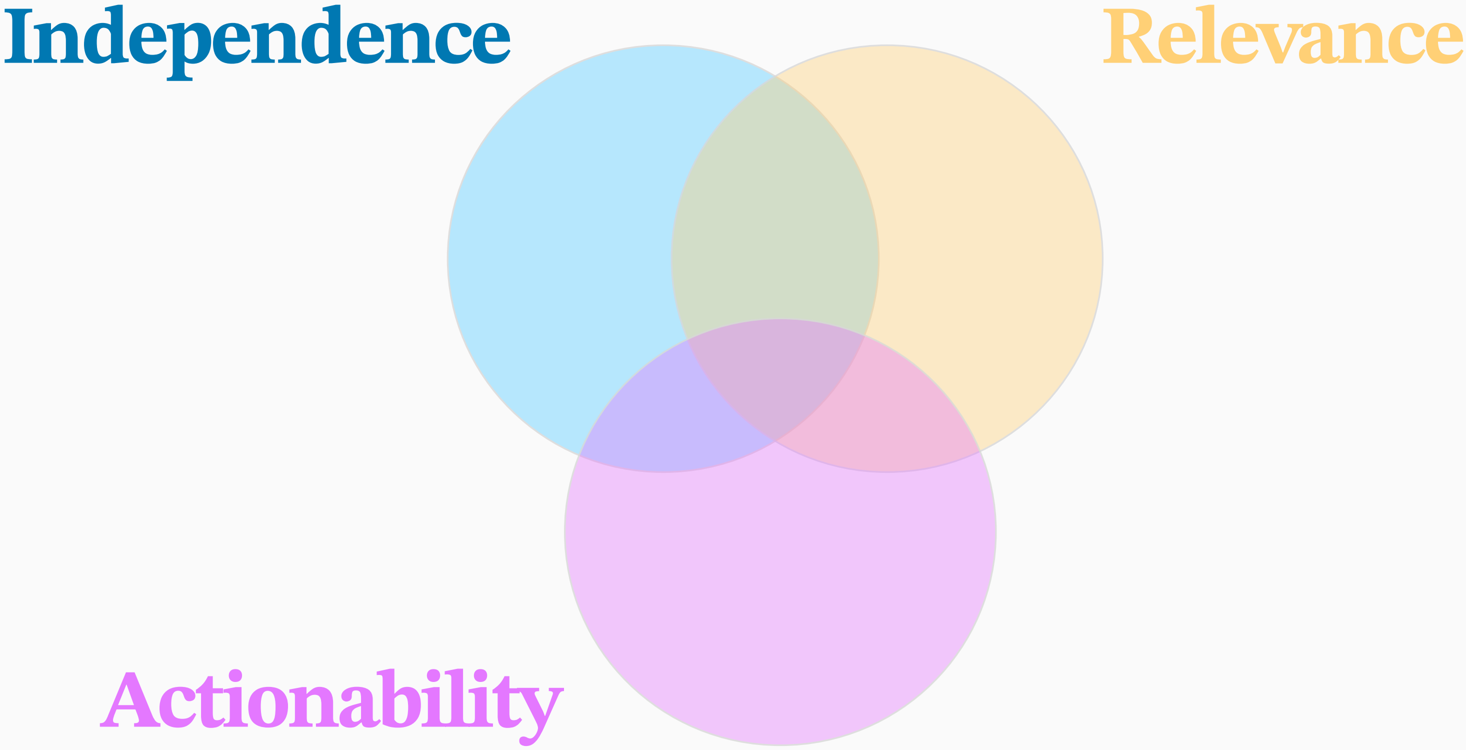
MAD: One-Shot Machine Activity Detector for Physics-Based Cyber Security

