ZABBIX SUMMIT 2024

Anomaly Detection in Zabbix: Present and Future

Aleksandrs Kalimulins

Product Team

Introduction

ZABBIX SUMMIT 2024

What is AI used for in IT infrastructure monitoring?

AI has become a crucial tool in IT infrastructure monitoring, providing a more proactive and efficient way to manage and optimize systems. Here are some key uses of AI in this area:

1. **Anomaly Detection**: AI algorithms can quickly identify deviations from normal behavior in IT systems. These anomalies might indicate potential issues like hardware failures, cyberattacks, or configuration errors. By detecting anomalies early, AI helps prevent these issues from escalating into serious problems.

What is an anomaly?

Image credit: Herluf Bidstrup

What is an anomaly?

anomaly noun

anom·a·ly ə-ˈnä-mə-lē

plural anomalies

Synonyms of *anomaly* >

1 : something different, abnormal, peculiar, or not easily classified : something anomalous

They regarded the test results as an *anomaly*.

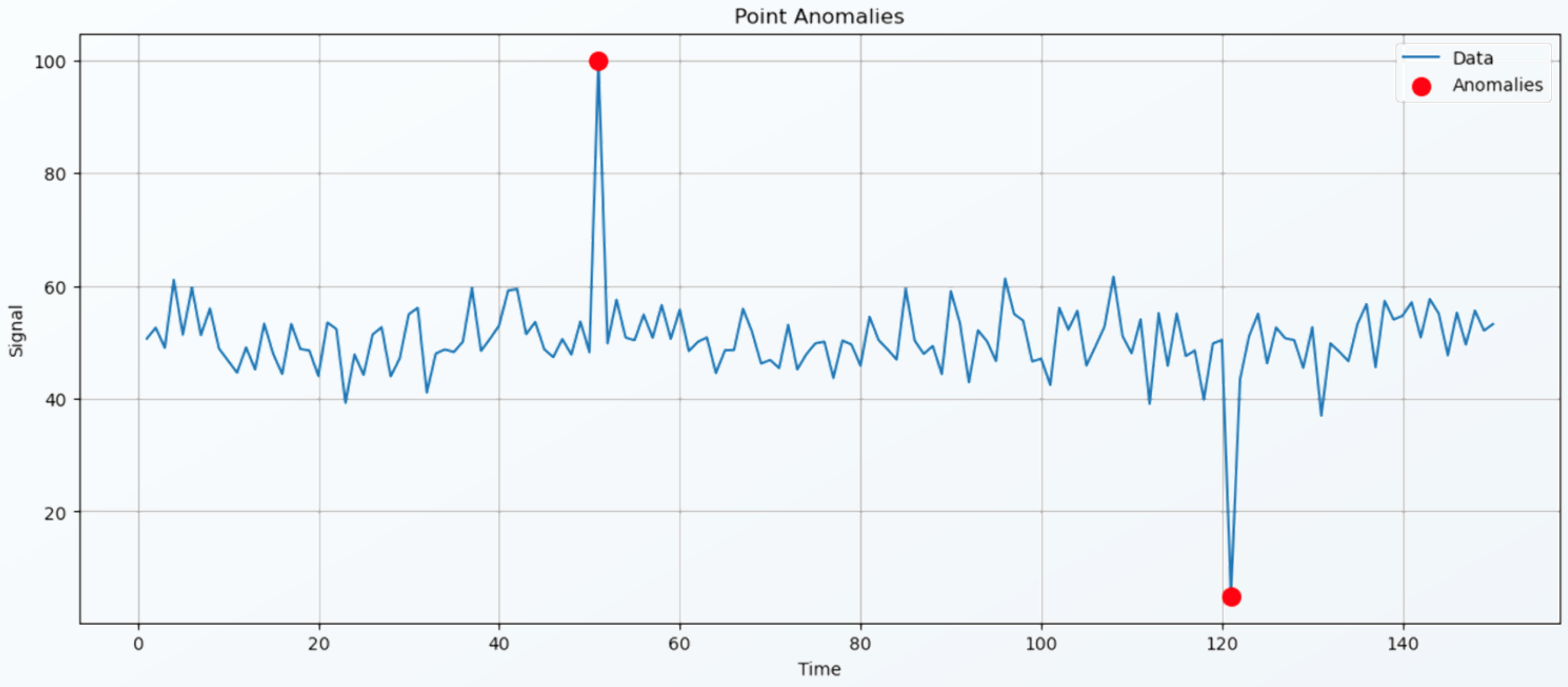
2 : deviation from the common rule : **IRREGULARITY**

What is an anomaly in time series?

*An anomaly in a time series is a **rare** or **unexpected** point or sequence occurring over a specified time interval, often considered unusual or undesirable.*

