Anomaly Detection

이론적 설명보다
경험과 노하우 중심으로 발표 진행

PHM (Prognostics and Health Management)

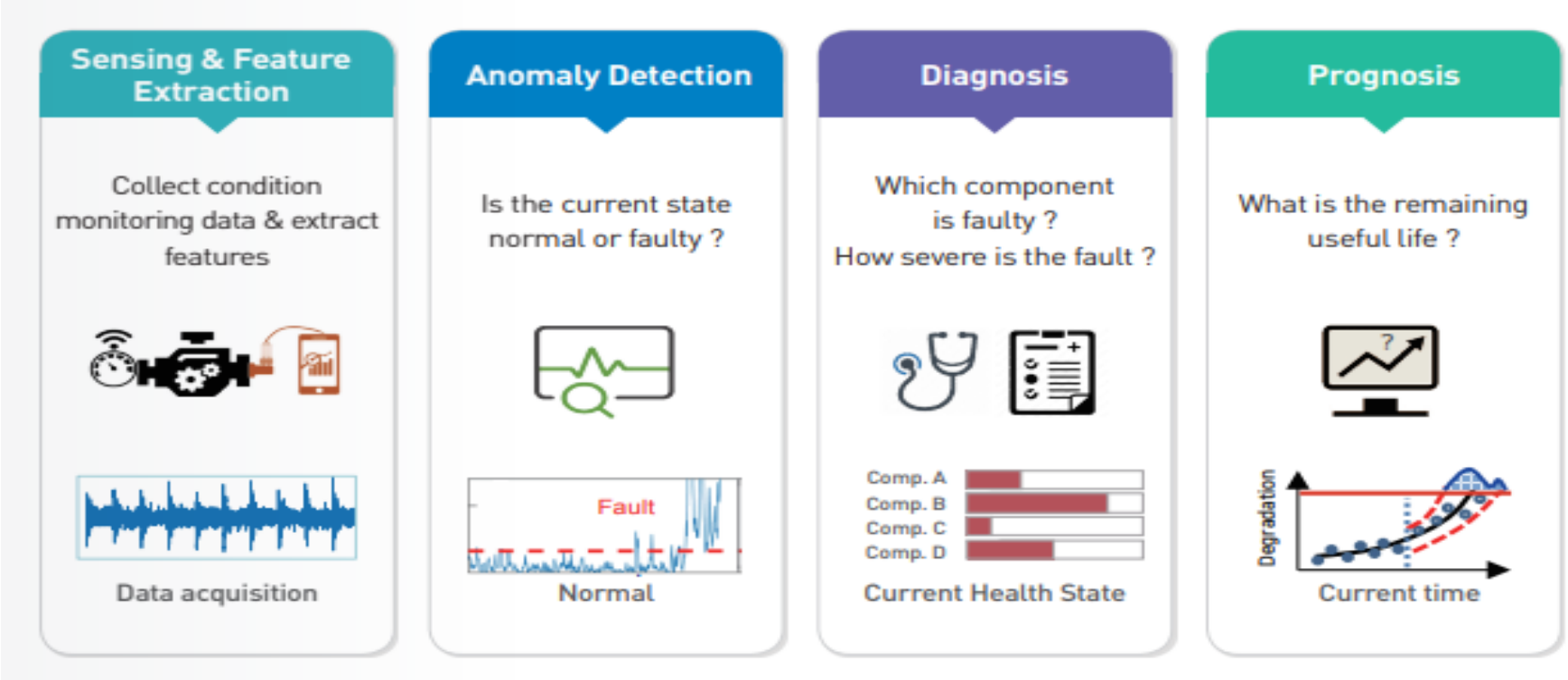
시스템의 건전성을 예측하고 관리하는 기술

계측
- 데이터 수집
- 데이터 품질 고도화

이상 탐지
- 정상 / 이상 구분

이상 분류
- 고장 부품 / 원인 확인

이상 예측
- 결함 예측 / 수명 예측



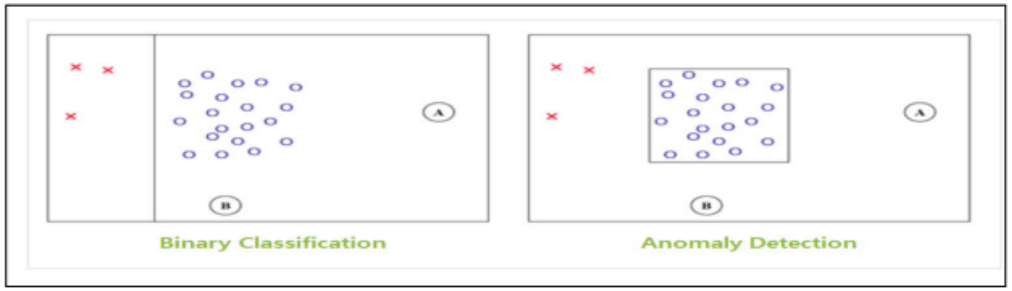
Anomaly Detection의 개념

예상하지 못한 패턴이나 정상 상태가 아닌 상태를 감지하는 기술

Hawkins(1980)의 정의:
"다른 관측치와 크게 벗어나 다른 메커니즘에 의해 생성
되었다는 의심을 불러일으키는 관측치"