Arthur Grisel-Davy, Sebastian Fischmeister

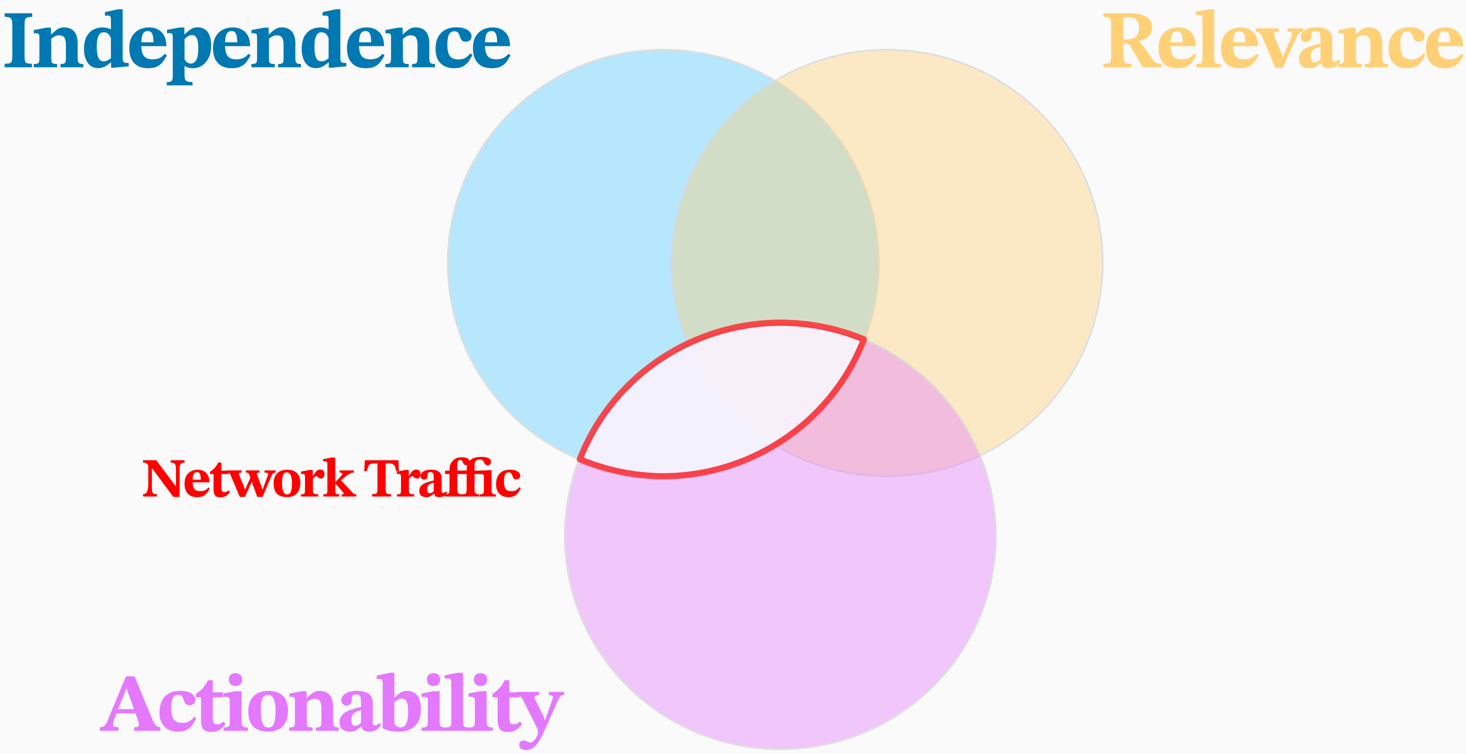
University of Waterloo

agriseld@uwaterloo.ca

