수 있다(G. E. Hinton and R. R. Salakhutdinov, 2006). 시스템 모니터링 분야에서의 이상탐지는 다차원 시계열 데이터에서 발생하는 문제점들에 대한 보완이 필요하다. 기존 연구에서는 시계열 데이터를 위해 주로 사용되는 RNN의 LSTM, GRU 등의 레이어로 신경망을 구성한 연구들을 수행하였다(D. Lee, 2017; Y. Su, Y. Zhao, C. Niu, R. Liu, W. Sun and D. Pei, 2019). 또한 Counter를 활용하여 False positive가 과도하게 많이 발생되는 문제점을 보완하고자 하는 시도가 있었다. 본 연구에서는 시계열 데이터의 문제를 해결하기 위하여 조건부 입력(conditional inputs)을 추가하였으며, 입력 변수를 모달별로 구성하여 다차원 데이터를 효과적으로 다룰 수 있도록 멀티모달 오토인코더를 구성하였다. 멀티모달은 일반적으로 음성과 영상과 같이 서로 다른 형태의 입력을 함께 학습하기 위해 사용되는데 본 연구에서는 CPU, Memory, Disk, Network, Process를 각각의 모달로 정의하였다. 멀티모달 신경망 구조를 통해 오토인코더의 병목 효과를 서로 다른 모달이 공유하여 상관관계를 학습하게 된다. 조건부 입력을 사용하게 되면 같은 병목 구간을 사용하여도 결과값을 조절할 수 있다는 장점이 있다. 시계열적인 요소를 반영하기 위하여 시간을 조건부 입력으로 사용하였다. 최종 제안하고자 하는 모델은 조건부 멀티모달 오토인코더(CMAE: Conditional Multi-modal AutoEncoder)이다.

1.2. 연구 범위 및 방법

오토인코더를 활용한 이상탐지는 입력 데이터를 복원(reconstruction)하여 이상 점수를 산출하는 과정과 임계치를 활용하여 이상을 탐지하는 과정으로 나뉜다. 이상탐지의 성능을 결정하는 것은 오토인코더의 구조와 임계치를 산정하는 과정 모두에 해당한다. 따라서 정상 데이터에 대한 복원 성능과 정상/이상 상태에 따른 임계치가 뚜렷이 구분되는지 확인해야 한다. 최종적으로 탐지 성능을 비교하여 이상탐지 모델의 성능을 비교한다. 본 연구에서는 기존 오토인코더의 문제점을 개선하기 위하여 CMAE를 제안하였다. 제안한 모델의 성능을 검증하기 위하여 UAE (Unimodal Autoencoder) 모델과 MAE(Multimodal Autoencoder)와 성능을 비교하여 제안한 모델에 대한 우수성을 검증하였다.

성능 비교를 위하여 이상 탐지에 가장 유효할 것으로 판단되는 5개의 모달(CPU, Memory, Network, Process, Disk)에서, 총 41개의 성능 정보를 수집하였다. 데이터는 에이전트(agent)를 통하여 서버의 성능 정보를 수집하였다. 여기서 수집 주기는 10초이며, 2일 간의 데이터를 정제하여 사용하였다. 해당 기간에는 장애가 발생하지 않은 정상 데이터만을 수집하였다. 데이터는 총 17280개()가 수집되었다. 이상 탐지의 성능을 평가하기 위하여 정상 데이터를 기반으로 이상 데이터를 생성하였다. 이상데이터는 정확한 성능 평가를 위하여 1) 스케일링, 2) 이상 패턴 추가, 3) 화이트 노이즈 추가의 단계를 수행하였다(Y. Pei and O. Zaiane, 2006). 이상 패턴은 약한 특이치(weak outlier)와 강한 특이치(strong outlier)가 결합된 형태로 4가지 유형으로 구성하였다. 이상 패턴에 균일 분포(uniform distribution)를 이용하여 화이트 노이즈를 추가하였다.

2. CMAE를 활용한 이상 탐지

2.1. 이상탐지 관련 연구

이상탐지는 확률적 모델과 선형 모델, 거리 및 근접 기반 모델, 기계 학습 기반 모델 등이 사용된다(Aggarwal, 2017). 확률적 모델에는 극한값 분석(extreme value analysis)(P. Billingsley, 1986; V. Barnett and T. Lewis., 1994; S. Roberts., 1999)과 깊이 기반(depth-based) 방법(T. Johnson, I. Kwok, and R. Ng., 1998; I. Ruts and P. Rousseeuw., 1996), 편차 기반(deviation-based) 방법(A. Arning, R. Agrawal, and P. Raghavan., 1996), 각도 기반(angle-based) 방법(H.-P. Kriegel, M. Schubert, and A. Zimek., 2008; M. Radovanovic, A. Nanopoulos, and M. Ivanovic., 2010; J. Laurikkala, M. Juholal, and E. Kentala., 2000; M.-L. Shyu, S.-C. Chen, K. Sarinnapakorn, and L., 2003), 거리 기반(distance-based) 방법(R. De Maesschalck, D. Jouan-Rimbaud, D.L. Massart, 2000; D. Pokrajac, A. Lazarevic, and L. Latecki., 2007; P. Rousseeuw and A. Leroy., 2003) 등이 있다. 선형 모델에는 주성분 분석(PCA, Principal Component Analysis), 선형 회귀 모델 등이 있다. 확률적 모델과 선형 모델은 모형을 간단하게 하여 적용이 간단하며, 해석하기 쉽다는 장점이 있다.

이상탐지 분야는 전통이 깊은 연구 분야로 초기에는 통계적인 방법과 회귀분석을 주로 사용하였으며, 현재는 기계학습(M. Amer, 2013; P. Juszczak and R. P. W. Duin, 2003; B. Raskutti and A. Kowalczyk, 2004)과 인공신경망(V. Ciesielski