anomaly, outlier, abnormal 등으로도 불리며, 주로 정상 데이터와 비교하여 비정상 데이터를 식별함

〔그림 2-1〕 Classification과 Anomaly Detection 차이



자료: 정재윤. (2017). Novelty Detection-Overvier. https://jayhey.github.io/novelty%20detection/2017/10/18/Novelty_detection_overview/〉에서 2018년 11월 인출

고장진단 기술의 발전 과정

- 1세대: 경험 기반 진단
- 2세대: 센서 및 신호 분석
- 3세대: 머신러닝 도입
- 4세대: 빅데이터 및 딥러닝 활용

Anomaly Detection의 활용

자동차 충전 중 이상 감지

고장 예측을 위한 건전성 지표 추출 연구

딥러닝 기반 FAB 공정 희소 불량 이상 감지 기술 개발

전력설비 유지보수 의사결정 최적화

회전체 기기의 상태 분류

Anomaly Detection의 주요 논문

"Deep Learning for Anomaly Detection: A Survey" (2021)
딥러닝 기반 이상 탐지 방법들을 포괄적으로 리뷰

"Anomaly Detection with Deep Perceptual Autoencoders" (2020)
오토인코더를 사용한 이상 탐지 방법을 제안하며, 비정상 샘플의 재구성 오류를 기반으로 이상치를 탐지합니다.

"Deep Anomaly Detection Using Geometric Transformations" (2018)
기하학적 변환을 활용한 딥러닝 기반 이상 탐지 방법을 소개합니다.

"Deep One-Class Classification" (2018)
One-Class 분류 문제를 딥러닝으로 해결하는 방법을 제안합니다.

"Unsupervised Anomaly Detection with Generative Adversarial Networks" (2017)
GAN을 활용한 비지도 학습 기반 이상 탐지 방법을 소개합니다.

"LSTM-based Encoder-Decoder for Multi-sensor Anomaly Detection" (2016)
LSTM을 사용한 시계열 데이터에서의 이상 탐지 방법을 제안합니다.

"Outlier Detection with Autoencoder Ensembles" (2017)
오토인코더 앙상블을 사용한 이상치 탐지 방법을 소개합니다.

"A Survey on GANs for Anomaly Detection" (2022)
GAN을 활용한 이상 탐지 방법들을 종합적으로 리뷰하고 있습니다.

Anomaly Detection의 어려움

- 데이터 불균형

  비정상 데이터가 매우 적어 모델 학습 / 검증이 어려움

  (실제 이상현상인지 vs 모델의 학습이 부족한 것인지)

- 이상의 재현성

  실제 필드에서 다양한 이상피 패턴을 어떻게 구분할 것인가?

  (ex. 서서히 고장, 순간적인 고장

- 정상/비정상 경계의 불명확성

  정상과 비정상의 구분 기준을 명확히 설정하는 것이 중요하나,

  정상과 비정상 경계선상에 있을 경우 어떻게 판단할 것인가?

