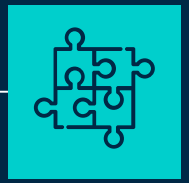
Anomaly Detection Literature Notes

Yunus Emre Işıkdemir

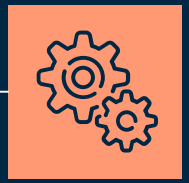
CONTENTS



01

Notion of Anomaly

The theory behind the anomaly detection



02

Survey Papers

Comparative analysis of existing methodologies.

03

Novel Approaches

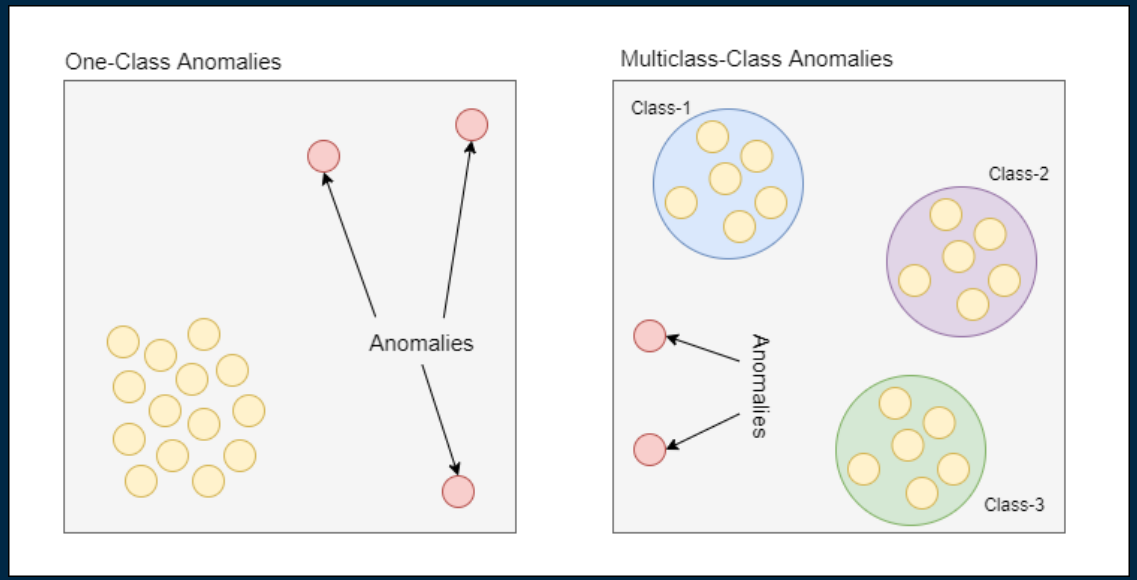
Novel approach papers

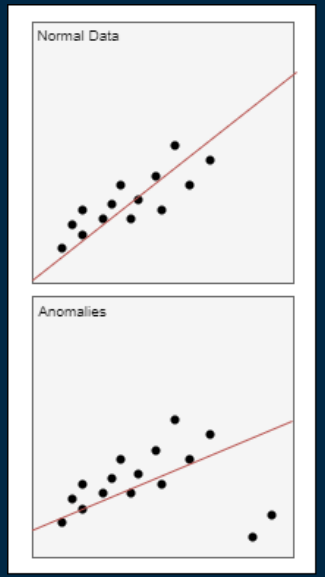
Notion of Anomaly Detection

01

What is Anomalies?

- Anomalies are rare events that do not fit into entire observations.
- Anomalies may lead to misinterpretation and wrong statistical inferences about the data.
- Anomalies highly affect the linear models for both regression and classification tasks.