Anomaly types

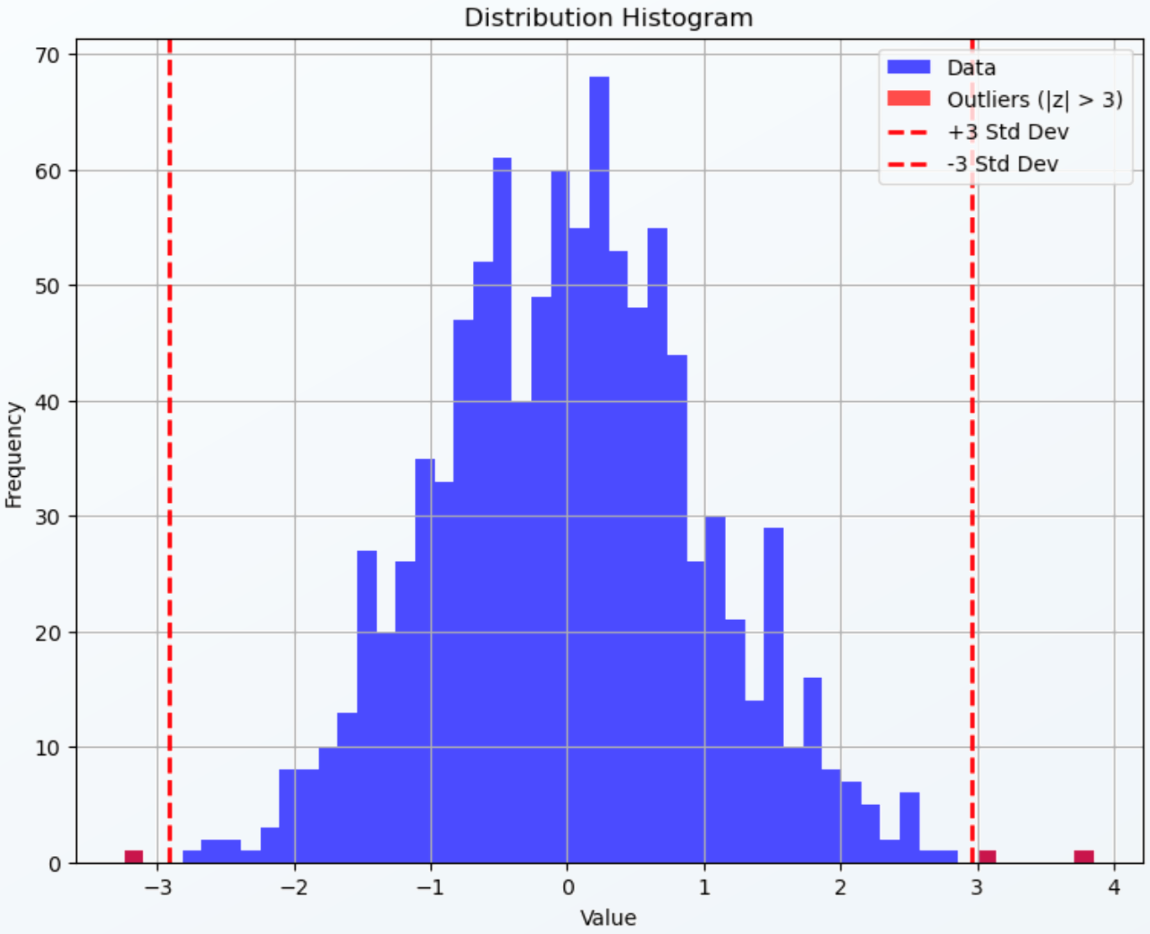
Point-based



Anomaly types

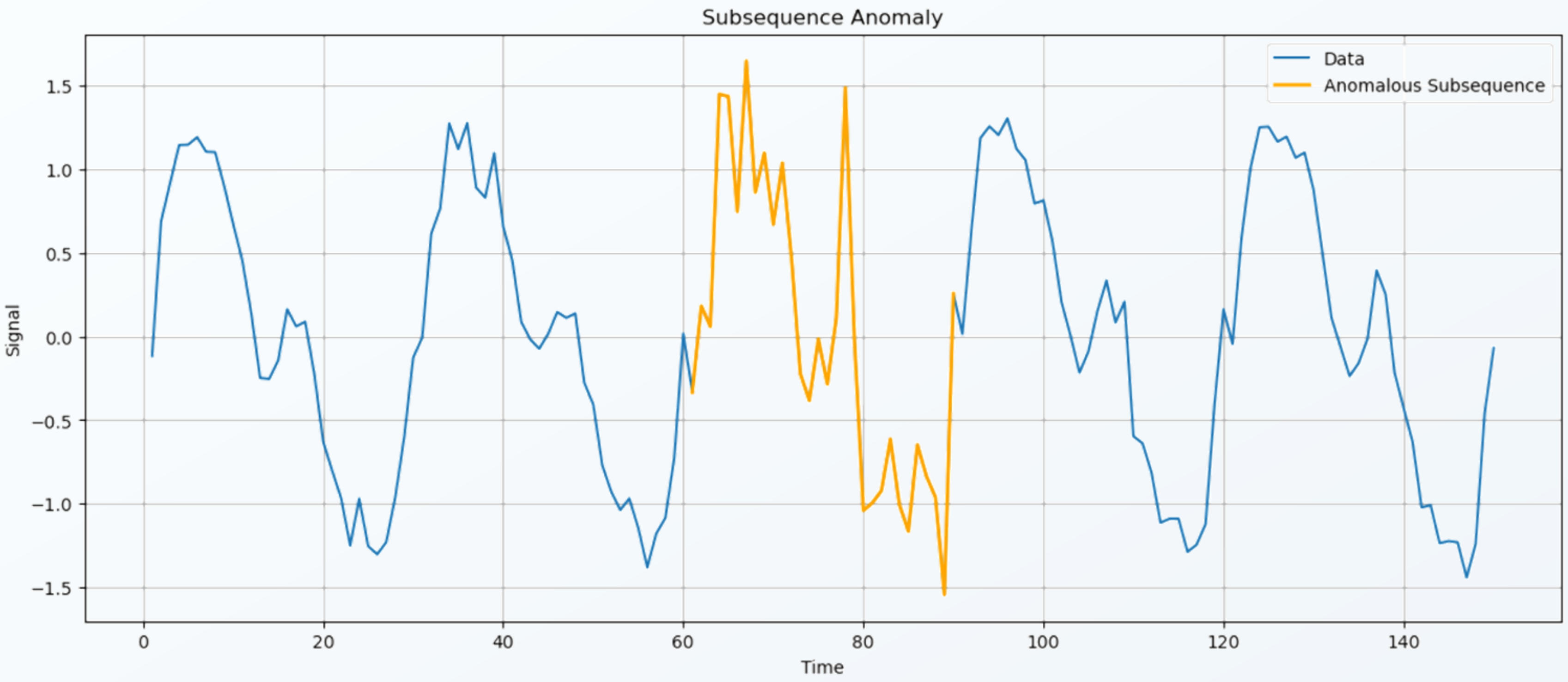
Point-based

- Short duration
- Easy to spot
- Easy to detect
  - sometimes even with `stddevsamp()`



Anomaly types

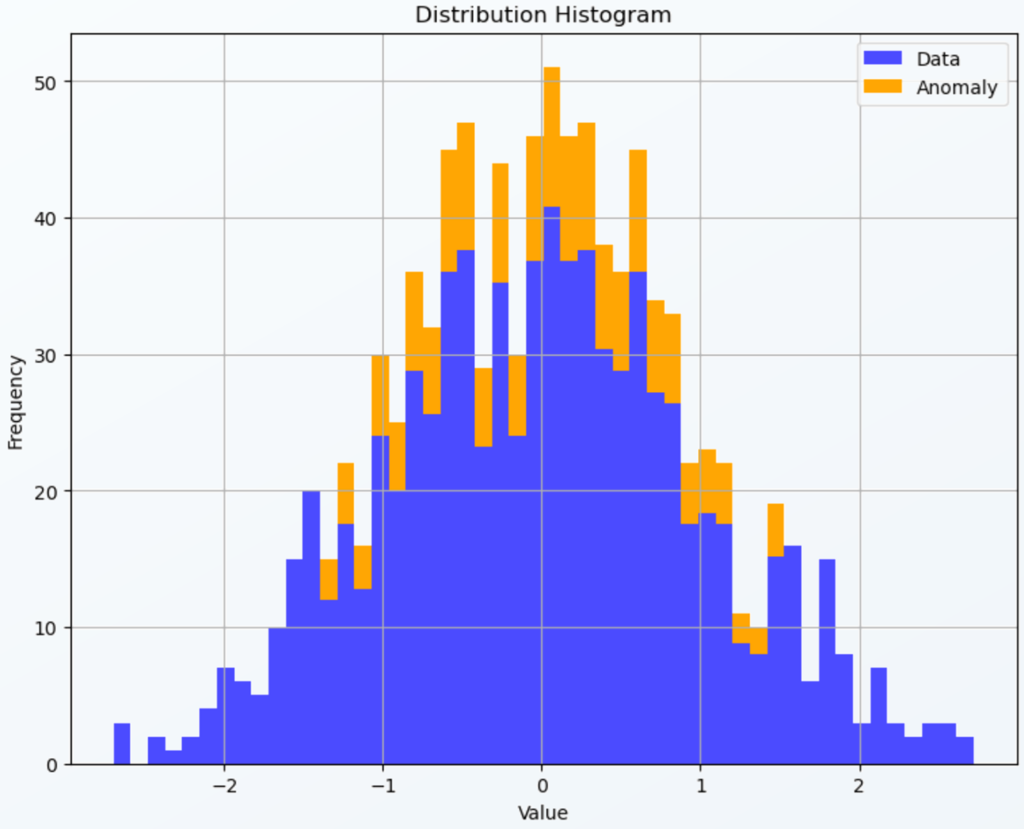
Subsequence-based



Anomaly types

Subsequence-based

- Longer duration
- Harder to spot
- Difficult to detect



How does Zabbix do it?

Trigger functions

- `stddevpop(), stddevsamp(), mad()`
- `varpop(), varsamp()`
- `baselinedev()`
- `trendstl()`

How does Zabbix do it?

`trendstl()`- features

- implements STL anomaly detection algorithm
- decomposes data into trend, seasons, residual
- data must have pronounced seasonal pattern

How does Zabbix do it?

`trendstl()`- shortcomings

- 7 parameters (need a data science degree)
  - `trendstl(/host/key,100h:now/h-10h,100h,2h,3,"mad”,1001)`
- careful choice of seasonality
- no support for multiple seasons
- subsequence-based anomalies out of scope

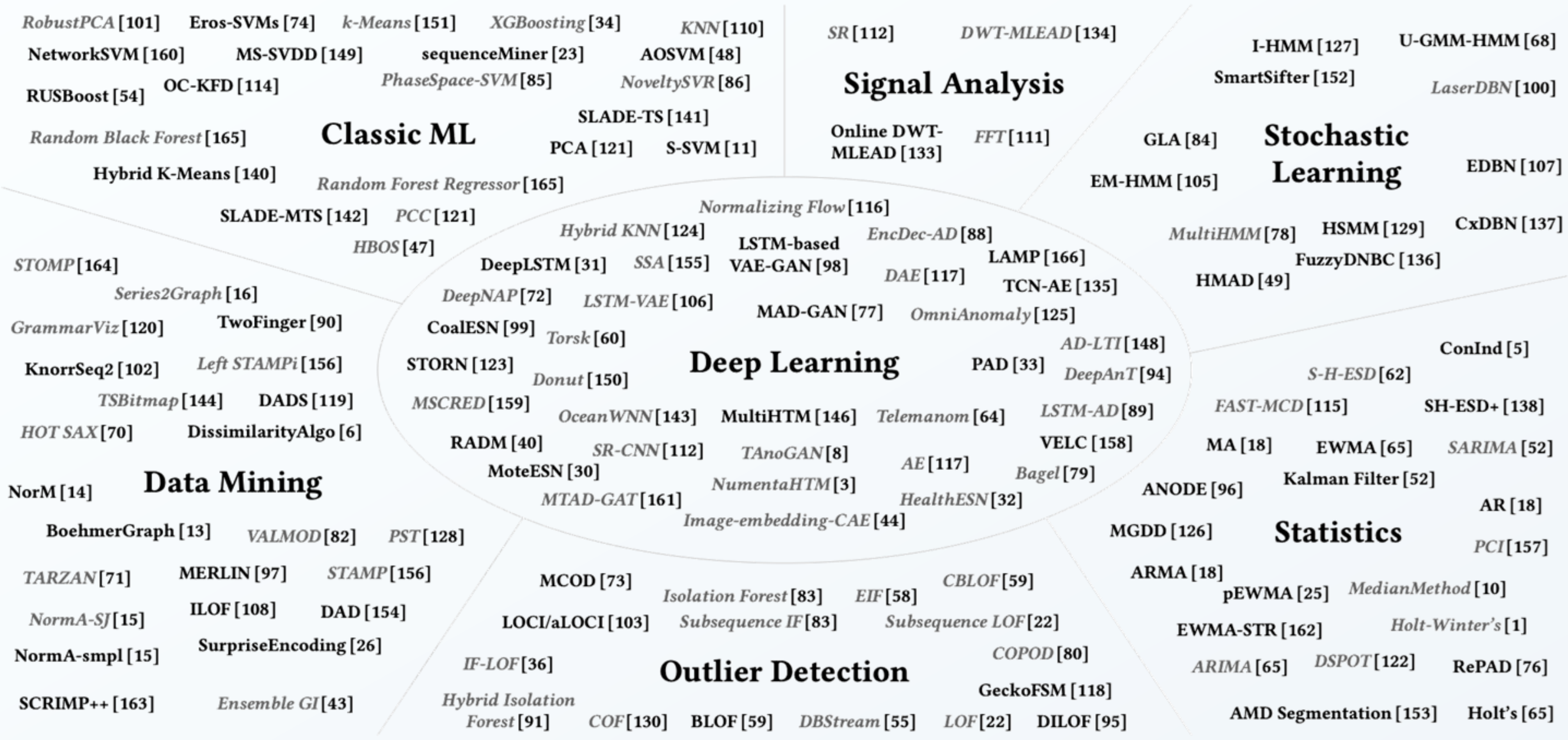
More detection methods

Requirements

- Performance and efficiency
- Easy to use (the less knobs and switches the better)
- Easy to understand and interpret results
- Subsequence-based anomalies
- Multiple seasonalities