- 왜 이상이 발생하였는지 원인 분석

데이터 수집

- 이상 데이터를 최대한 확보

  명확하게 Label을 붙일 수 있는 데이터 확보

- 추가가 필요한 feature가 있으면 최대한 적극적으로 확보

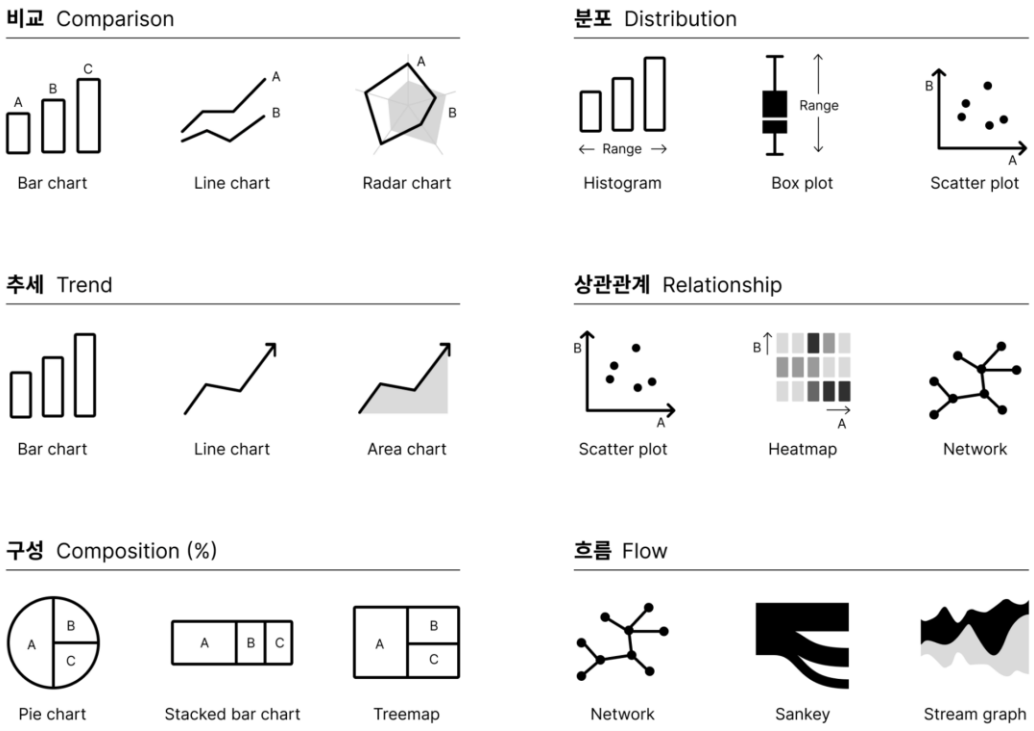
  데이터 거버넌스와의 협업 중요

- 대용량의 데이터 저장 / 관리

  SQL적인 측면에서 관리 필요성 느낌

데이터 분석

- 기초 통계량: 평균, 분산, 최대값, 최소값 등
- 시각화: 히스토그램, 박스 플롯, 산점도 등을 사용하여 데이터 분포와 관계 탐색
- 상관 관계 분석: 변수들 간의 상관 관계 분석
- 군집 분석 : 비슷한 특성을 가진 데이터를 그룹으로 분류하는 비지도 학습 기법

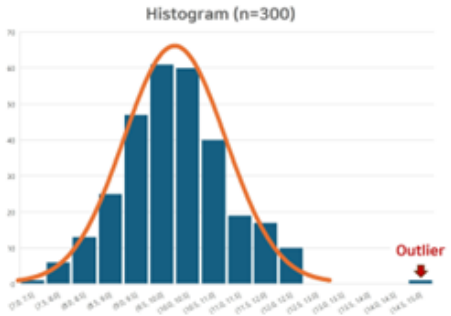


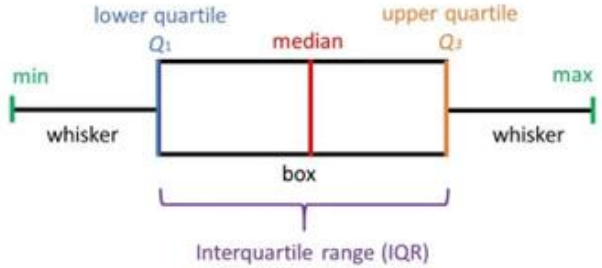
데이터셋 구축

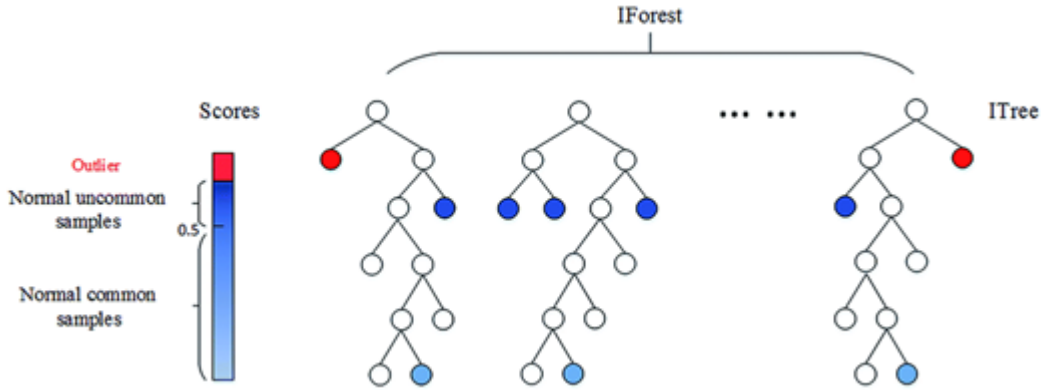
- **데이터 클리닝**
  - 결측치 처리: 누락된 값을 예측하거나 대체값으로 채움
  - 이상치 제거: 다른 값들과 크게 차이나는 값을 제거하거나 대체