Survey Papers

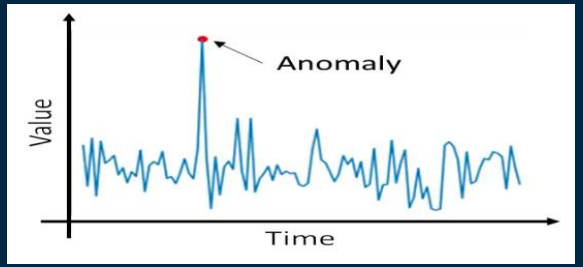
02

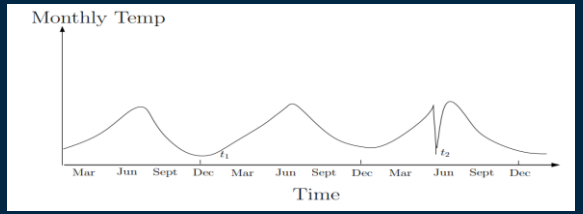
Anomaly Types

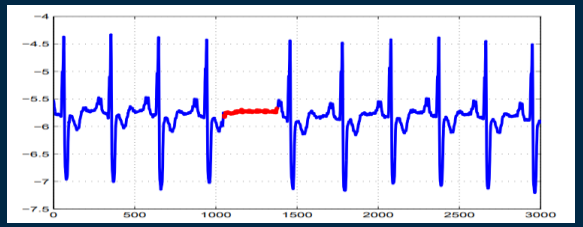
- **Point Anomalies:** Simplest form the anomalies. An observation that not fits the entire dataset is treated as anomalies. As an example, Fraud detection only considering the exreme expenditure relative the rest of the payment.

- **Contextual Anomalies:** Also known as conditional anomalies. Context anomalies are data points that are considered abnormal when viewed against meta-information associated with the data points. As an example, average expenditure of a person is 100$. However, in christmas, the payment may be 1000$ every year for this specific condition.

- **Collective Anomalies:** A sample may not be anomaly, but a sequence of observations may be anomalos event together.





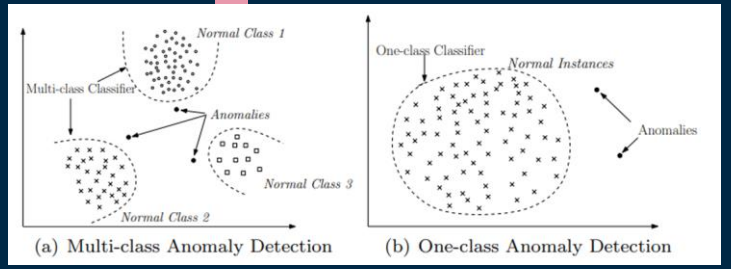


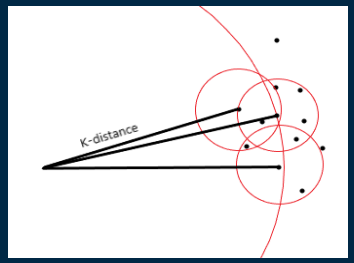
Anomaly Detection Techniques

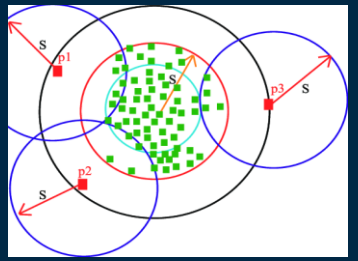
- **Supervised Anomaly Detection:** At the beggining of the problem, labels should be marked as anomalous or normal for each observation. In this way, machine learning models can map the features to target variable to learn identify anomalies. The limitation is that labeling process may be bothering and time consuming.

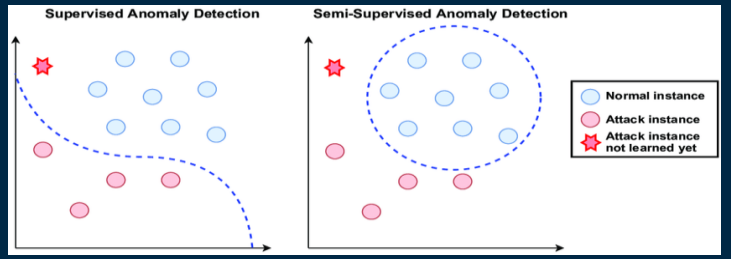
- **Unsupervised Anomaly Detection:** The technique do not requires the labels. Euclidean distance can be calculated for the observations. Instances that higher neighborhood distances can be marked as abnormal observation. Local outlier factor is widely used algorithm for this process.

- **Semi-supervised Anomaly Detection :** Train dataset only includes normal labels. Model learns the single class pattern, and the observations assigned as anomalies which has non-similar patterns that is learnt by model.