Anomaly detection methods

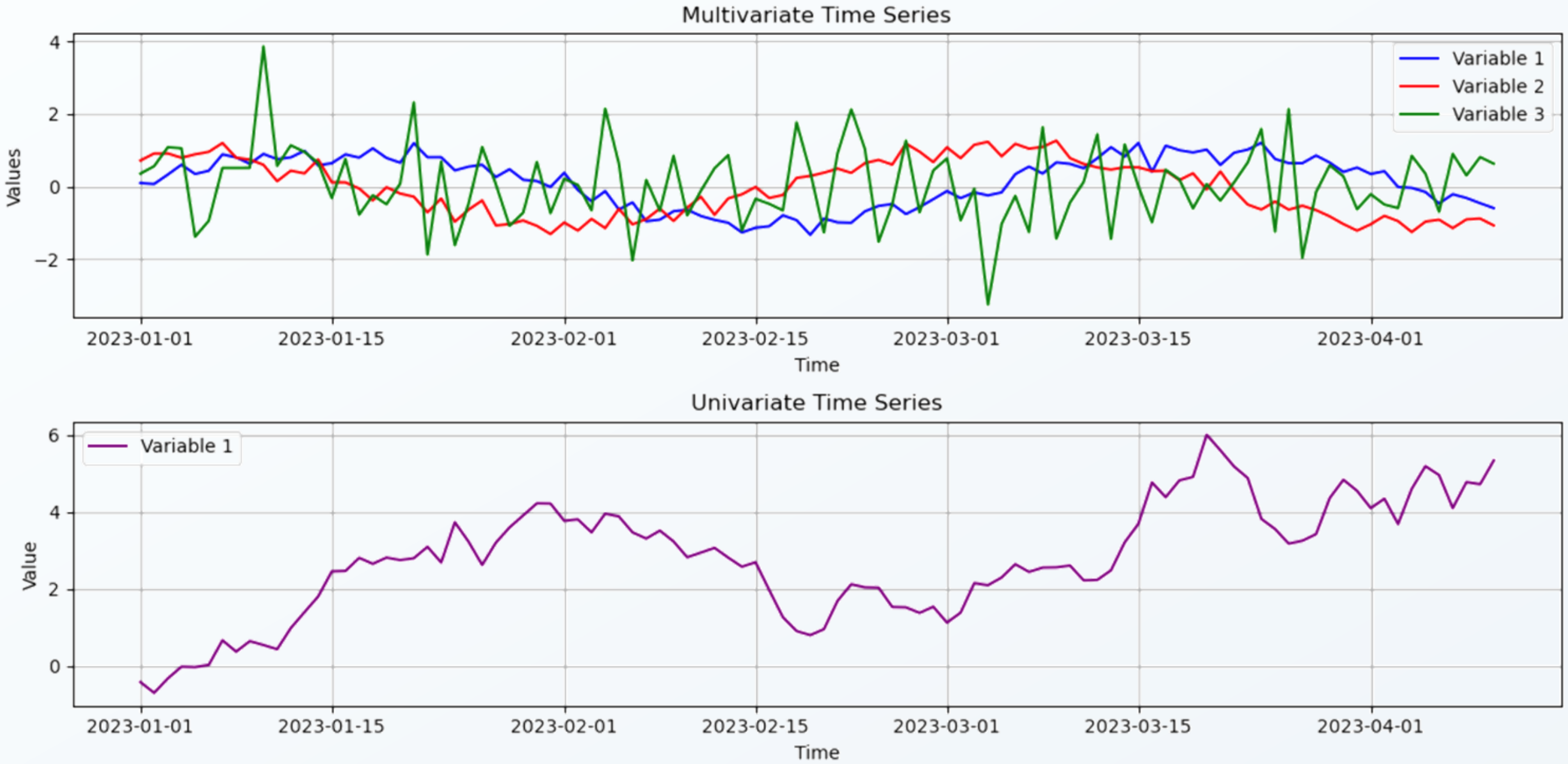
ZABBIX SUMMIT 2024



"Anomaly Detection in Time Series: A Comprehensive Evaluation"

Anomaly detection methods

Input types



Anomaly detection methods

Training types

- Supervised
  - Manual training
- Semi-supervised
  - Training on a clean data
- Unsupervised
  - No training

Image credit: Herluf Bidstrup

ZABBIX SUMMIT 2024

Anomaly detection methods

ZABBIX SUMMIT 2024

Anomaly detection methods

Types

- Statistical methods
  - Z-score, Moving Average, ARIMA, …
- Machine learning and data analysis methods
  - STL, FFT-based anomaly detection, …
- Deep learning methods
  - LSTM autoencoders, RNN, …

Deep learning – is it any good?

Deep learning methods

- Autoencoders
- Recurrent Neural Networks (RNNs)
- Generative Adversarial Networks (GANs)
- Convolutional Neural Networks (CNNs)
- LLMs (even!)

Deep learning – is it any good?

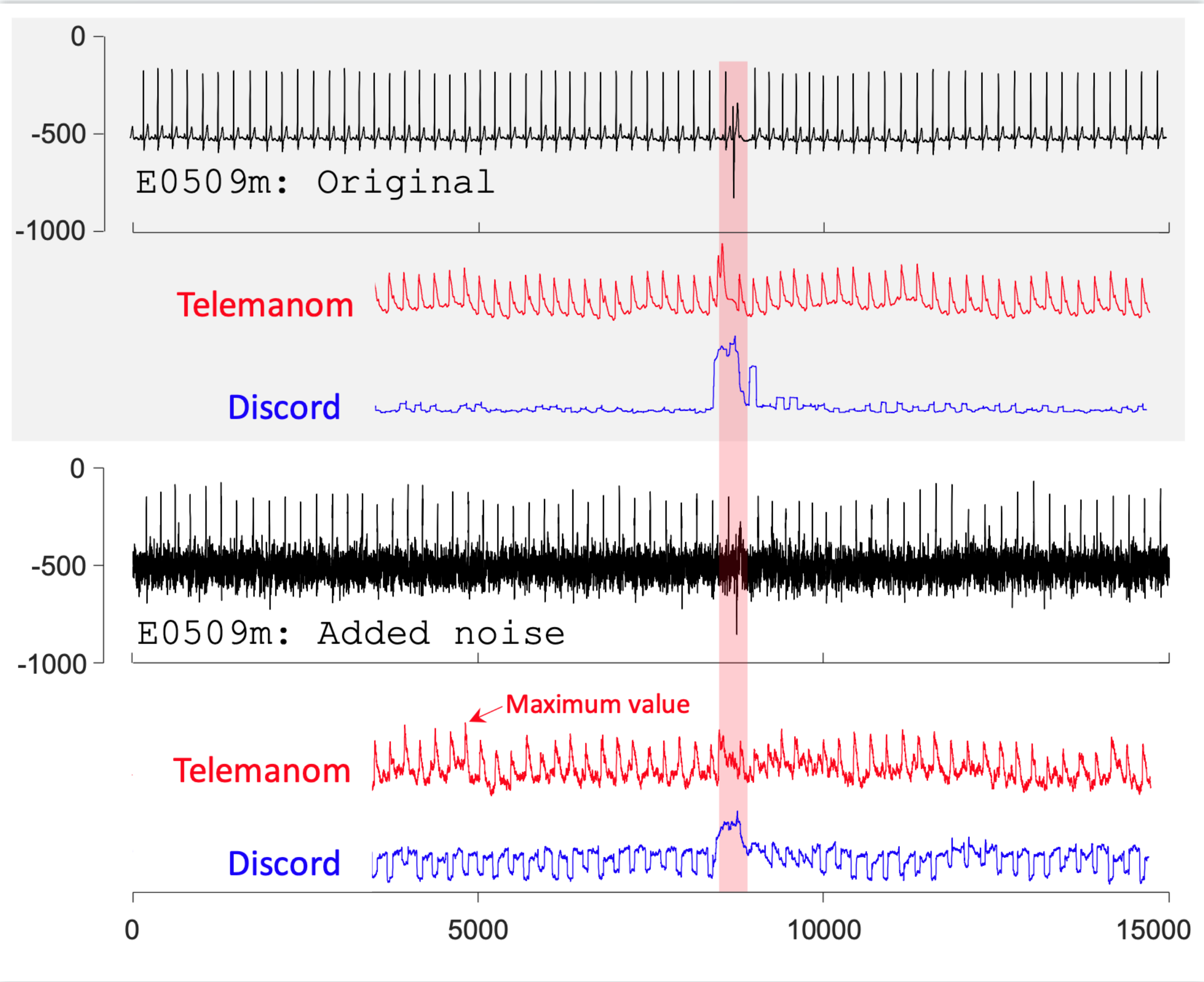
“most anomaly detection algorithms, especially ones based on deep learning, have ten or more parameters”

Wu, R., et al. "Current Time Series Anomaly Detection Benchmarks are Flawed and are Creating the Illusion of Progress" (2020)

“we are not aware of a single paper that presents forceful reproducible evidence that deep learning outperforms much simpler methods”

Wu, R., et al. "Current Time Series Anomaly Detection Benchmarks are Flawed and are Creating the Illusion of Progress" (2020)

Deep learning – is it any good?