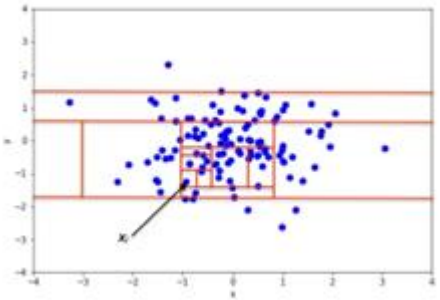
분포 활용(히스토그램, IQR)를 활용하되, 경험상 결국 도메인 지식으로 결정하게 되었음

feature가 많은 경우, 결정트리도 활용 가능함





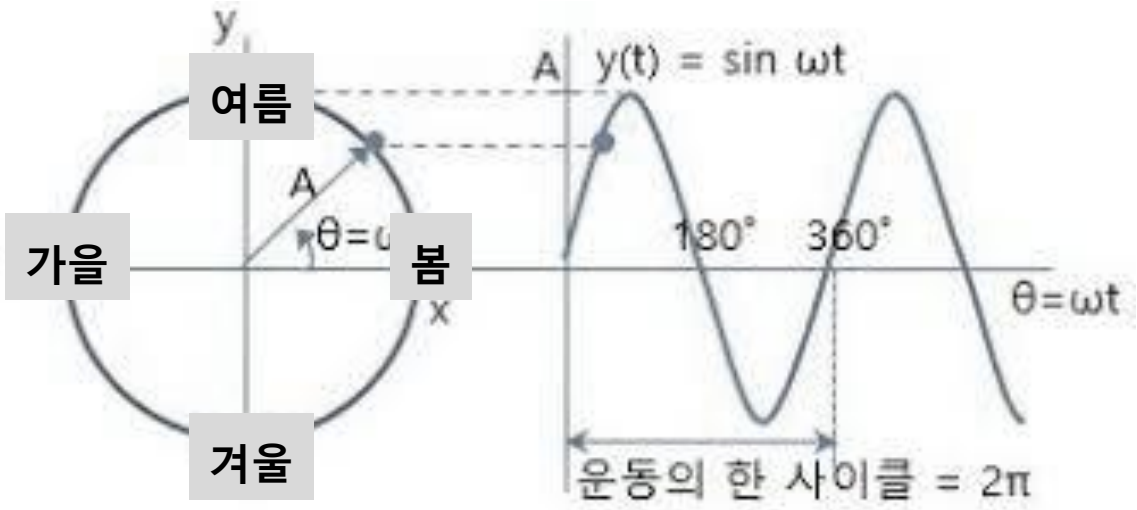




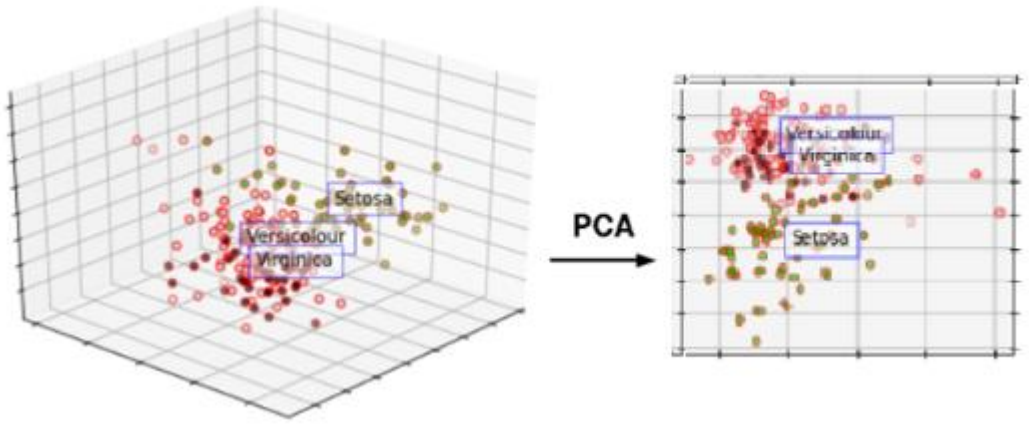
데이터셋 구축

- **feature 엔지니어링**
  - 현업에서는 도메인 지식이 제일 중요했음 (데이터적으로만 feature를 선정하기 무서워서...)
  - 확보한 feature를 변형하는 것도 도움이 되었음
    : 물리적, 계절성, 연관성, 노이즈 제거 등의 목적으로 변형하여서 feature를 새로 생성하여 사용함