and V. Ha, 2009)을 적용하는 연구가 활발하게 진행되고 있다. 이상탐지는 결과물에 따라 이상 점수로 환산되는 모델과 라벨을 직접 반환하는 모델로 구분 될 수 있다. 연구 초기에는 다변량 데이터에 대한 고려와 시계열 데이터, 공간 데이터, 텍스트 데이터 등 데이터의 유형이 고려 되지 않은 통계적인 방법들이 주를 이루었다. 통계적인 방식의 핵심적인 아이디어는 정규 분포를 활용하여 극단에 존재하는 발생 확률이 낮은 지점을 찾는 것이다. 데이터를 정규분포로 가정하여 관측값의 유의확률을 z-test를 통해 이상을 탐지한다. 이러한 방식은 단변량에는 적용이 용이하나, 다변량의 경우 적용에 어려움이 있다. 다변량의 경우 데이터는 기하학적 거리(Euclidian distance)를 계산하거나, PCA를 적용하여 차원을 축소하기도 한다. 거리 기반의 경우 연산량이 으로 데이터양의 증가에 효과적으로 대응하기 어려우며, PCA는 변수 간 스케일에 큰 영향을 받는다. 이에 대한 보완으로 변수 간 상관관계를 고려할 수 있으며, 고유 벡터(Eigen vector)를 활용하여 효과적으로 계산되는 Mahalanobis 거리를 활용할 수 있다(R. De Maesschalck, D. Jouan-Rimbaud, D.L. Massart, 2000). 이러한 통계 기반의 방법들은 데이터가 비동차형(non-homogeneous)인 경우 적용이 어렵고, 로컬 특이치(local outlier)를 잘 감지하지 못한다. 회귀분석 방법은 모수적 통계에 기반한 회귀식을 학습 후 예측 값과 실제 값을 비교하여 이상을 탐지한다. 회귀분석을 활용한 이상 탐지는 모델이 견고하지 않아 데이터의 잡음이나 이상치가 포함되어 있을 경우 성능이 저하된다는 단점이 있다. 노이즈나 이상치가 제거된 학습 데이터를 사용해야 한다는 제약이 있다.

2.2. 오토인코더를 활용한 이상탐지

오토인코더는 인공신경망을 활용한 비지도학습의 일종이다(D. Bank, N. Koenigstein and R. Giryes, 2020). 오토인코더는 인코더와 디코더가 합쳐진 구조이다. 오토인코더에는 두 가지 주요한 특징이 있다. 첫 번째 특징은 입력 데이터와 최대한 비슷하게 출력하도록 학습된다는 것이다. 학습 과정에서 별도의 라벨이나 타겟 변수가 필요 없다. 입력 데이터 그 자체를 학습한다. 두 번째 특징은 병목 효과를 주기 위하여 인코더의 출력 차원을 입력 데이터 차원보다 작게 한다는 것이다. 이러한 제약으로 인하여 인코더는 입력 데이터의 주요한 특징을 효과적으로 추출할 수 있도록 학습된다. 차원이 축소된 인코더의 출력을 잠재 공간이라 한다. 오토인코더의 또 다른 부분인 디코더의 역할은 축소된 잠재 공간에서 원래의 데이터를 복원하는 것이다. 일반적으로 잠재공간에서 데이터의 손실이 발생하기 때문에 복원된 데이터는 원본에 비해 주요하지 않은 특징들은 흐려지고 새로운 데이터를 기존 학습 데이터와 유사하게 복원하는 특징이 있다. 이를 활용하여 입력과 출력 데이터의 차이가 큰 경우 새로운 데이터나 이상이 발생했음을 감지할 수 있다. 여기서 입력과 출력 데이터의 차이를 이상 점수(Anomaly Score)로 사용하며, 임계치(Threshold)를 적용하여 이상을 탐지한다.

이러한 특성들을 이용하여 시스템 모니터링 분야에 적용한 연구에서 주요한 특징들을 조사하였다. 시스템 모니터링 데이터는 다차원의 시계열 데이터라는 특성을 가진다. 기존 연구 사례에서는 이러한 특성을 고려하기 위하여 순환신경망(RNN)인 LSTM을 오토인코더 구조에 적용하는 연구 사례가 있다. 최근에는 생성 모델에

〈Table 1〉 Pros and cons of techniques for timeseries

기법	장점	단점
슬라이딩 윈도우 기법	- 처리방법이 간단함 - 기법에 대한 이해가 쉬움	- 차원이 크게 증가로 학습 시간이 많이 소요됨 - 차원의 저주에 빠지기 쉬움
시계열 분해	- 분해를 통해 비정상(non-stationary) 데이터를 정상(stationary) 데이터로 변환 가능 - 예측 성능 향상	- 시계열 분해를 위한 매개변수 결정이 필요 - 데이터 변화 시 매번 직접 지정해야 하는 번거로움이 있음)
Conditional Autoencoder	- 시간 데이터를 조건부 입력으로 사용하여 영향을 효과적으로 학습	- 모델 구조가 다소 복잡해짐 → 다만 슬라이딩 윈도우 기법에 비해 차원 증가가 적음

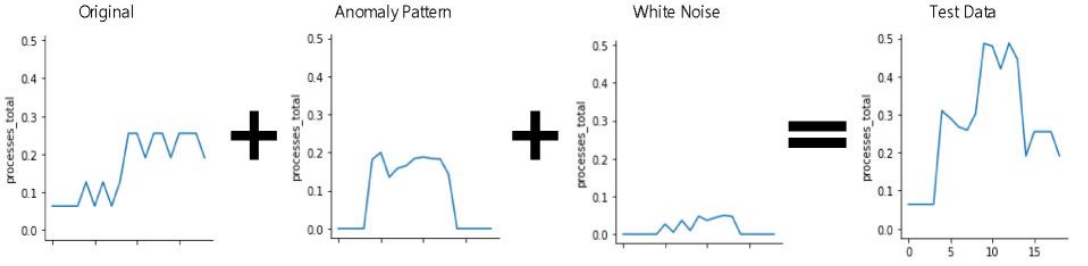
주로 사용되는 VAE(Variational Autoencoder)를 이상탐지에 활용한 연구도 존재한다(Y. Guo, W. Liao, Q. Wang, L. Yu, T. Ji and P. Li, 2018, Q. P. Nguyen, K. W. Lim, D. M. Divakaran, K. H. Low and M. C. Chan, 2019). VAE는 데이터가 평활화되는 효과가 있으며 데이터가 단일 정규분포를 따라야 한다는 제약이 있다. 이에 대한 개선을 위하여 GANs(Generative Adversary Networks)을 활용하기도 한다(V. H. Son, U. Daisuke, H. Kiyoshi, M. Kazuki, S. Pranata and S. M. Shen, 2019).