"Current Time Series Anomaly Detection Benchmarks are Flawed and are Creating the Illusion of Progress"

ZABBIX SUMMIT 2024

Deep learning – is it any good?

ZABBIX SUMMIT 2024

“We found that deep learning approaches are not (yet) competitive despite their higher processing effort on training data”

Schmidl, S., et al. “Anomaly Detection in Time Series: A Comprehensive Evaluation.” (2022)

“Our experiments showed that the classical machine learning methods … outperform the deep learning methods.”

Rewicki, F., et al. “Is it worth it? Comparing six deep and classical methods for unsupervised anomaly detection in time series” (2023)

Deep learning – is it any good?

“The experiments showed that the statistical approaches perform best on univariate time-series … They also require less computation time compared to the other two classes.

Although deep learning approaches have gained huge attention by the … community in the last years, our results have revealed that they are not … able to achieve the accuracy values of the statistical methods on the univariate time-series benchmarks”

Braei, M., et al. “Anomaly Detection in Univariate Time-series: A Survey on the State-of-the-Art” (2020)

Deep learning – is it any good?

ZABBIX SUMMIT 2024

"… those [deep learning] methods, though potentially useful …, do not bring much additional value for the task of TAD [anomaly detection] and their complexity is definitely not justified.

What is even more worrisome, is that they managed to create up to now an illusion of progress"

M. Saquib Sarfraz, et al. "Position: Quo Vadis, Unsupervised Time Series Anomaly Detection?" (2024)

Deep learning – is it any good?

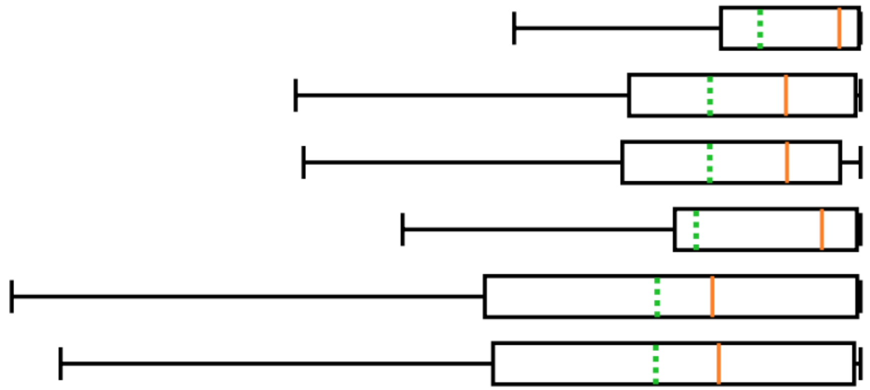
ZABBIX SUMMIT 2024

Zabbix requirements

- ~~Performance and efficiency~~
- ~~Easy to use (the less knobs and switches the better)~~
- ~~Easy to understand and interpret results~~
- Subsequence-based anomalies
- Multiple seasonalities

Distance-based methods

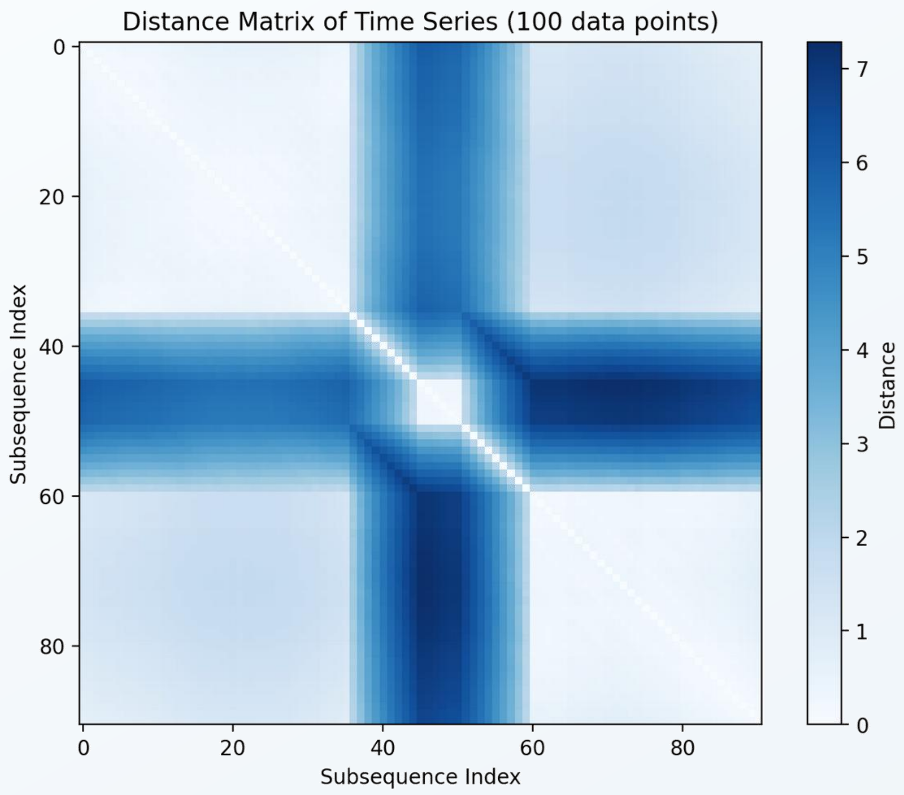
Learn.	Algorithm	TL	OOM	ERR	AUC-ROC all datasets
	● Sub-LOF [22]	2 %	0 %	0 %	
	▼ GrammarViz [120]	3 %	0 %	0 %	
	▲ DWT-MLEAD [134]	0 %	0 %	0 %	
	● VALMOD [82]	1 %	9 %	11 %	
	● SAND [17]	5 %	1 %	22 %	
	● Left STAMPi [156]	2 %	0 %	1 %	



"Anomaly Detection in Time Series: A Comprehensive Evaluation"

Matrix Profile

- Method, not an algorithm
  - STAMP, STOMP, SCRIMP, SCRIMP++, SCAMP, VALMOD, MERLIN, …
- Distance-based
  - Calculates nearest neighbours
- Subsequences of constant length
  - Motifs – similar subsequences
  - Discords – anomalies
- Fast on long subsequences
- Predictable time

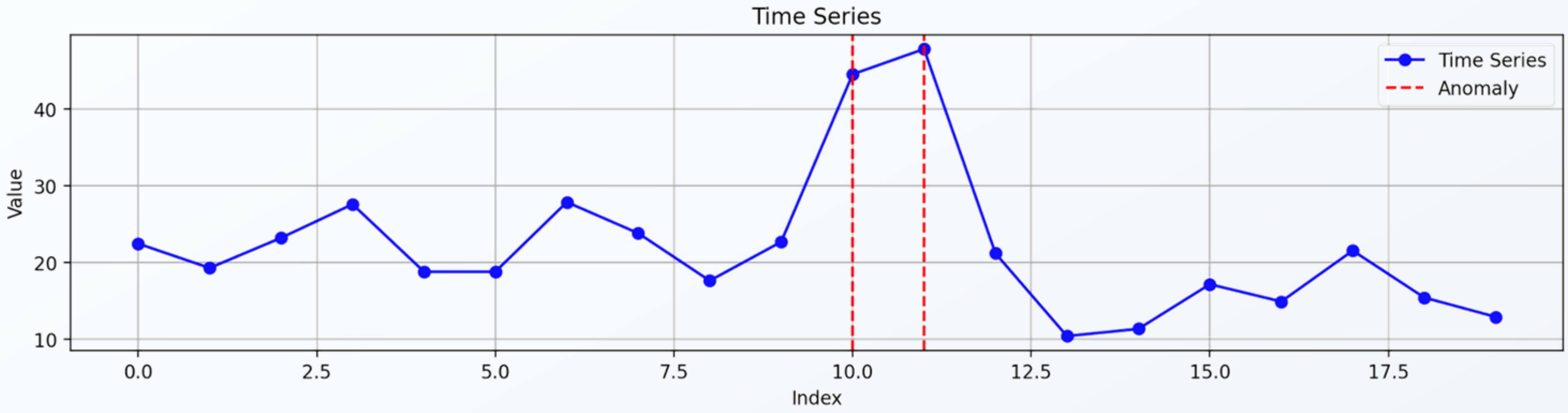


Matrix Profile

- Applicable for subsequence and point-based anomalies
- Easily parallelizable
- No false positives
- No tuning parameters
- Used in many domains
  - IT infrastructure, IoT, space and sattelites, medicine, seismology, industrial equipment, water distribution, …