계절성 정보 feature 생성



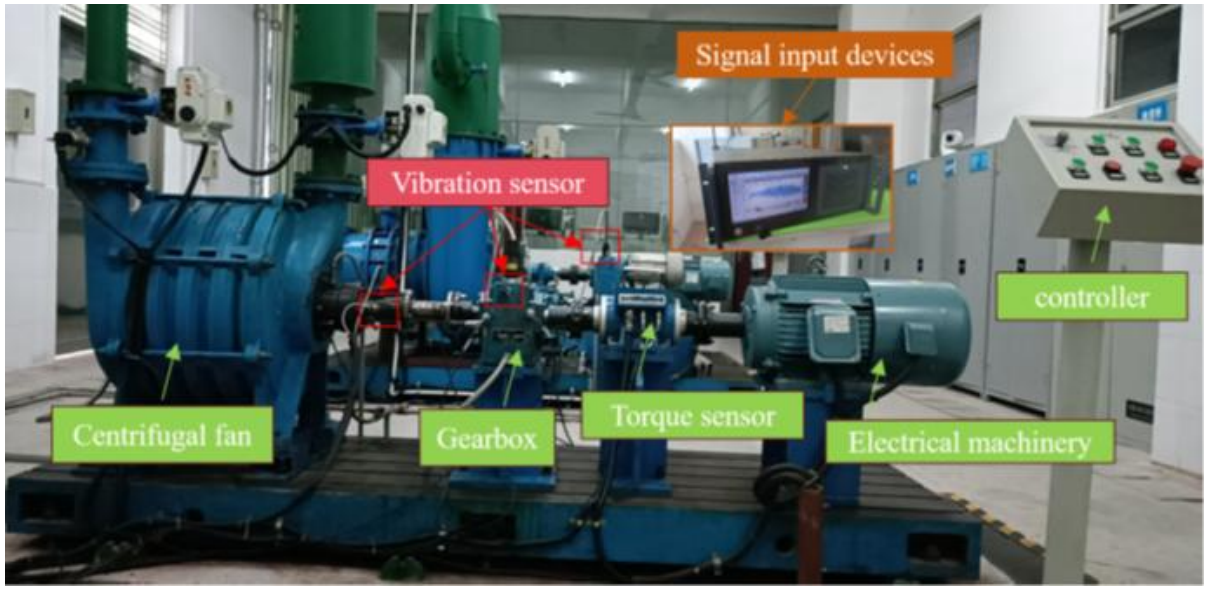
PCA 차원축소 (feature 5개 → 1개)

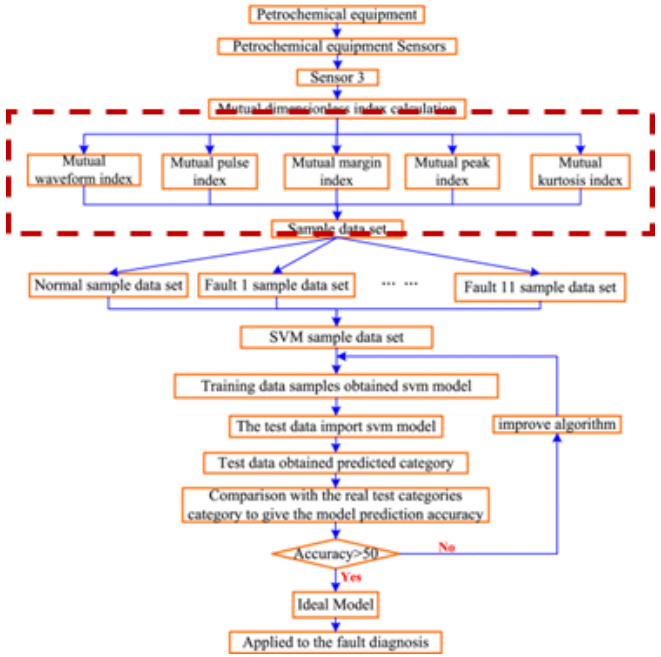


데이터셋 구축

- **특성 엔지니어링**
  - 현업에서는 도메인 지식이 제일 중요했음 (데이터적으로만 feature를 선정하기 무서워서...)
  - 확보한 featur를 변형하는 것도 도움이 되었음
    : 물리적, 계절성, 연관성, 노이즈 제거 등의 목적으로 변형하여서 feature를 새로 생성하여 사용함