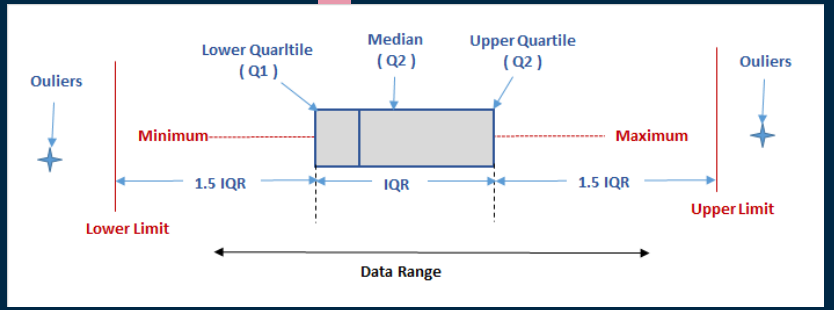




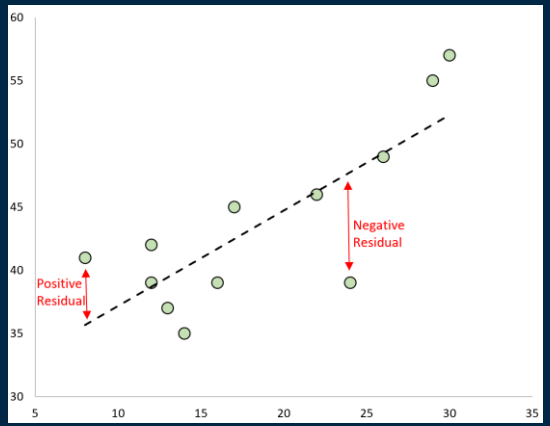


Anomaly Detection Techniques

- **Statistical Anomaly Detection**: Normal observations located on the high probability region. In contrary, abnormal observations inside the low probability region. Deviation from the mean and median can be used to detect anomalies.

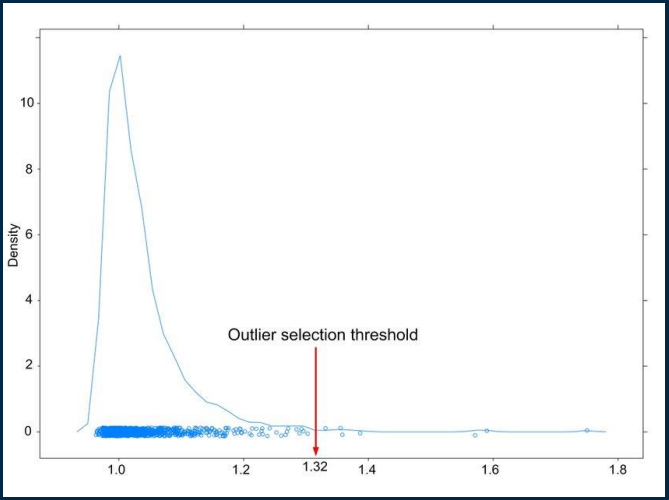


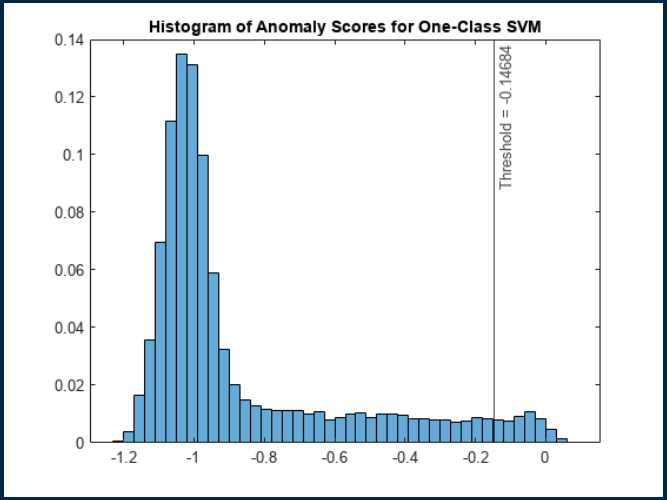
- **Regression-based Anomaly Detection**: Robust regression techniques can be used to fit the data. Once the model is fit, absolute residuals can be used as anomaly scores. Top-k highest residuals (or thresholds) can be used to detect anomalies.



Output of the Anomaly Detection

- **Labels:** Lables of the each observation either be normal or abnormal.
- **Scores:** Instead of crisp labels, degree of anomaliness can be used to identify anomalies. The scores can be calculated in many ways. Deviation from the average value can be used as a score for each observation. In addition, in supervised anomaly detection, the probability of belonging the normal class can also be a anomaly score.