Matrix Profile

Calculation

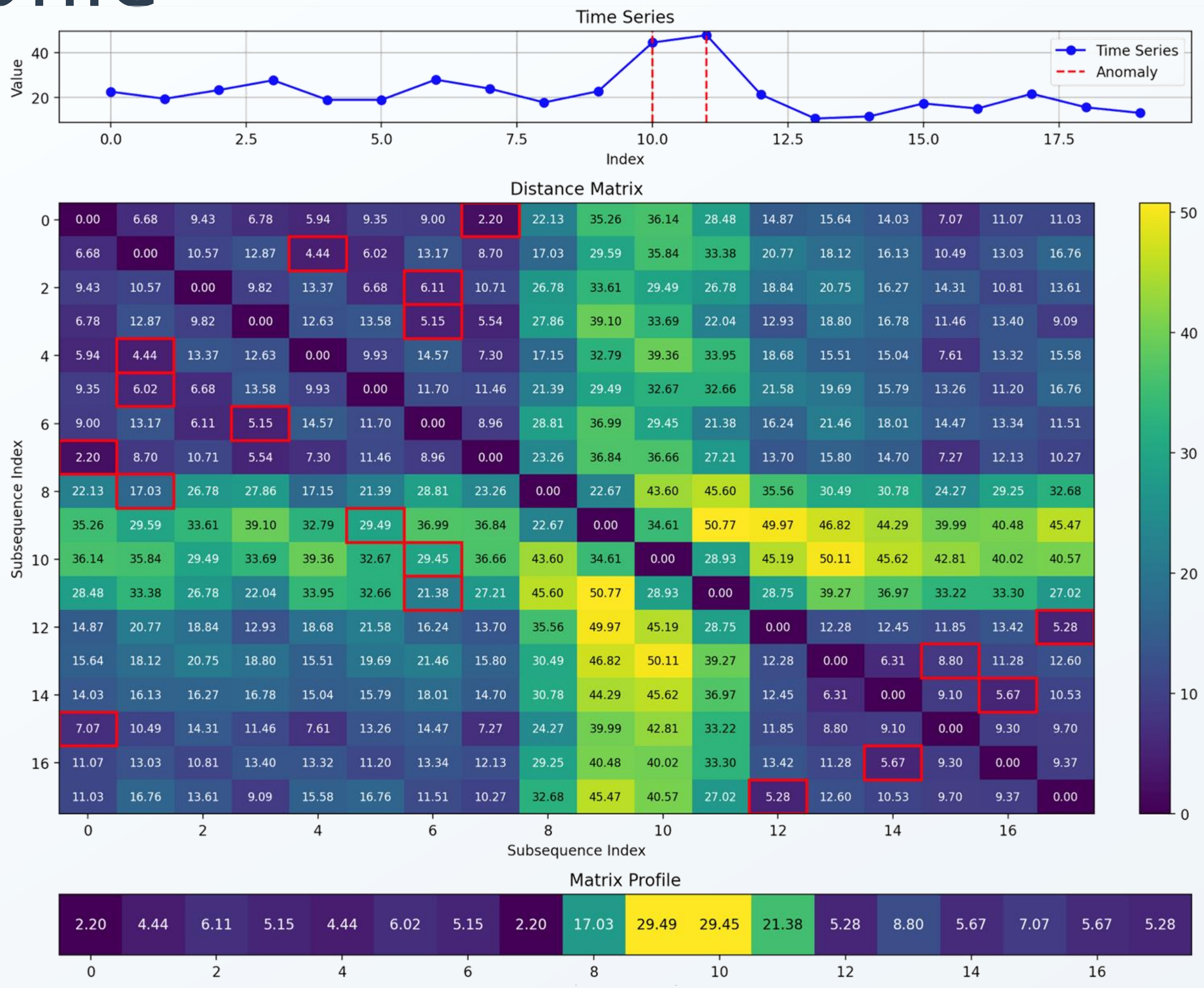


Matrix Profile

Calculation

(naïve approach)

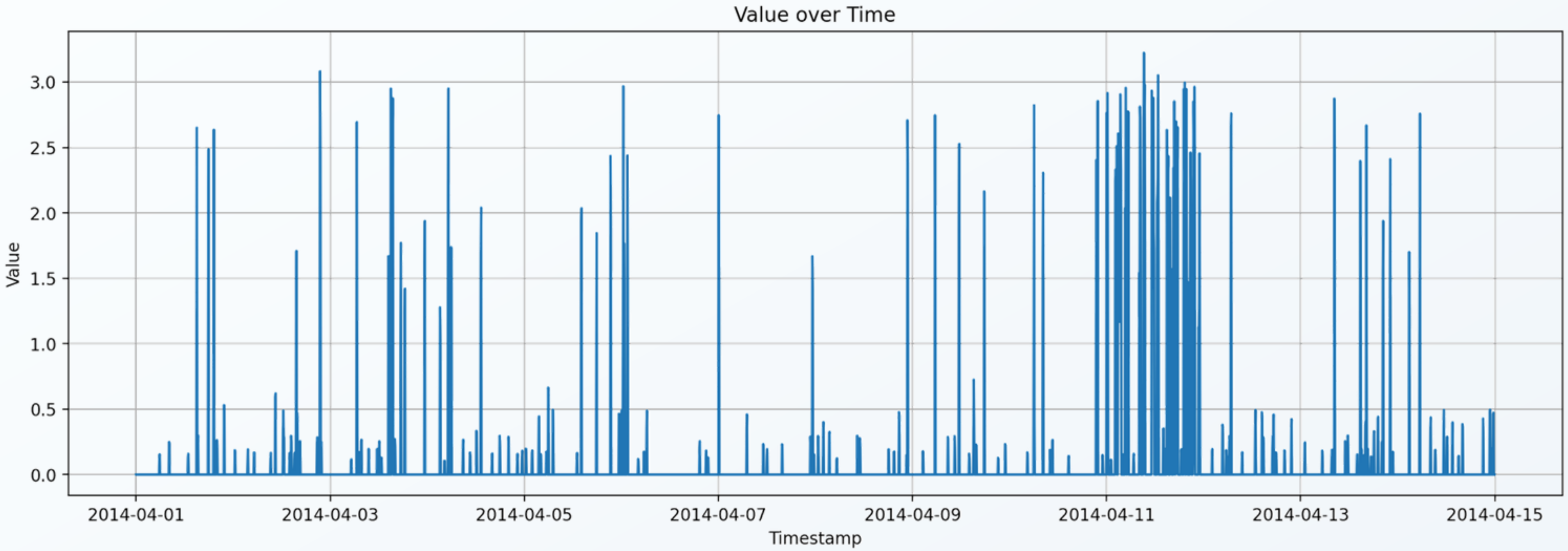
- Get distances between all subsequences
- Get minimum for every row
- Compose profile