각 데이터 세트에 대해 차원 없는 지수 5개를 얻은 다음 데이터 세트에 대한 지원 벡터 머신(SVM) 모델 투영을 사용하여 고장 유형을 판단



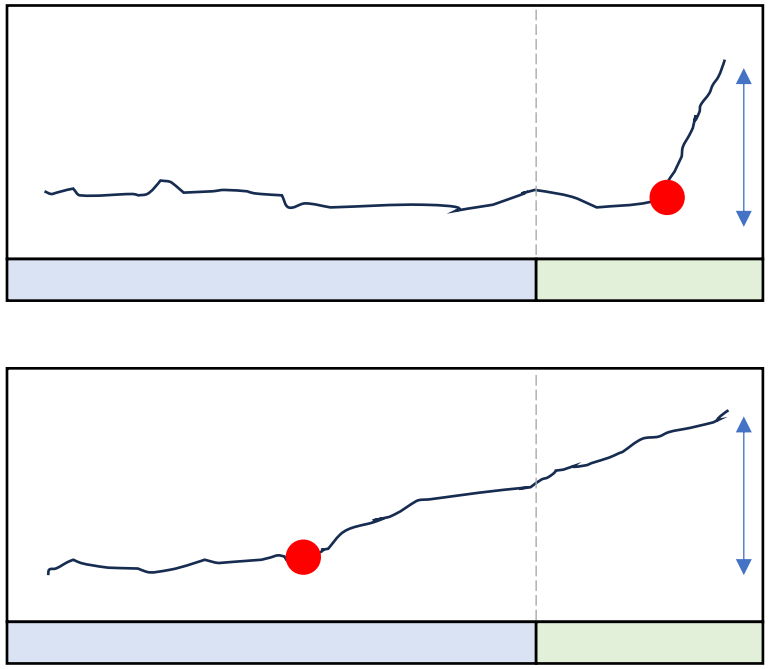


데이터셋 구축

- **데이터 분할**
  - 학습 데이터와 테스트 데이터로 분리

데이터 분할 기본

Anomaly detection 관점



학습 구간 선정을 위한 별도의 모델

랜덤 포레스트나 분류모델 등을 활용하여 값이 이상적으로 상승하는 구간을 찾음

그 구간을 기점으로 training/testing 구간을 나눌 수 있음

데이터셋 구축

- **데이터 정규화**
  - 데이터의 값 범위를 조정하여 모델 학습에 적합한 형태로 변환
- **데이터 증강**
  - 현장에서 데이터 불균형인 사례가 여럿있을 수 있음
  - 일부 영역에 데이터가 몰려있을 수도 있음, 그럼에도 불구하고 데이터 생성은 적용하지 않았음
    : 생성된 데이터에 대한 신뢰도를 검증할 수가 없었음

현장에서 데이터 불균형은 흔히 있을 수 있음

생성된 데이터 검증

- 통계적적으로 분포 확인, 차원 축소 검증
- RF 등으로 Classifier-based Turing Test
- Autoencoder를 활용한 feature space 비교

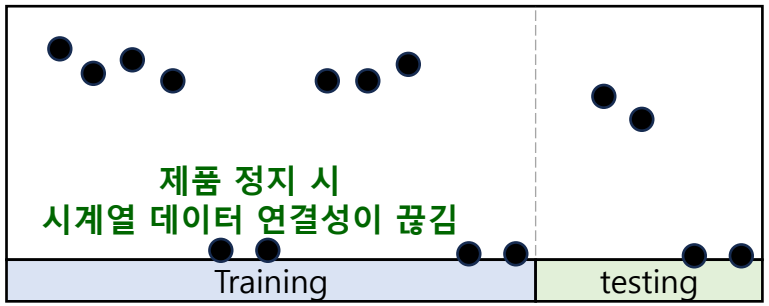
But 비교할만한 raw data가 없다!!!

데이터셋 구축

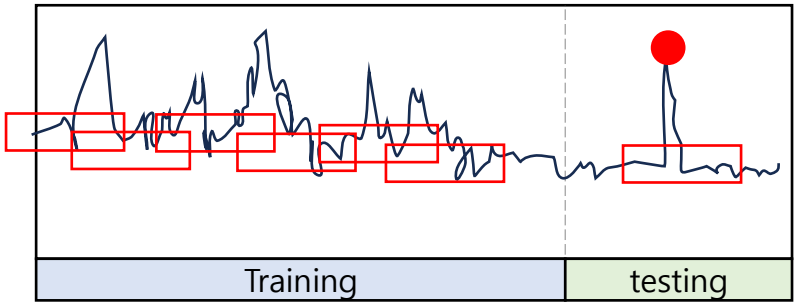
- **시계열 데이터 처리**
  - 시계열인 데이터지만, 시계열이 아닌 일반 수치형 데이터라고 생각함
  - 학습데이터의 변동성이 커서 윈도우 처리법을 시도하였으나, 진단 시 이상데이터의 정보가 축소되어서 적용안함

수집된 센서 데이터 (시계열)