2.3. CMAE를 활용한 이상탐지

본 연구에서는 기존 연구들에서 많이 활용한 오토인코더에 2가지 요소를 가미하였으며 이는 로컬 특이치와 시계열 특성을 고려함으로써 이상탐지의 성능을 높이고자 하였다. 다차원 데이터가 가지고 있는 로컬 특이치 식별에 대한 한계점 개선을 위하여 멀티모달을 적용하였다. 멀티모달은 일반적으로 음성과 영상과 같이 서로 다른 종류의 입력을 같이 학습하기 위해 주로 사용된다. 오토인코더의 병목 효과를 서로 다른 모달이 공유하여 상관관계를 학습하게 된다(Y. Guo, W. Liao, Q. Wang, L. Yu, T. Ji and P. Li, 2018).

멀티모달 오토인코더는 서로 다른 특성을 가지는 모달들을 통합하여 학습하는 것을 말한다. 모달을 통합하는 방법은 크게 두가지로 나뉘는데 Joint representation 방식과 coordinated representation 이 있다. Joint representation은 잠재 공간을 공유하는 형태로 구성한다. coordinated representation은 잠재 공간을 따로 사용하나, 각각의 잠재 공간의 분포가 유사하도록 학습 손실에 제약을 둔다. 두 방법 모두 여러 모달의 데이터를 동시에 학습한다는 점에서 잠재 공간가 정보가 효과적으로 추출된다는 장점이 있다. 모달별로 입력 데이터의 특징을 추출할 뿐만 아니라 모달 간의 영향이 함께 학습되기 때문이다. 본 연구에서는 joint representation 형태로 구성한 멀티모달 오토인코더를 적용하였다. joint representation 형태로 구성한 경우 특정 도메인 데이터가 누락된 상황에서도 활용할 수 있다는 장점이 있다(T. Baltrušaitis, C. Ahuja, and L. Morency, 2017).

본 연구에서는 시스템 성능 데이터를 CPU, Memory, Disk, Network, Process 의 5개 모달로 구성했다. 이는 시각, 청각 등 서로 다른 형식의



〈Figure 1〉 Generating test data with anomaly pattern and white noise

데이터를 병행하는 멀티모달과 같이 시스템의 자원의 특성별로 구분함으로써 개별 모달별 특성뿐만 아니라 병합한 특성도 고려할 수 있다는 장점을 활용하였다. 또한, 시계열 데이터의 특징을 데이터의 차원을 늘리지 않고 효과적으로 학습하기 위하여 조건부 오토인코더 구조를 활용하였다. 일반적으로 조건부 입력은 카테고리 변수를 주로 사용하지만, 본 연구에서는 주기성을 학습하도록 시간을 조건으로 사용하여 구성하는 시도를 하였다. 본 실험에서는 2일 치의 제한된 데이터를 사용했기 때문에 시, 분, 초에 대한 시간을 조건으로 활용했으며, 장기간의 데이터를 학습할 시에는 주, 월, 분기 등의 주기성을 추가로 반영할 수 있다.

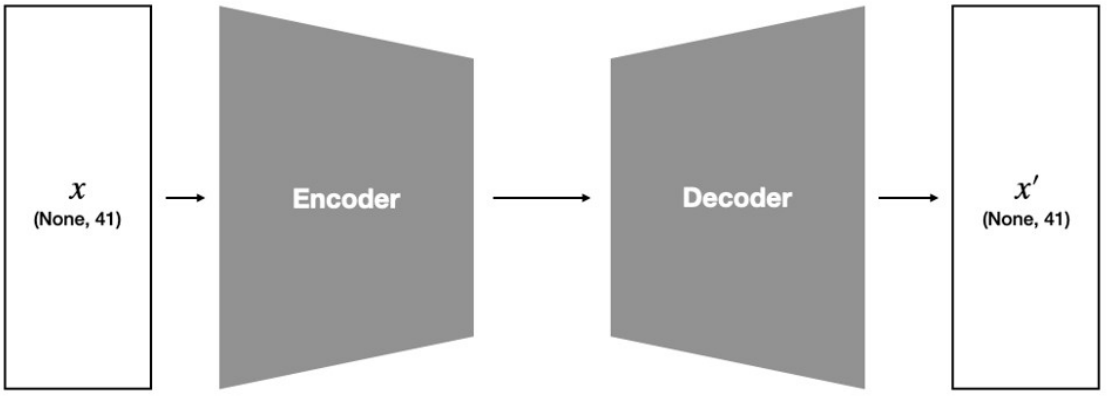
3. 오토인코더 구성 및 성능 검증 절차

3.1. 데이터 수집 및 데이터 전처리

테스트를 위한 대상 서버를 구성하였으며, 5개의 모달(CPU, Memory, Disk, Network, Process)에 대하여 총 41개의 성능 정보를 수집하였다(Table 2). 각 컬럼별 데이터의 범위가 모두 달라 Min-Max Scale을 적용하였다. 수집 주기는 10초이며, 2일 간의 데이터를 정제하여 사용하였다. 데이터는 총 17280개(2일×24(시간)×60(분)×6$\left(\frac{개}{분}\right)$)수집되었다. 학습을 위한 데이터 수집 기간에는 장애가 발생하지 않은 정상 데이터만을 수집하였다.

3.2. 이상치 데이터 생성

오토인코더 학습에는 정상 데이터만을 사용하였으며, 테스트 데이터는 이상 데이터 패턴을 추가하여 성능을 평가하였다. 이상 데이터는 일정한 이상 패턴에 화이트 노이즈를 추가하는 방법을 사용하였다(Yaling Pei and Osmar zaiane, 2006). 총 3단계로 구성하였으며, 1) 스케일링, 2) 이상 패턴 추가, 3) 화이트 노이즈 추가의 단계를 수행하였다(Figure 1). 패턴은 3가지 유형별로 3개의 레벨로 구성하여 총 9종으로 구성하였다. 화이트 노이즈는 정규분포를 사용하였다. 이상 데이터는 패턴별로 100개의 임의의 지점에 더하여 테스트 데이터를 구성하였다. Figure 1은 이상 패턴에 대한 예시이며 9,000개(3 × 3 × 10 × 100개)의 이상 데이터를 생성하였다.



〈Figure 2〉 Structure of Unimodal Autoencoder(UAE)

3.3. 모델 학습 및 성능 평가

2.2절에서 언급한 바와 같이 멀티모달과 조건부 구조를 이용하여 기존 오토인코더를 개선하고자 하였다. 오토인코더의 학습 목표는 입력 데이터를 최대한 유사하게 복원하는 것이다. 가장 기본적인 오토인코더인 유니모달 오토인코더의 구조는 Figure 2와 같다. 여기서 인코더는 입력된 전체 데이터의 차원을 축소를 통해 추출된 특징을 잠재 공간에 매핑한다. 디코더는 인코더와 반대로 잠재 공간에서 원래의 입력 데이터로 복원한다. 인코더와 디코더는 각각 θ와 $\varnothing$의 학습 파라미터를 학습하며, 병목 효과를 위하여 $x \in \mathbb{R}^m$, $z \in \mathbb{R}^n$일 때, $n < m$을 만족하도록 구성하여야 한다.