Matrix Profile - Examples

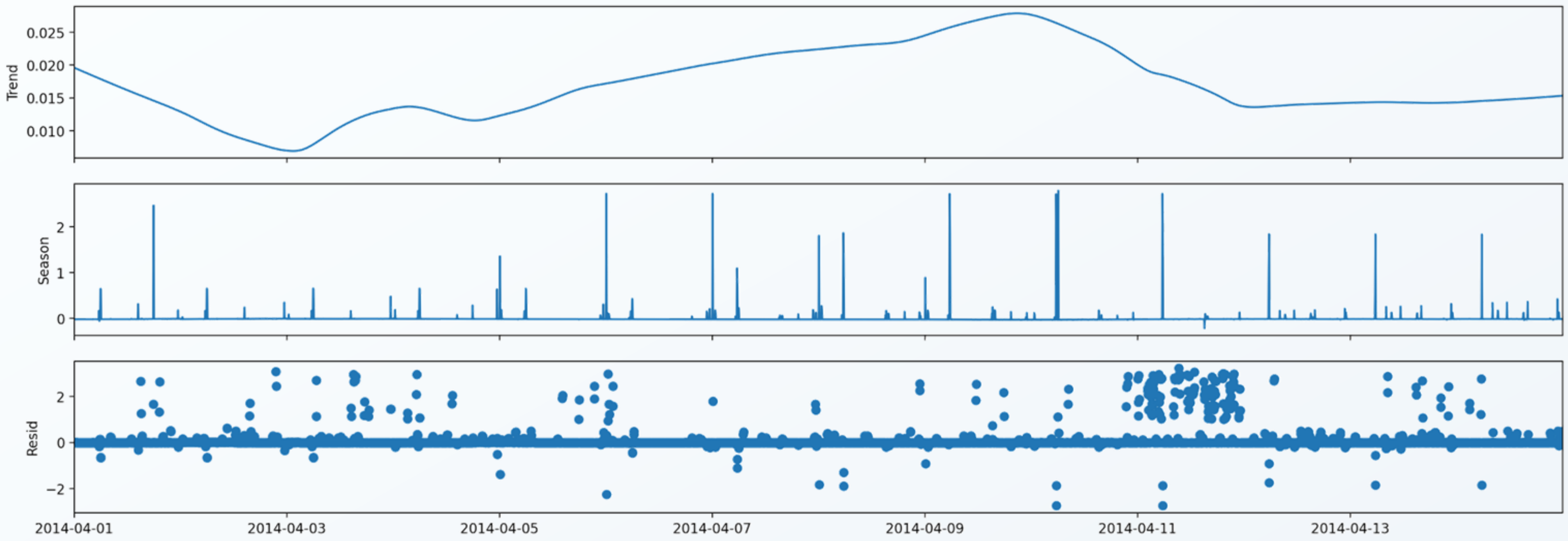
ZABBIX SUMMIT 2024

Raw data - load



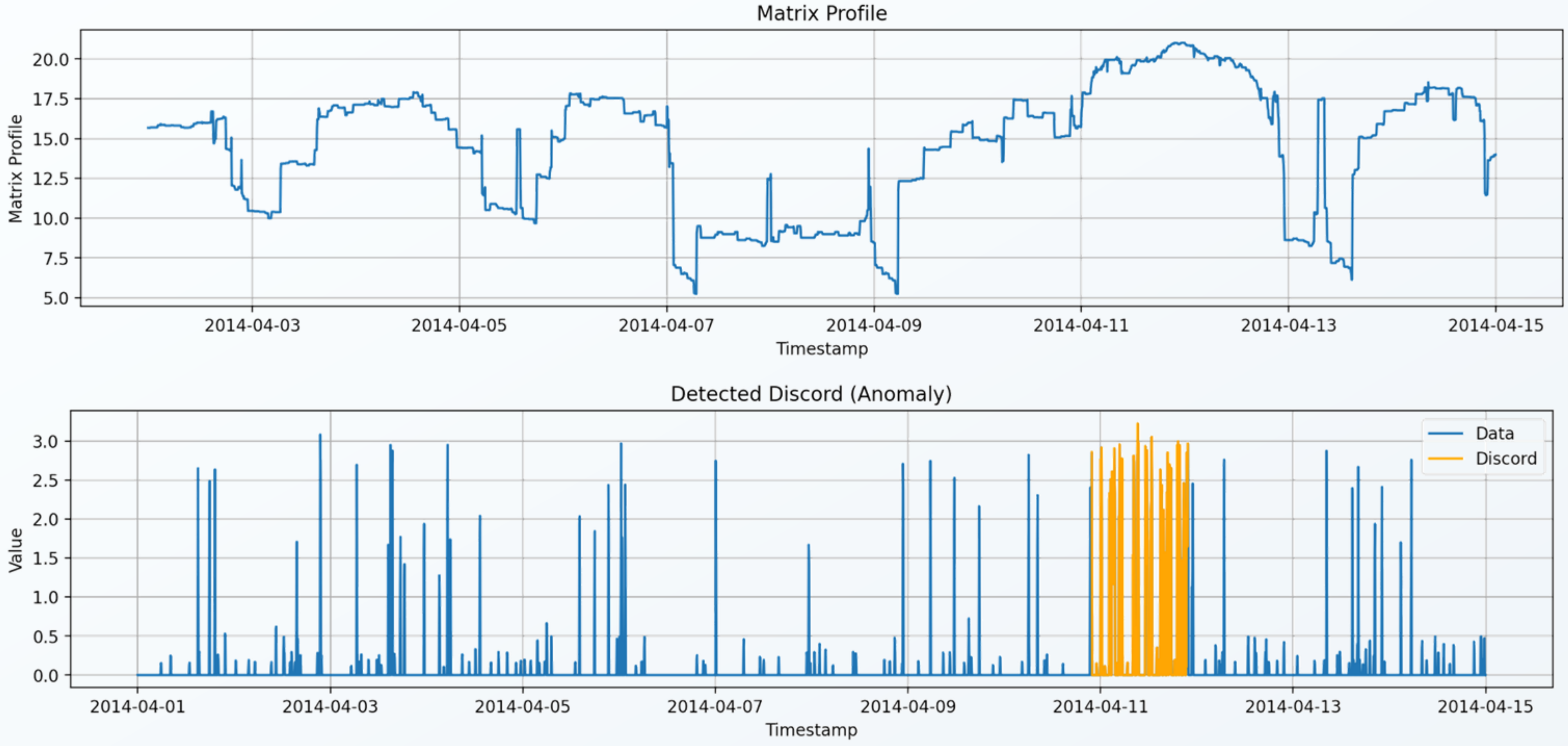
Matrix Profile - Examples

STL analysis – not good



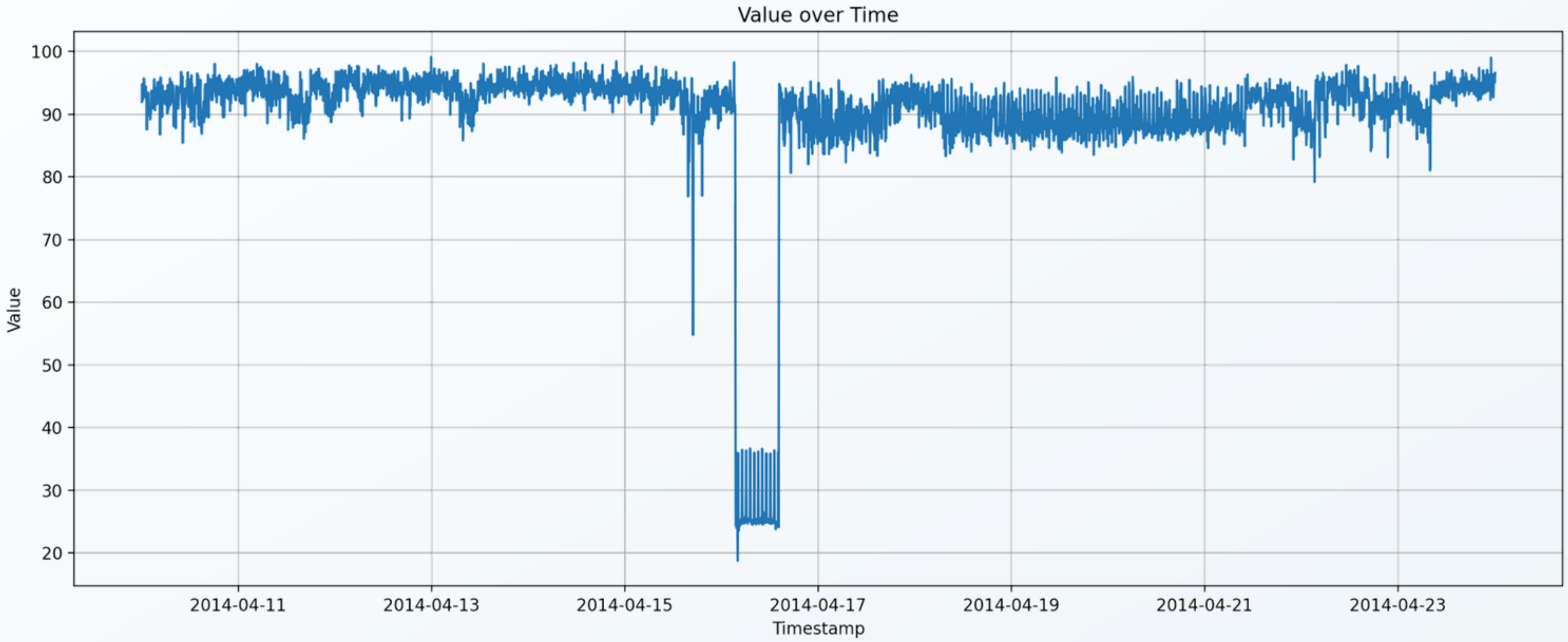
Matrix Profile - Examples

Matrix Profile analysis



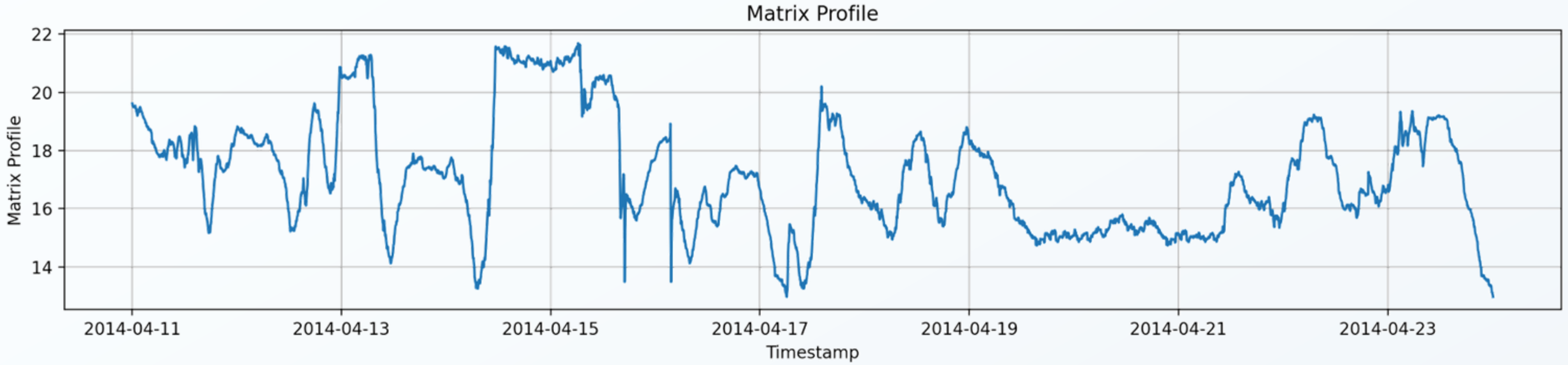
Matrix Profile - Examples

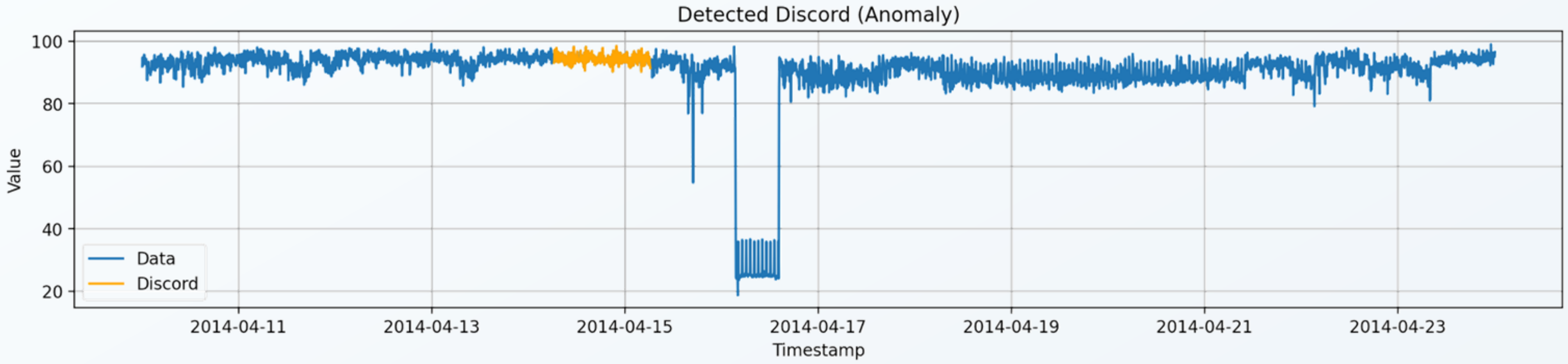
Raw data – CPU utilization



Matrix Profile - Examples

Matrix Profile analysis: Z-normalization

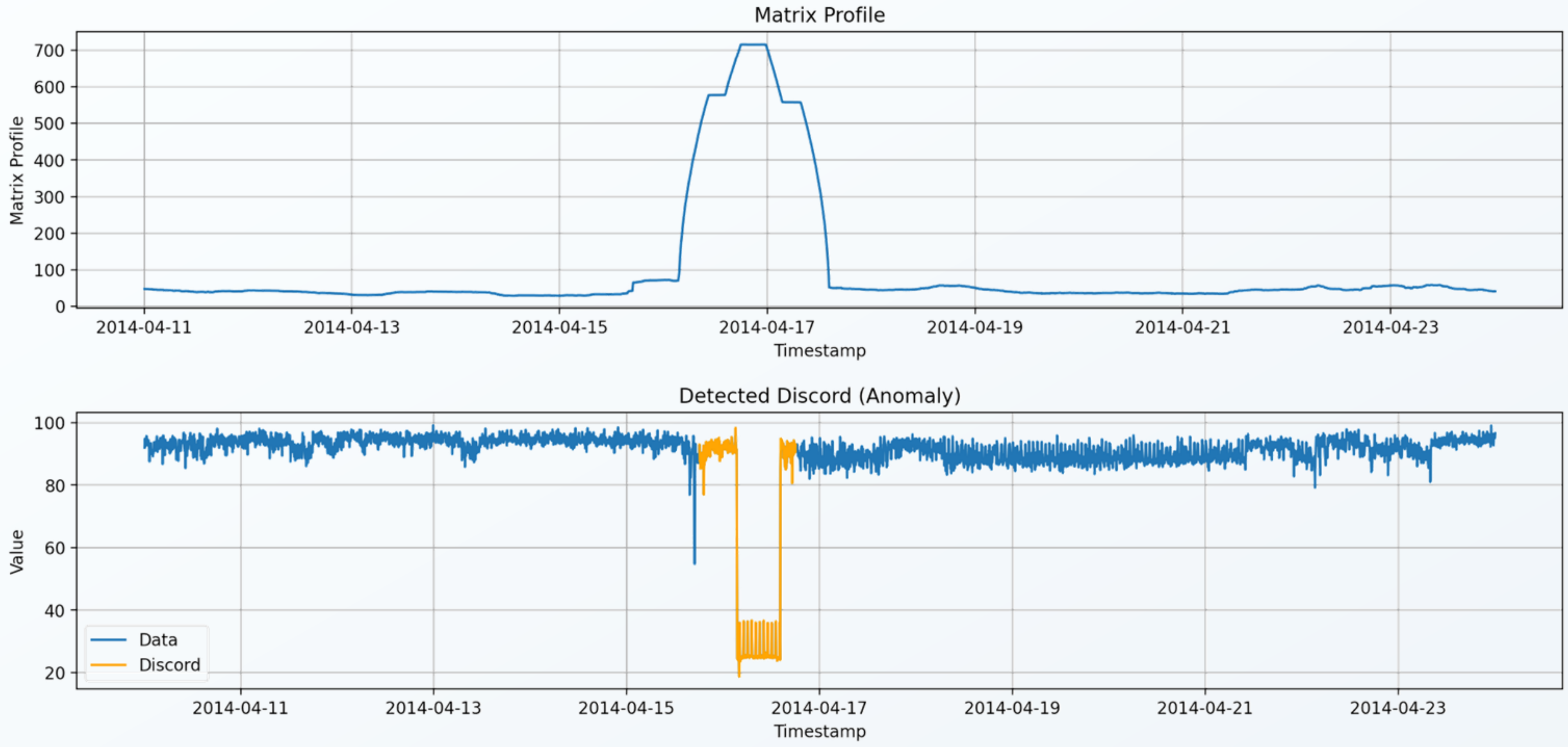




Matrix Profile - Examples

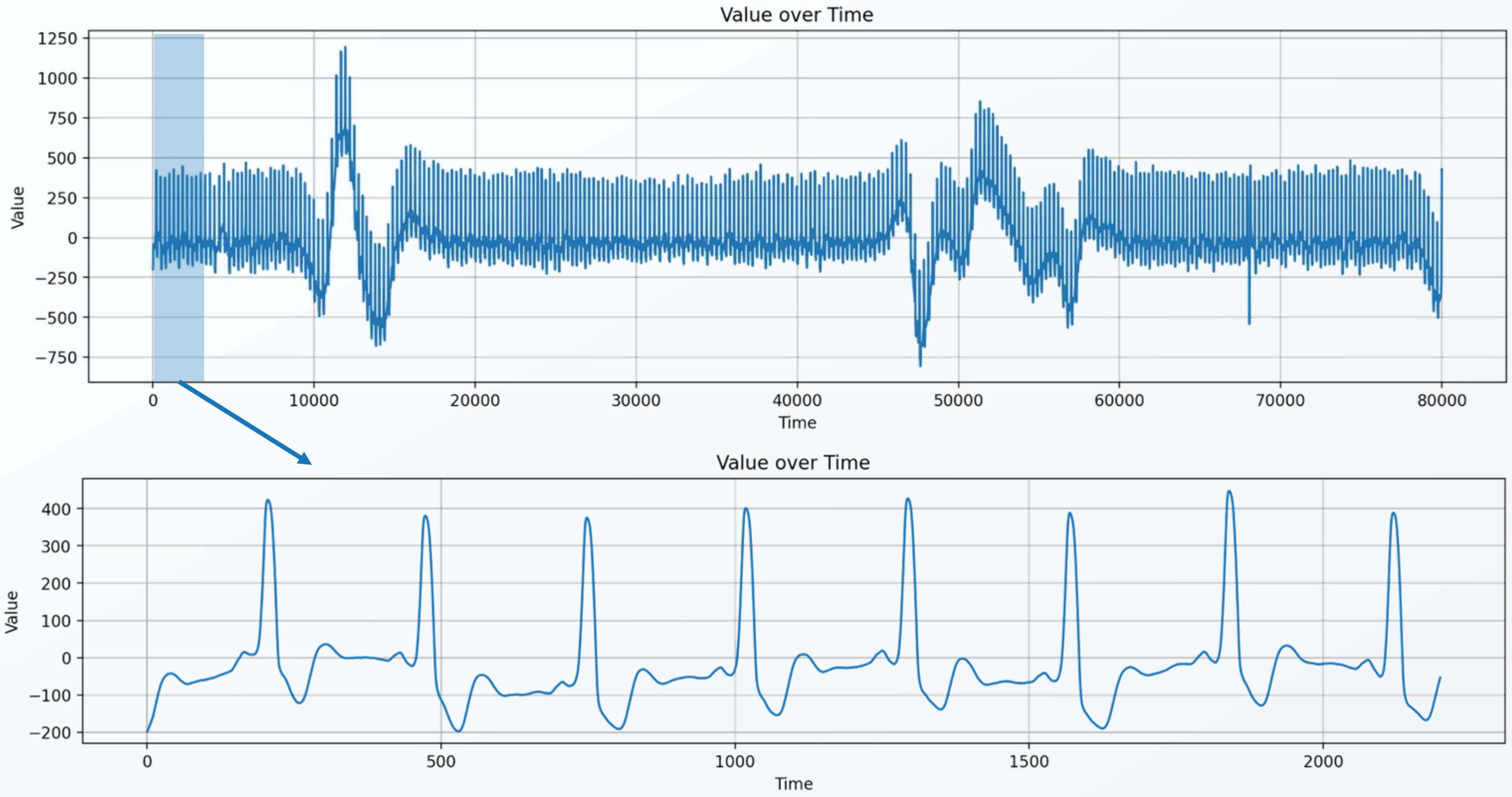
ZABBIX SUMMIT 2024

Matrix Profile analysis: Z-normalization off



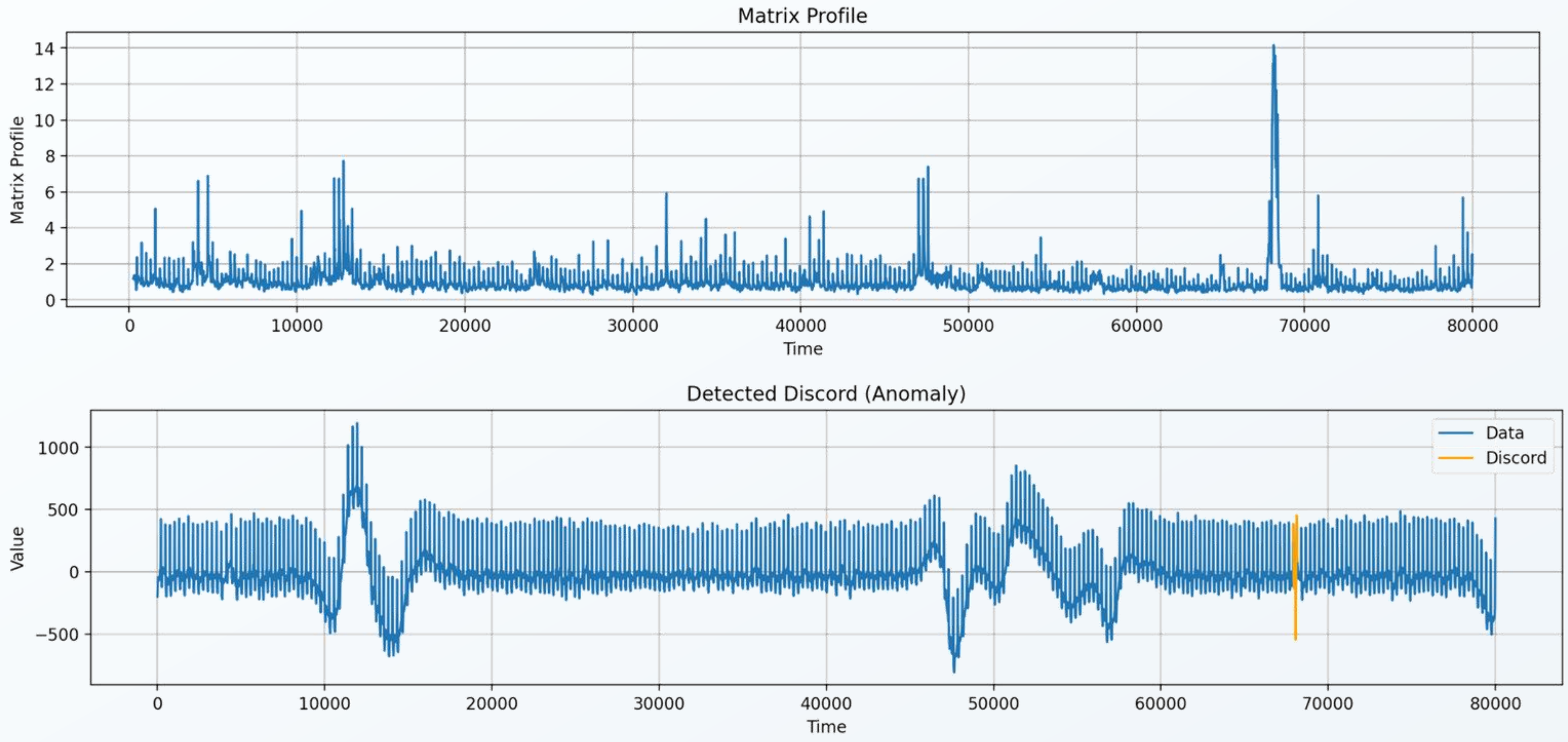
Matrix Profile - Examples

Raw data – ECG



Matrix Profile - Examples

Matrix Profile analysis



Matrix Profile

ZABBIX SUMMIT 2024

Zabbix requirements

- Performance and efficiency ☑
- Easy to use ☑
- Easy to understand and interpret results ☑
- Subsequence-based anomalies ☑
- Multiple seasonalities

ZABBIX SUMMIT 2024

Multiple seasonalities

Contenders

- Prophet
  - Released by Facebook in 2017
  - Unlimited seasonalities
  - Easy to use
  - Designed for business data
  - Primary goal is forecasting

Forecasting at Scale

Sean J. Taylor*†
Facebook, Menlo Park, California, United States
sjt@fb.com

and

Benjamin Letham†
Facebook, Menlo Park, California, United States
bletham@fb.com

Abstract

Forecasting is a common data science task that helps organizations with capacity planning, goal setting, and anomaly detection. Despite its importance, there are serious challenges associated with producing reliable and high quality forecasts – especially when there are a variety of time series and analysts with expertise in time series modeling are relatively rare. To address these challenges, we describe a practical approach to forecasting "at scale" that combines configurable models with analyst-in-the-loop performance analysis. We propose a modular regression