	A	B	C
1:00	1	2	2
2:00	3	5	5
3:00	0	0	0
4:00	0	0	0
5:00	4	4	3
6:00	2	2	1

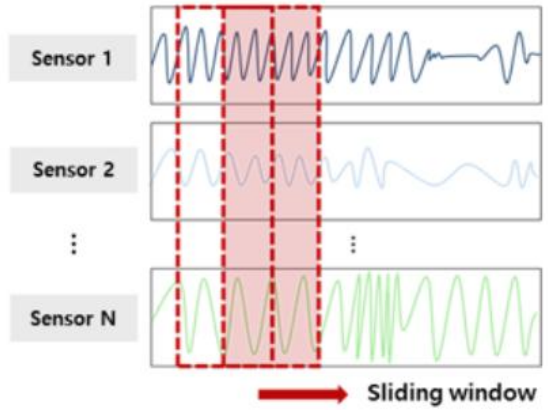


윈도우 처리법



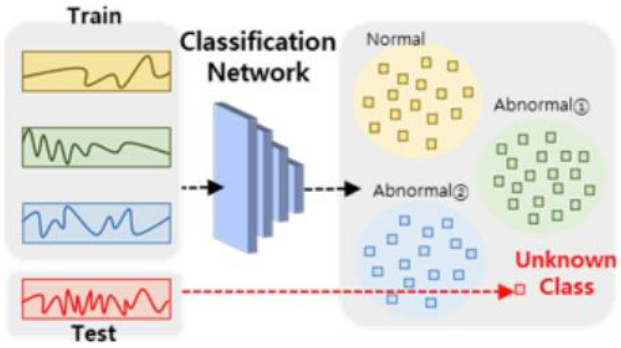
데이터셋 구축

1. 전처리 및 사전분석



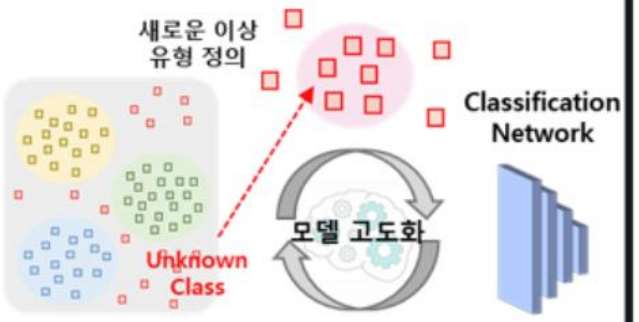
- 데이터 확보
- 데이터 특성 파악
- 데이터 전처리 수행
- 기본 이상 탐지 모델 구축

2. 오픈셋 모델 구축



- 오픈셋 이상 패턴 정의
- 오픈셋 실험 상황 가정
- 오픈셋 모델 구축
- 분류 성능 확인

3. 모델 고도화 및 결과 해석



- 하이퍼파라미터 탐색
- 오픈셋 이상 탐지 결과 해석
- 오픈셋 이상 진단 원인 파악
- 적응형모델 제안

- Feature가 아주 많지 않고, 비선형 구간도 다수 존재하여 딥러닝보다 머신러닝 계열에서 알고리즘을 선택함
- 데이터와 목적에 따라서 알고리즘 선정 (개인적으로는 많은 알고리즘을 검토하는 것을 추천)

이상탐지 (Anomaly Detection)

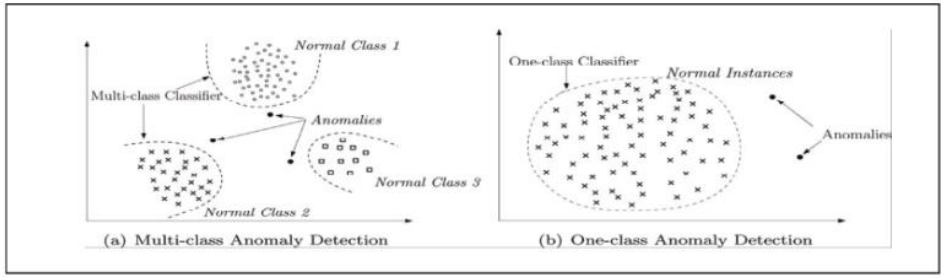
지도 학습 (Supervised Learning)

- XGBoost
- RandomForest
- SVM(Support Vector Machine)
- KNN(K-Nearest Neighbors)

준지도 학습 (Semi - Supervised Learning)

- One Class SVM

〔그림 3-1〕 분류 기반 이상 탐지



자료: Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM computing surveys (CSUR), 41(3), 15. 21page

비지도 학습 (Unsupervised Learning)

- Isolation Forest
- Deep Autoencoder
- K-means
- DBSCAN
- GMM (Gaussian Mixture Model)