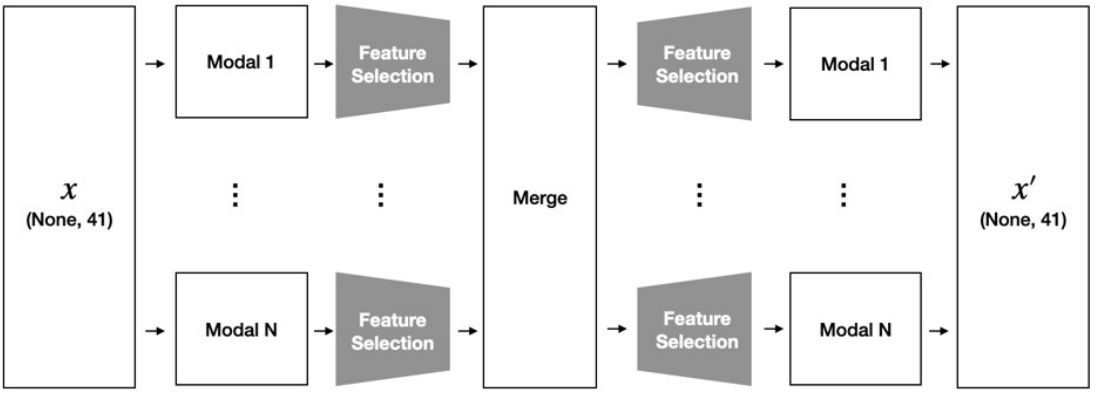
$$\text{Encoder: } p_\theta(x) = z$$
$$\text{Decoder: } q_\phi(z) = \hat{x}$$

학습 시 손실 함수(loss function)는 MSE (mean squared error)를 사용하였으며, 아래 식과 같이 표현된다.

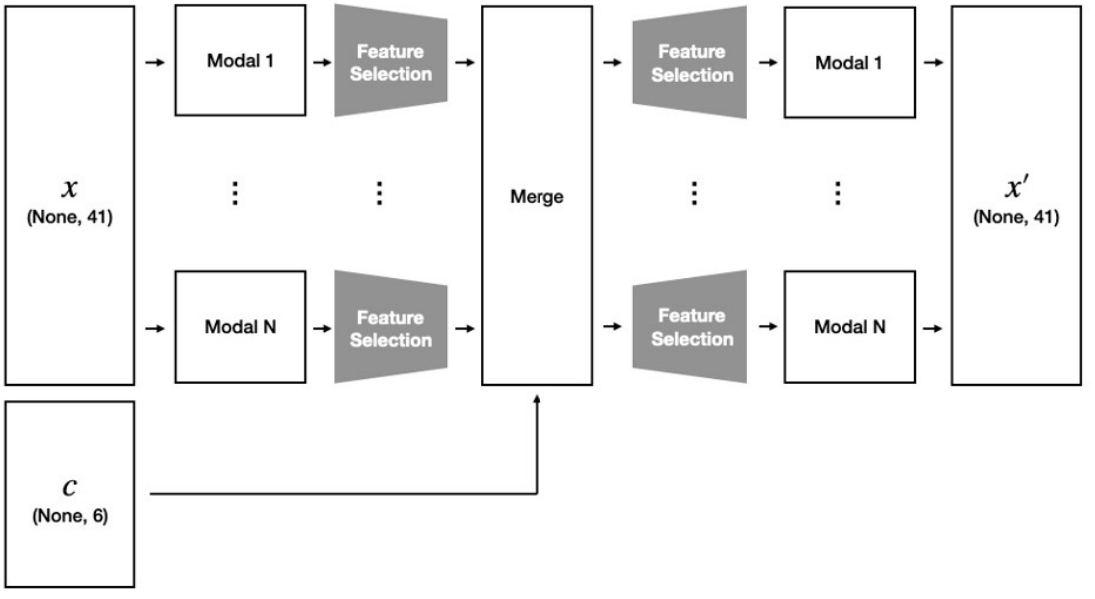
$$argmin_{\theta,\phi} mean\ squared\ error(x - q_\phi(p_\theta(x)))$$

Figure 3는 MAE의 구조를 나타낸 것이다. 앞서 설명한 바와 같이 모달별로 학습 될 수 있도록 구성하였다. 각 모달에서 차원이 축소되는 특징 추출(Feature selection) 과정은 레이어가 연결되지 않고, 축소 후 병합되는 레이어(Merge layer)를 통해 잠재 공간(latent space)만을 공유하도록 구성되어 있다. 이러한 과정을 통하여 모달별로 데이터의 특징을 효과적으로 추출하여 학습할 수 있게 된다.

Figure 4는 본 연구에서 제안하고자 하는 CMAE를 표현한 것이다. 데이터를 복원 시 시간 조건을 추가하여 성능을 높일 수 있도록 구성하였다. Figure 3와 비교하면 MAE의 잠재 공간인 병합 계층(Merge layer)에 조건부 입력 부분이 추가된 것을 확인할 수 있다. 본 연구에서 조건부 입력은 시간을 직접 추가하는 것이다. 여기서 시간이 가지고 있는 주기적 특징을 고려하기 위해



〈Figure 3〉 Structure of multi-modal autoencoder (MAE)



〈Figure 4〉 Structure of conditional multi-modal autoencoder (CMAE)

서 시간은 sin 함수와 cos 함수를 활용하여 계산하였다. 2.3절에서 언급한 바와 같이 입력 차원이 증가하는 것을 최소화하면서 시계열 데이터의 특징을 효과적으로 학습할 수 있다.

3.4. 이상탐지 성능 평가

이상탐지는 앞서 언급한 바와 같이 2가지 과정으로 구성되어있으며, 각각 오토인코더 모델과 임계치 산정 결과에 영향을 받는다. 따라서

〈Table 3〉 Results of training

Modal name	Losses by modal		
	UAE	MAE	CMAE
CPU	0.0017	0.0008	0.0004
Memory	0.0001	0.0001	0.0001
Disk	0.0001	0.0003	0.0001
Network	0.0002	0.0	0.0
Processes	0.0018	0.0018	0.0018

각 프로세스에 대한 평가가 필요하다. 오토인코더 모델이 산출하는 이상점수는 정상 데이터와 이상 데이터에 대한 분포가 뚜렷하게 구별되어야 한다. 이에 대해 확인하기 위한 방법으로 box plot과 paired t-test 방법을 사용하였다.