model with interpretable parameters that can be intuitively adjusted by analysts with domain knowledge about the time series. We describe performance analyses to compare and evaluate forecasting procedures, and automatically flag forecasts for manual review and adjustment. Tools that help analysts to use their expertise most effectively enable reliable, practical forecasting of business time series.

Keywords: Time Series, Statistical Practice, Nonlinear Regression

Multiple seasonalities

Contenders

- **MSTL**
  - New, published in 2021
  - Extension of STL
  - Unlimited seasonalities, detects seasons automaticaly
  - Tuning parameters
  - Faster than Prophet

MSTL: A Seasonal-Trend Decomposition Algorithm for Time Series with Multiple Seasonal Patterns

Kasun Bandara[a,*], Rob J Hyndman[b], Christoph Bergmeir[c]

[a]*School of Computing and Information Systems, Melbourne Centre for Data Science, University of Melbourne*
[b]*Department of Econometrics and Business Statistics, Monash University*
[c]*Department of Data Science and AI, Monash University*

Abstract

The decomposition of time series into components is an important task that helps to understand time series and can enable better forecasting. Nowadays, with high sampling rates leading to high-frequency data (such as daily, hourly, or minutely data), many real-world datasets contain time series data that can exhibit multiple seasonal patterns. Although several methods have been proposed to decompose time series better under these circumstances, they are often computationally inefficient or inaccurate. In this study, we propose Multiple Seasonal-Trend decomposition using Loess (MSTL), an extension to the traditional Seasonal-Trend decomposition using Loess (STL) procedure, allowing the decomposition of time series with multiple seasonal patterns. In our evaluation on synthetic and a perturbed real-world time series dataset, compared to other decomposition benchmarks, MSTL demonstrates competitive results with lower computational cost. The implementation of MSTL is available in the R package *forecast*.