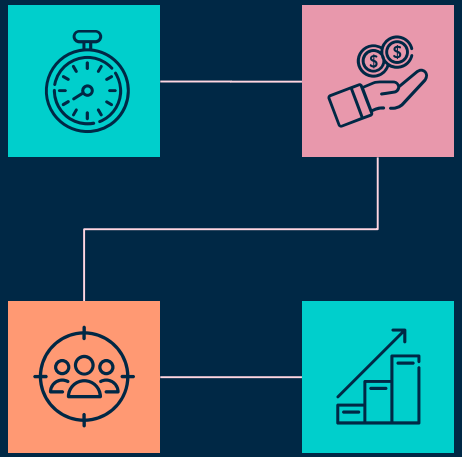
Application Areas

Fraud Detection

Based on transactions, payment peaks

Brain Tumor Segmentation

Detection of abnormal tissues on image data



Fault Detection

Bearing fault detection depending on vibration signal analysis

Network Intrusion Detection

Detection of the cyber attacks with analysing requests and logs.

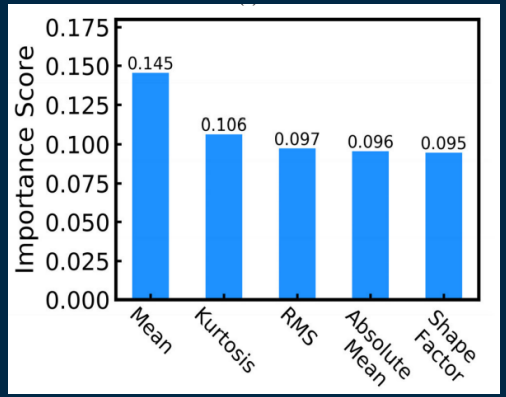
Novel Approaches

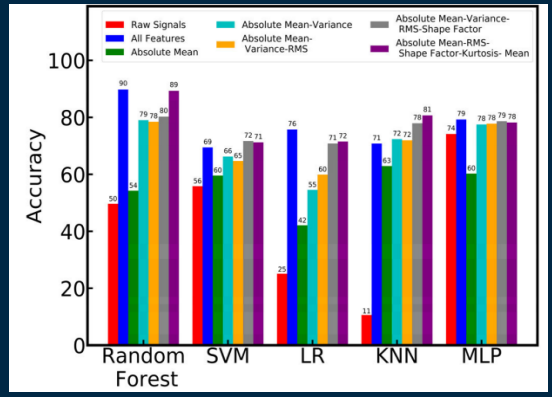
03

FaultNet: A Deep Convolutional Neural Network for Bearing Fault Classification

- MAGAR et. al., in their study, used vibration signals of the mechanical systems with bearings.
- They used descriptive statistics and signal processing techniques to extract features from the raw signal.
- The data set used in this study is sampled with 12kHz sampling frequency. The motor speed was approximately 1720 rpm during the data gathering.

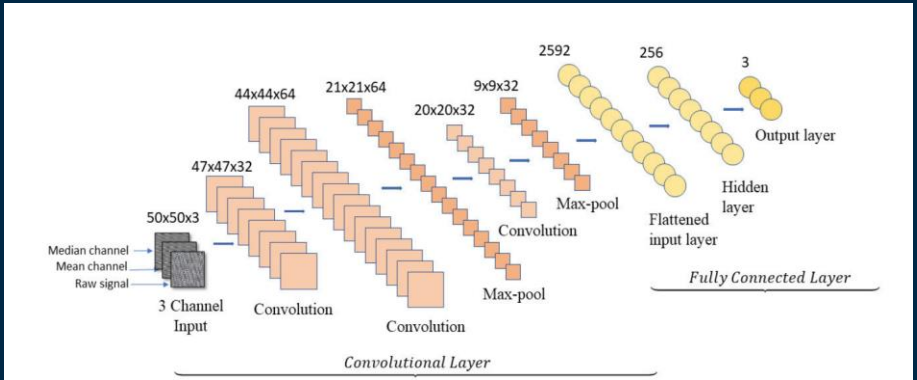
Health Condition	Fault size (mm)	Total dataset	class labels
Normal	-	280	0
ball fault	0.18	280	1
ball fault	0.36	280	2
ball fault	0.53	280	3
inner race fault	0.18	280	4
inner race fault	0.36	280	5
inner race fault	0.53	280	6
outer race fault	0.18	280	7
outer race fault	0.36	280	8
outer race fault	0.53	280	9