알고리즘은 점수 산출 과정과 점수를 기반으로 이상을 탐지하는 과정으로 이루어져있다. 따라서, 이상 점수 산출에 대한 결과와 이상 탐지 성능을 모두 평가하였다. 이상과 정상 그룹 간의 이상 점수 분포가 명확하게 구분되는 지에 대하여 정량적으로 평가하기 위하여 paired t-test를 수행하였다. t-score를 계산하고 이를 이용하여 정규분포상에서의 p-value로 환산하여 가설을 검증한다. t-score는 두 집단의 차이의 평균($\overline{D}$)과 편차(S_d)를 이용하여 계산된다.

$$\overline{D} = \frac{\sum_{i=1}^{n}\left(X_{A,i} - X_{B,i}\right)}{n}$$

$$S_D = \sqrt{\frac{\sum_{i=1}^{n}\left(X_{A,i} - X_{B,i} - \overline{D}\right)^2}{n-1}}$$

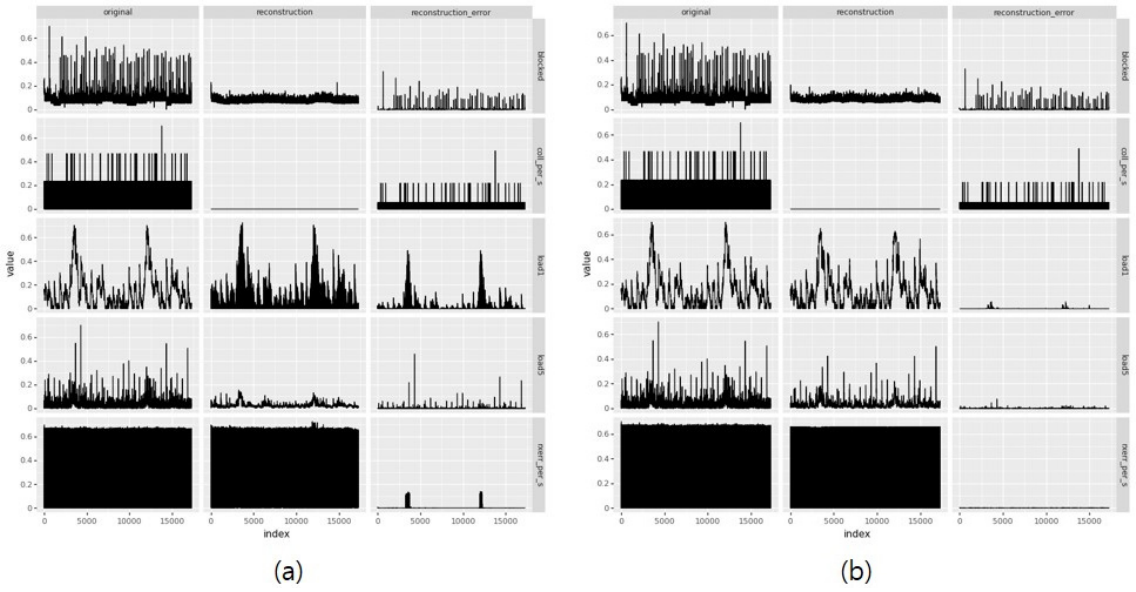
$$\mathrm{t} = \frac{\overline{D} - d_0}{S_d/\sqrt{n}}$$

오토인코더를 활용하여 산출된 이상 점수가 이상 탐지에 효과적인지 확인하기 위하여 ROC curve를 적용하였다. ROC curve는 이진 분류에서 임계치의 변화에 따른 True Positive Rate과 False Positive Rate을 비교한 것이다. ROC curve의 면적인 AUC가 1에 가까울수록 분류 성능이 좋은 모델로 판정할 수 있다.

4. CAME 모델의 평가 결과

4.1. 복원(Reconstruction) 성능 평가

41개의 변수에 대한 오토인코더의 복원 성능을 확인하였다. 변수별로 복원 성능에 차이가 있으며, Table 3와 같이 모달별 복원 성능을 비교하였다. 3개의 오토인코더 모델 모두 Memory, Disk, Network 모달에 대해서는 손실 값이 작아 복원이 정상적으로 잘 동작함을 알 수 있다. Process는 3개의 모델 모두 큰 차이를 보이지 않았으며, CPU 모달은 CMAE의 경우 성능이 우수하게 나타났다. Figure 5는 원본 데이터와 복원한 데이터를 비교한 것으로 첫번째 열은 원본, 두 번째 열은 복원 데이터, 세 번째 열은 오차를 나타낸 것이다. Figure 5는 가장 큰 차이를 보이는 AE와 CMAE를 비교한 것이다.

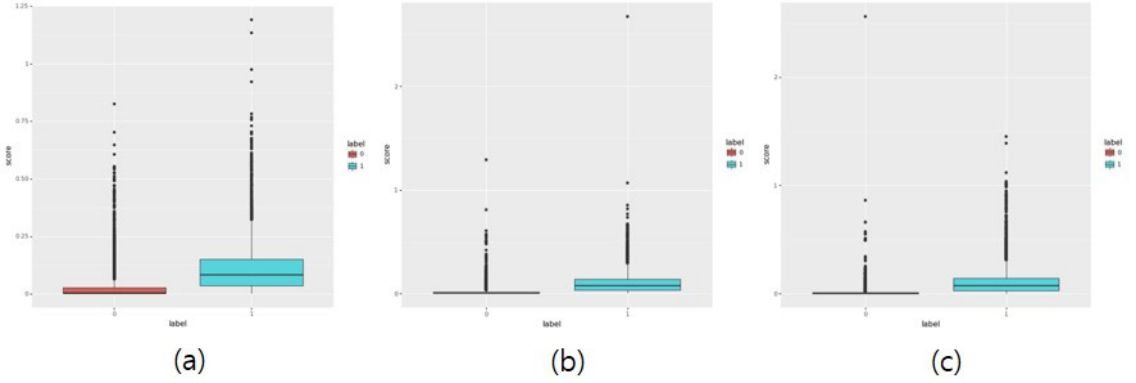


〈Figure 5〉 (a) reconstruction result of UAE model, (b) reconstruction result of CMAE model

4.2. 이상 점수 산출 결과

이상 점수 산출은 원본 데이터와 복원 데이터의 MSE를 이용하였다. 산출 결과의 타당성을 검토하기 위하여 box-plot과 t-test를 수행하였다. 아래 그림은 이상 발생 유무에 따른 점수의 차이를 box-plot으로 나타낸 것이다.