알고리즘

비교 항목	회귀 방식	군집 방식
기본 원리	정상 패턴을 학습 예측값과 실제값의 차이가 크면 이상으로 판단	데이터 군집화를 통해 정상 그룹과 이상 그룹을 구분
필요한 데이터 유형	연속적 데이터에 적합	정형 및 비정형 데이터 모두 가능
지도학습 여부	주로 지도학습	비지도학습
실시간 적용 가능성	실시간 이상 탐지 가능	실시간 적용이 어려울 수 있음
이상 탐지 기준	예측값과 실제값 차이(잔차) **(장점) 잔차의 트렌드로 이상탐지 결과를 해석할 수 있음** **(장점) 결과의 가시화가 용이함**	군집 내 거리, 밀도 기반 이상값 탐지
고차원 / 대용량 데이터 적용	가능 (딥러닝 활용) **(장점) 일반적으로 회귀방식이 더 빠름**	차원 축소 필요할 수도 있음
설정 난이도	**(단점) 임계값(threshold)을 직접 설정**	K 값 설정(K-Means) 또는 밀도 기준 설정(DBSCAN) 필요
활용	센서 데이터 이상 탐지 (온도, 압력, 전류 등) 주가 예측을 통한 이상 탐지	사용자 행동 분석(로그 데이터 기반) 제조 공정에서 이상 제품 탐지

방법론	예제 알고리즘	특징
통계적 방법	Z-score, IQR, Grubbs' Test	계산이 빠르지만 데이터 분포에 민감
비지도 학습	Isolation Forest, One-Class SVM, DBSCAN	데이터 패턴을 학습하여 이상 탐지
지도 학습	XGBoost, CNN, LSTM	라벨이 있을 때 강력한 성능
준지도 학습	Autoencoder, GAN	정상 데이터만 학습 가능
딥러닝	Transformer, LSTM, CNN	고차원 데이터에서 높은 성능

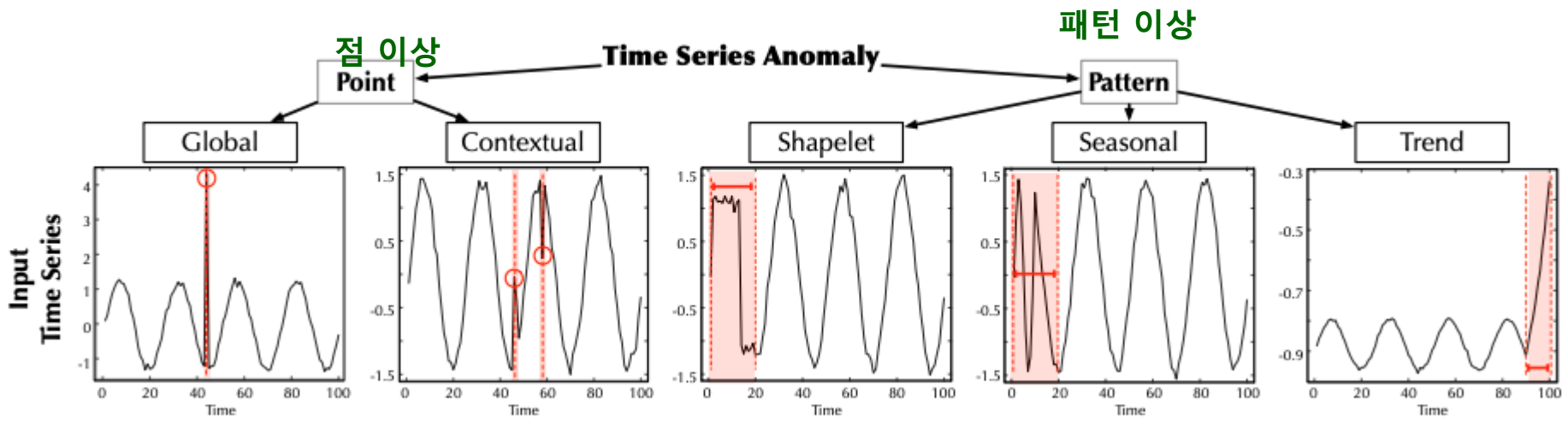
Anomaly 판단

- 룰 기반 : IQR 방법, 표준편차 기반 방법(Z-score, Sigma Rule), Percentile 기반

- 통계적 : Shapiro-Wilk Test, Mahalanobis Distance 활용
  잔차가 정규분포를 따르는지 검정 다변량 데이터에서 거리기반으로 이상 탐지

- Machine Learning 활용 : K-Means Clustering, Isolation Forest, Autoencoder 등
  정상 데이터 중심과 거리를 계산 데이터가 격리되는 정도

- 다양한 방법을 Ensemble하여 정밀도를 높일 수도 있음
  필요 시 고장여부를 판단하는 임계선이 상황별로 여러 개 있을 수 있음



Anomaly Detection 검증

- 개발된 모델로 최대한 다양한 실제 제품의 데이터를 이상감지한다.
- 실제 필드에는 정상이 대부분이다. 정상을 정상으로 잘 판단해야 한다.

  이상 탐지 모델은 정상 데이터가 압도적으로 많기 때문에 정확도 대신

  Precision, Recall, F1-score, AUC-ROC, AUC-PR 등의 지표를 권장함