Keywords: Time Series Decomposition, Multiple Seasonality, MSTL, TBATS, STR

*Corresponding Author Name: Kasun Bandara, Affiliation: School of Computing and Information Systems, Melbourne Centre for Data Science, University of Melbourne, Melbourne, Australia, Postal Address: School of Computing and Information Systems, The University of Melbourne, Victoria 3052, Australia, E-mail address: Kasun.Bandara@unimelb.edu.au

ZABBIX SUMMIT 2024

Coming to Zabbix

ZABBIX SUMMIT 2024

Trigger functions

- `trendmp(/host/key,eval,detect,subseq)`
  - Number of discords
- `trendmseason(/host/key,eval,detect)`
  - Anomaly rate

Further plans and research

- Include anomaly detection in standard templates
- MERLIN, VALMOD
- Multivariate anomaly detection
- Untie from trends
- Mark anomalies on graphs

References

- Schmidl, S., et al. "*Anomaly Detection in Time Series: A Comprehensive Evaluation.*", 2022
- Rewicki, F., et al. "*Is it worth it? Comparing six deep and classical methods for unsupervised anomaly detection in time series*", 2024
- Braei, M., et al. "*Anomaly Detection in Univariate Time-series: A Survey on the State-of-the-Art*", 2020
- Wu, R., et al. "*Current Time Series Anomaly Detection Benchmarks are Flawed and are Creating the Illusion of Progress*", 2020
- M. Saquib Sarfraz, et al. "*Position: Quo Vadis, Unsupervised Time Series Anomaly Detection?*", 2024
- Keogh, E., et al. "*Matrix Profile I: All Pairs Similarity Joins for Time Series: A Unifying View that Includes Motifs, Discords and Shapelets*", 2016
- Taylor, S.J., Letham, B. "*Forecasting at Scale*", 2017
- Bandara, K. "*MSTL: A Seasonal-Trend Decomposition Algorithm for Time Series with Multiple Seasonal Patterns*", 2021
- Hoang, D., et al. "The UCR Time Series Classification Archive", https://www.cs.ucr.edu/~eamonn/time_series_data_2018/
- Numenta, "Numenta Anomaly Benchmark", https://github.com/numenta/NAB

Thank you!