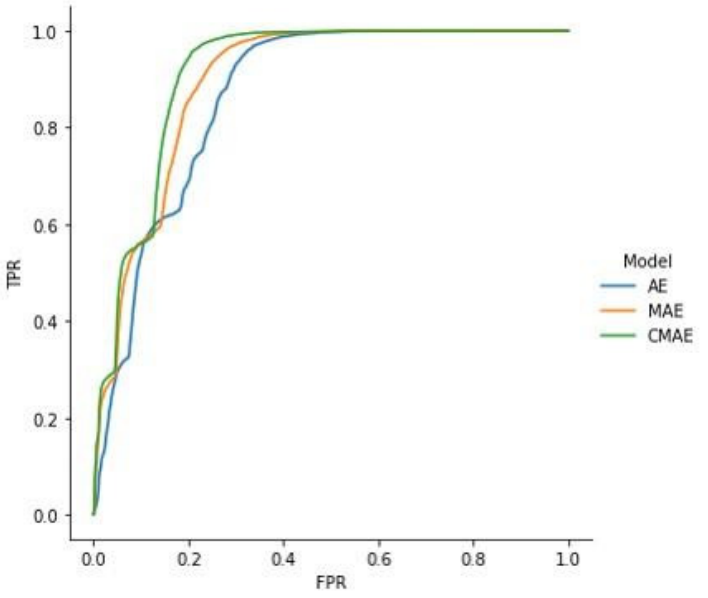
Figure 6를 확인한 결과 3개의 모델 모두 이상 발생 유무에 따른 점수 분포가 큰 차이를 보이고 있다. 세 개 모델에서 t-test를 수행한 결과 모두 p-value가 0으로 분포가 명확하게 다름을 알 수 있다. 따라서 이상 분류를 위한 점수로 활용이



〈Figure 6〉 comparison of anomaly scores between normal and abnormal, (a) UAE, (b) MAE, (c) CAME

〈Table 4〉 Results of anomaly detection

	UAE	MAE	CMAE
AUC	0.8641	0.8974	0.9145
Accuracy	0.7832	0.8491	0.8712
Precision	0.7796	0.8035	0.8104
Recall	0.8138	0.9403	0.9828
F1-score	0.7963	0.8665	0.8883



〈Figure 7〉 ROC(receiver operating characteristic) curve

가능하다고 판단된다.

4.3. 이상 탐지 성능 평가

이상탐지 성능 평가를 위하여 ROC curve를 작성하였으며, AUC, 정확도(accuracy), 정밀도(precision), 재현율(recall), F1-score를 비교하였다(Table 4). 모든 지표에서 CMAE, MAE, AE 순으로 성능이 좋게 나타났다. 특히 재현율은 CMAE의 경우 0.9828로 거의 대부분의 이상을 탐지하는 것을 확인할 수 있다. CMAE는 AE와 비교하여 1521개의 이상을 탐지 하였다. 정확도에서도 많은 향상이 있었으며, 87.12%로 나타났다. 또한, F1-score도 0.8883으로 이상탐지에 적합한 모델이라고 판단된다(Table 4).

본 연구에서 제안한 CMAE를 활용할 경우 모달(modality)과 시계열 특징이 잘 학습되는 것을 확인할 수 있다. Process 모달의 경우 변동성이

불규칙하여 3개의 모델 모두 성능이 유사함을 알 수 있다. UAE 에서 성능이 좋지 않은 CPU 모달의 경우 CMAE로 적용할 경우 0.0017에서 0.0004로 성능이 크게 향상되었다. Network 모달 또한 0.0002애서 0으로 성능이 향상되었다. 복원 성능은 이상 점수를 산출하는데 영향을 끼치며 이는 이상 분류에도 영향이 있음이 검증되었다. 추가로 ROC 곡선을 통해 성능 비교했으며, Figure 7에서 볼 수 있듯이 본 연구에서 제안한 CMAE 모델에서 우수한 결과를 나타냈음을 확인할 수 있다.

결과적으로 본 연구에서 제안한 CMAE는 로컬 특이치와 시계열성을 고려함으로써 기존 오토인코더보다 좋은 결과를 나타냄으로써 이상탐지에 있어 효과적이다는 것을 알 수 있다.

5. 결론

다차원 시계열 데이터는 다차원 데이터를 다루기 위한 특성과 시계열 데이터가 가진 특성들을 모두 고려해야하는 어려움이 있다. 다차원 데이터는 변수 간 상관성을 고려해야 한다. 확률 및 선형 기반, 거리 기반 등과 같은 기존 방법은 차원의 저주로 불리는 제약사항으로 인해 이상탐지 효과가 저하된다. 또한, 시계열 데이터의 경우 자기 상관성 분석을 위해 슬라이딩 윈도우 기법, 시계열 분해 등을 적용하여 전처리 한다. 이러한 기법들은 데이터의 차원을 증가시키는 원인이 되므로 이에 대한 보완이 필요하다.

오토인코더는 기존의 확률 및 선형 기반 모델과 군집 분석, 지도 학습 등과 비교하여 많은 장점이 있다. 확률 분포나 선형 가정을 만족하지 않는 데이터에도 적용이 가능하다. 또한 지도 학습을 위한 라벨 데이터가 없이 비지도 학습이 가능하다.

본 논문에서는 이러한 문제를 해결하고자 멀티모달을 적용하고 시계열 기반의 조건부 입력을 추가한 형태의 CMAE 모델을 제안하였다. 제안 모델은 잠재 공간을 공유하는 구조로 모달 간의 특징을 효과적으로 학습하였다. 또한 시간 정보를 조건으로 추가 입력함으로써 시계열 데이터 특성을 고려하였다. 기존 UAE와 비교하였을 때 F-1 score가 0.7963에서 0.8883으로 많은 성능 향상이 있음을 확인하였다. 정확도는 0.8641에서 0.9145로 향상되었으며, Precision이 0.7796에서 0.8104로 향상되었다. 이는 False positive가 줄었음에도 정확도가 향상되어 이상탐지 성능이 좋아졌음을 알 수 있다.