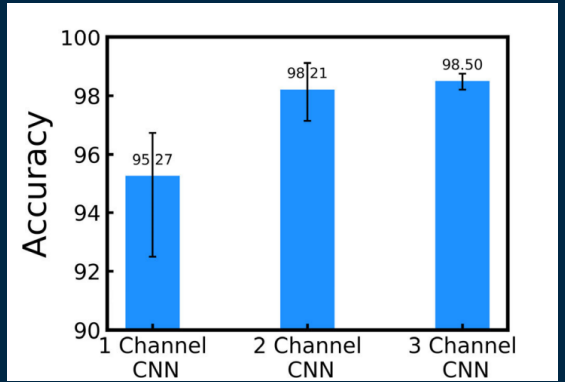




FaultNet: A Deep Convolutional Neural Network for Bearing Fault Classification

- They proposed an CNN architecture called faultnet that uses rgb channels as raw signal channel, median channel and mean channel.
- Raw singal channel: Raw signal is parsed into subsignals and reshaped to satisfy the 50x50 size condition
- Mean channel: Is used for the augment raw signal. Mean filter is used to signal to derive mean channel with including 10 observation at a timestep.
- Median channel: Is used for the augment raw signal. Median filter is used to signal to derive median channel with including 10 observation at a timestep.





Anomaly Detection Novel Techniques

- Deep learning approaches are such a way to detect abnormal observations for the dataset which has complex patterns. Convolutional Neural Networks (**CNN**) are deep-learning-based networks that are widely used in the computer vision domain using the convolution layer to extract features from complex patterns. Moreover, it can be used for anomaly detection with proper configuration. Wen et. al. in **their study converted signals into 2D images and fed the LeNet-5 architecture** to extract features through the convolution layer. They can achieve 99.79% accuracy in classifying faulty signals in the motor bearing dataset.

- Shao et. al. in their study used deep **autoencoder** to learn features for fault diagnosis on machinery. They used maximum cross-entropy to improve the feature learning process. They also adapt autoencoders to signal features using a fish swarm algorithm.

- Fernández et. al., train a **one-class SVM with only the normal condition label** to identify whether the signal belongs to normal or abnormal events. Once the class is identified, Hilbert transform and bandpass filters are used to locate defection.

Anomaly Detection Novel Techniques

- Konar et. al. used support vector machines with the **continuous wavelet transform** to bear the fault diagnosis problem. They achieved promising results and show the continuous wavelet transform can be better than the discrete wavelet transform for this domain .

- Shao et. al. in their study used deep autoencoder to learn features for fault diagnosis on machinery. They used maximum cross-entropy to improve the feature learning process. They also adapt autoencoders to signal features using a fish swarm algorithm.

- There are also various anomaly detection techniques in literature such as isolation forest, feature extraction for supervised anomaly detection.

References

- Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM computing surveys (CSUR), 41(3), 1-58.
- Blázquez-García, Ane, et al. "A review on outlier/anomaly detection in time series data." ACM Computing Surveys (CSUR) 54.3 (2021): 1-33.
- Cook, A. A., Mısırlı, G., & Fan, Z. (2019). Anomaly detection for IoT time-series data: A survey. IEEE Internet of Things Journal, 7(7), 6481-6494.
- Ahmed, M., Mahmood, A. N., & Islam, M. R. (2016). A survey of anomaly detection techniques in financial domain. Future Generation *Computer Systems*, *55*, 278-288.
- Zhang, S., Zhang, S., Wang, B., & Habetler, T. G. (2020). Deep learning algorithms for bearing fault diagnostics—A comprehensive review. *IEEE Access*, *8*, 29857-29881.
- Wen, L., Li, X., Gao, L., & Zhang, Y. (2017). A new convolutional neural network-based data-driven fault diagnosis method. *IEEE Transactions on Industrial Electronics*, *65*(7), 5990-5998.
- Shao, H., Jiang, H., Zhao, H., & Wang, F. (2017). A novel deep autoencoder feature learning method for rotating machinery fault diagnosis. *Mechanical Systems and Signal Processing*, *95*, 187-204.
- Chen, Z., & Li, W. (2017). Multisensor feature fusion for bearing fault diagnosis using sparse autoencoder and deep belief network. *IEEE Transactions on Instrumentation and Measurement*, *66*(7), 1693-1702.
- Konar, P., & Chattopadhyay, P. (2011). Bearing fault detection of induction motor using wavelet and Support Vector Machines (SVMs). *Applied Soft Computing*, *11*(6), 4203-4211.
- Fernández-Francos, D., Martínez-Rego, D., Fontenla-Romero, O., & Alonso-Betanzos, A. (2013). Automatic bearing fault diagnosis based on one-class ν-SVM. *Computers & Industrial Engineering*, *64*(1), 357-365.