실무적인 측면에서는 모델의 성능 향상에 더하여 부수적인 장점을 갖고 있다. 시계열 분해나 슬라이딩 윈도우 같은 기법을 사용할 경우 불필요한 절차들을 관리해야 하는 단점이 있다. 또한, 차원 증가는 추론 시 연산 속도 저하를 야기할 수 있다. 추론 속도와 모델 관리 등 실무에 적용하기 용이한 특징을 갖고 있다.

추후 연구에서는 KDD Cup, UGR 16, DARPA 등의 오픈 데이터를 활용한 이상 탐지 대회 참가를 통해 모델의 범용성을 확인할 필요가 있을 것이다. 검증 시 사용한 데이터는 짧은 기간(2일)이기에 실용성을 입증하기에는 부족함 감이 있다. 따라서 실제 운영하고 있는 데이터에 적용함으로써 실질적인 유효성을 입증할 필요가 있을 것이다.

참고문헌(References)

A. Arning, R. Agrawal, and P. Raghavan. A Linear Method for Deviation Detection in Large Databases. *ACM KDD Conference*, 1996.

B. Jin, Y. Tan, A. Nettekoven, Y. Chen, U. Topcu, Y. Yue and A. Sangiovanni-Vincentelli, "An encoder-decoder based approach for anomaly detection with application in additive manufacturing", *18th IEEE International Conference On Machine Learning And Applications (ICMLA)*, 2019.

C. C. Aggarwal, Outlier analysis, 2nd, Springer, New York, 2017.

D. Bank, N. Koenigstein and R. Giryes, "Autoencoders", *arXiv eprints*, March, 2020.

D. E. Rumelhart, G. E. Hinton and R. J. Williams, "Learning Internal Representations by Error Propagation", MIT Press, 1987.

D. Pokrajac, A. Lazarevic, and L. Latecki, *Incremental Local Outlier Detection for Data Streams. CIDM Conference*, 2007.

D. Lee, "Anomaly detection in multivariate non-staionary time series for automatic DBMS diagnosis", *16th IEEE International Conference on Machine Learning and Applications (ICMLA)*, 2017.

G. E. Hinton and R. R. Salakhutdinov, "Reducing the dimensionality of data with neural networks", *Science*, vol. 313, Issue 5786(2006), 503-507.

G. E. Hinton and Simon Osindero, "A fast learning algorithm for deep belief nets", *Neural Computation*, 18(7), 2006, 1527-1554.

H. P. Kriegel, M. Schubert, and A. Zimek. “Angle-based Outlier Detection in High-Dimensional Data”, *ACM KDD Conference*, 2008.

H. Ren, B. Xu, Y. Wang, C. Yi, C. Huang, X. Kou, T. Xing, M. Yang, J. Tong and Q. Zhang, "Time-series anomaly detection service at Microsoft”, *Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*, 2019.

H. Xu, W. Chen, N. Zhao, Z. Li, J. Bu, Z. Li, Y. Liu, Y. Zhao and D. Pei, "Unsupervised anomaly detection via variational auto-encoder for seasonal KPIs in web applications", *Proceedings of the 2018 World Wide Web Conference*, 2018.

I. Ruts and P. Rousseeuw, “Computing Depth Contours of Bivariate Point Clouds”, *Computational Statistics and Data Analysis*, 23, pp. 153–168, 1996.

J. Laurikkala, M. Juholal, and E. Kentala. Informal Identification of Outliers in Med- ical Data. *Fifth International Workshop on Intelligent Data Analysis in Medicine and Pharmacology*, Journal of systems and software, vol. 63(1), 2000.

J. J. Jiang, G. Klein and R. Discenza, "Perception differences of software success: provider and user views of system metrics", *Journal of Systems and Software*, 2002.

M. Radovanovic, A. Nanopoulos, and M. Ivanovic. “On the Existence of Obstinate Results in Vector Space Models”, *ACM SIGIR Conference*, 2010.

M.-L. Shyu, S.-C. Chen, K. Sarinnapakorn, and L. Chang, “A Novel Anomaly Detection Scheme based on Principal Component Classifier”, *ICDM Conference*, 2003.

N. Abe, B. Zadrozny, J. Langford, "Outlier detection by active learning", 2006

N. Laptev, S. Amizadeh and I. Flint, "Generic and scalable framework for automated time-series anomaly detection", *Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 2015, 1939-1947.

P. Billingsley. Probability and Measure, Second Edition. Wiley, 1986.

P. Rousseeuw and A. Leroy, “Robust Regression and Outlier Detection”, Wiley, 2003.

P. Baldi, "Autoencoders, Unsupervised Learning, and Deep Architectures", 27, *JMLR*, 2012, 37-50

Pastcal Vincent, Hugo Larochelle, Isabelle Lajoie, Yoshua Bengio and Pierre-Antoine Manzagol, "Stacked denoising autoencoders: learning useful representations in a deep network with a local denoising criterion", *JMLR*, 2010.

Q. P. Nguyen, K. W. Lim, D. M. Divakaran, K. H. Low and M. C. Chan, "GEE: A gradient-based explainable variational autoencoder for network anomaly detection", *IEEE Conference on Communications and Network Security (CNS)*, 2019

R. De Maesschalck, D. Jouan-Rimbaud, D.L. Massart, "The Mahalanobis Distance", *Chemometrics and Intelligent Laboratory Systems*, 2000. 1−18

S. Roberts. Novelty “Detection using Extreme Value Statistics”, *IEEE Proceedings on Vision*, 146(3). pp. 124−129, 1999.

S. Sarawagi, R. Agrawal, and N. Megiddo. “Discovery-driven Exploration of OLAP Data Cubes”, *EDBT Conference*, 1998.

T. Baltrušaitis, C. Ahuja, and L. Morency, “Multimodal Machine Learning: A Survey and Taxonomy”, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2017

T. Johnson, I. Kwok, and R. Ng. “Fast Computation of 2-dimensional Depth Contours”, *ACM KDD Conference*, 1998.

V. Barnett and T. Lewis, “Outliers in Statistical Data”, Wiley, 1994.

V. H. Son, U. Daisuke, H. Kiyoshi, M. Kazuki, S. Pranata and S. M. Shen, "Anomaly detection with adversarial dual autoencoders", *arXiv eprint*, 2019.

Y. Bengio and Y. LeCun, "Scaling learning algorithms towards AI", MIT Press, 2007, 321-359.

Y. Pei and O. zaiane, "Synthetic data generator for clustering and outlier analysis", 2006.

Y. Su, Y. Zhao, C. Niu, R. Liu, W. Sun and D. Pei, "Robust anomaly detection for multivariate time series through stochastic recurrent neural network", *Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*, 2019, 2828 − 2837.

Y. Guo, W. Liao, Q. Wang, L. Yu, T. Ji and P. Li, “Multidimensional Time Series Anomaly Detection: A GRU-based Gaussian Mixture Variational Autoencoder Approach”, *Proceedings of the 10th Asian Conference on Machine Learning,* PMLR, 2018, 97-112.

Y. Ikeda, K. Ishibashi, Y. Nakano, K. Watanabe, and R. Kawahara, "Anomaly detection and interpretation using multimodal autoencoder and sparse optimization", *arXiv eprint*, 2018.

Abstract

A Study of Anomaly Detection for ICT Infrastructure using Conditional Multimodal Autoencoder

Byungjin Shin* · Jonghoon Lee** · Sangjin Han** · Choong-Shik Park***

Maintenance and prevention of failure through anomaly detection of ICT infrastructure is becoming important. System monitoring data is multidimensional time series data. When we deal with multidimensional time series data, we have difficulty in considering both characteristics of multidimensional data and characteristics of time series data.

When dealing with multidimensional data, correlation between variables should be considered. Existing methods such as probability and linear base, distance base, etc. are degraded due to limitations called the curse of dimensions. In addition, time series data is preprocessed by applying sliding window technique and time series decomposition for self-correlation analysis. These techniques are the cause of increasing the dimension of data, so it is necessary to supplement them.

The anomaly detection field is an old research field, and statistical methods and regression analysis were used in the early days. Currently, there are active studies to apply machine learning and artificial neural network technology to this field.

Statistically based methods are difficult to apply when data is non-homogeneous, and do not detect local outliers well. The regression analysis method compares the predictive value and the actual value after learning the regression formula based on the parametric statistics and it detects abnormality. Anomaly detection using regression analysis has the disadvantage that the performance is lowered when the model is not solid and the noise or outliers of the data are included. There is a restriction that learning data with noise or outliers should be used.

The autoencoder using artificial neural networks is learned to output as similar as possible to input data. It has many advantages compared to existing probability and linear model, cluster analysis, and map learning. It can be applied to data that does not satisfy probability distribution or linear assumption. In

* Moadata Co., Ltd.
** Moadata Co., Ltd
*** Corresponding Author: Choong Shik Park
Dept. of Smart IT, U1 University
52-70 Yeonamsan-ro, Eumbong-myen, Asan city, Chungcheongbuk-do (31415), Korea
Tel: +82-41-536-5723, Fax: +82-41-536-5729, E-mail: leciel@u1.ac.kr

addition, it is possible to learn non-mapping without label data for teaching. However, there is a limitation of local outlier identification of multidimensional data in anomaly detection, and there is a problem that the dimension of data is greatly increased due to the characteristics of time series data.

In this study, we propose a CMAE (Conditional Multimodal Autoencoder) that enhances the performance of anomaly detection by considering local outliers and time series characteristics. First, we applied Multimodal Autoencoder (MAE) to improve the limitations of local outlier identification of multidimensional data. Multimodals are commonly used to learn different types of inputs, such as voice and image. The different modal shares the bottleneck effect of Autoencoder and it learns correlation. In addition, CAE (Conditional Autoencoder) was used to learn the characteristics of time series data effectively without increasing the dimension of data. In general, conditional input mainly uses category variables, but in this study, time was used as a condition to learn periodicity.

The CMAE model proposed in this paper was verified by comparing with the Unimodal Autoencoder (UAE) and Multi-modal Autoencoder (MAE). The restoration performance of Autoencoder for 41 variables was confirmed in the proposed model and the comparison model. The restoration performance is different by variables, and the restoration is normally well operated because the loss value is small for Memory, Disk, and Network modals in all three Autoencoder models. The process modal did not show a significant difference in all three models, and the CPU modal showed excellent performance in CMAE. ROC curve was prepared for the evaluation of anomaly detection performance in the proposed model and the comparison model, and AUC, accuracy, precision, recall, and F1-score were compared. In all indicators, the performance was shown in the order of CMAE, MAE, and AE. Especially, the reproduction rate was 0.9828 for CMAE, which can be confirmed to detect almost most of the abnormalities. The accuracy of the model was also improved and 87.12%, and the F1-score was 0.8883, which is considered to be suitable for anomaly detection.

In practical aspect, the proposed model has an additional advantage in addition to performance improvement. The use of techniques such as time series decomposition and sliding windows has the disadvantage of managing unnecessary procedures; and their dimensional increase can cause a decrease in the computational speed in inference.The proposed model has characteristics that are easy to apply to practical tasks such as inference speed and model management.

Key Words : Anomaly detection, Multimodal, Artificial intelligence, Autoencoder, System monitoring

Received : May 21, 2021 Revised : June 24, 2021 Accepted : June 30, 2021
Corresponding Author : Choong Shik Park

저 자 소 개

신 병 진

서울과학기술대학교 토목공학과에서 공학학사(2015년), 공학석사(2018)를 취득하였으며, 모아데이타에서 전임연구원으로 재직 중이다. 주요 관심 분야는 기계 학습, 인공 지능, 시스템 모니터링, 이상 탐지 등이다.

이 종 훈

숭실대학교 정보통신전자공학부에서 공학학사(2005년), 공학석사(2014)를 취득하였으며, 모아데이타에서 AI 본부장으로 재직 중이다. 멀티모달, 이상탐지, 로그 이상탐지, 그리고 생존분석에서의 신경망 연구에 관심을 갖고 있다.

한 상 진

한국항공대학교 경영학과에서 경영학사(1996년)를 취득하였으며, 현재 모아데이타에서 대표이사로 재직 중이다. 주요 관심 분야는 기계 학습, 인공 지능, 시스템 모니터링, 이상 탐지 헬스케어 등 이다.

박 충 식

현재 유원대학교 스마트IT학과 교수이다. 연세대학교 대학원 전자공학과에서 인공지능 전공으로 박사학위를 취득하였다. 컴퓨터 비전, 빅데이터, 그리고 인공지능의 기호처리 기술과 신경망 기술의 융합 연구에 관심을 가지고 있다.