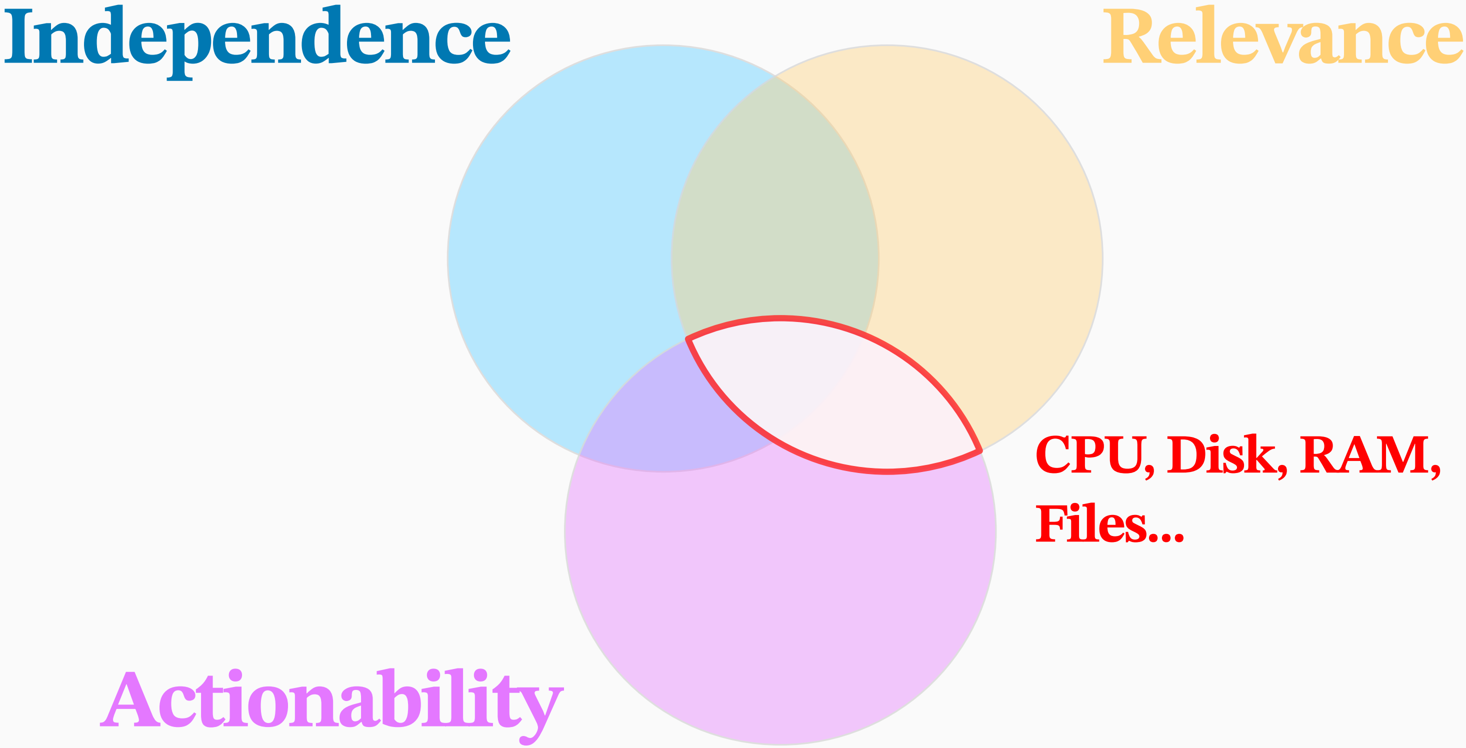
Introduction



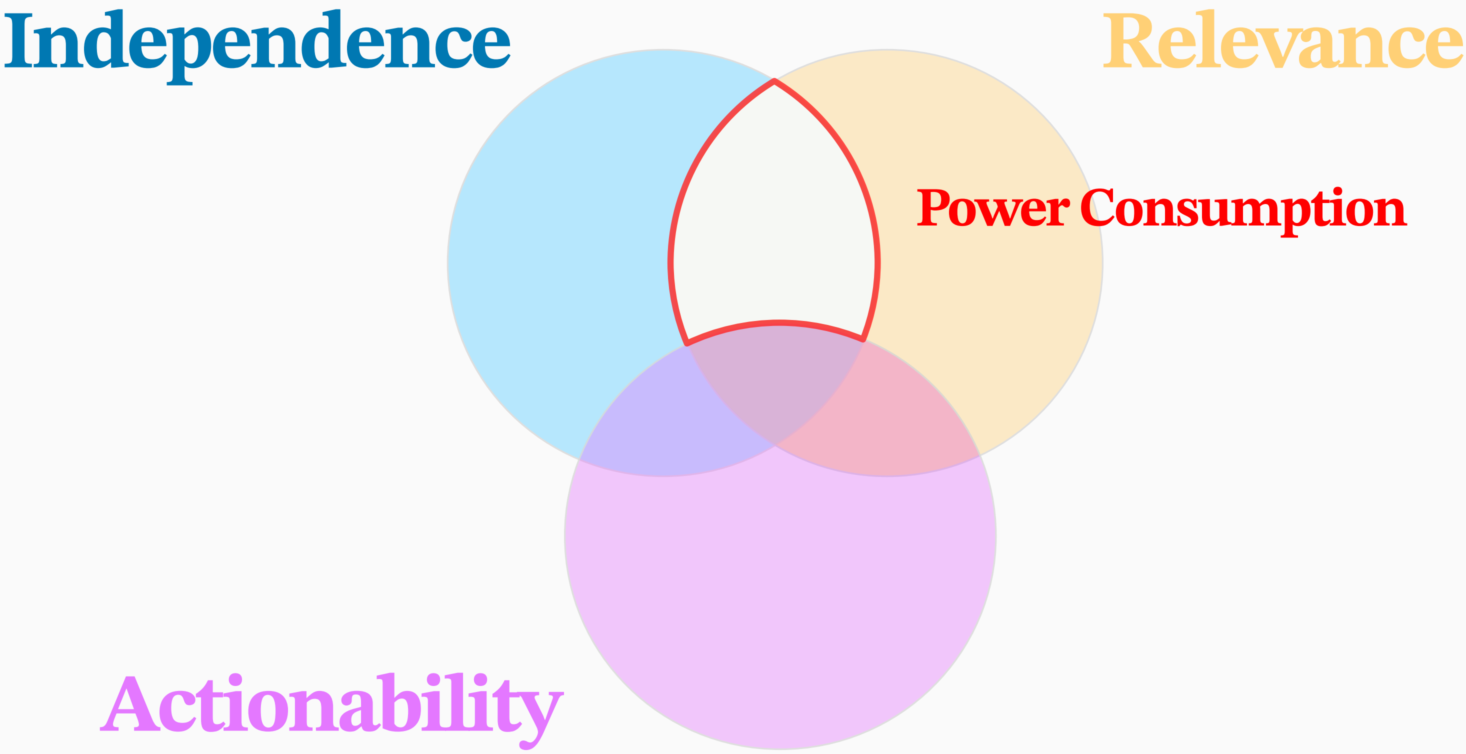
Introduction



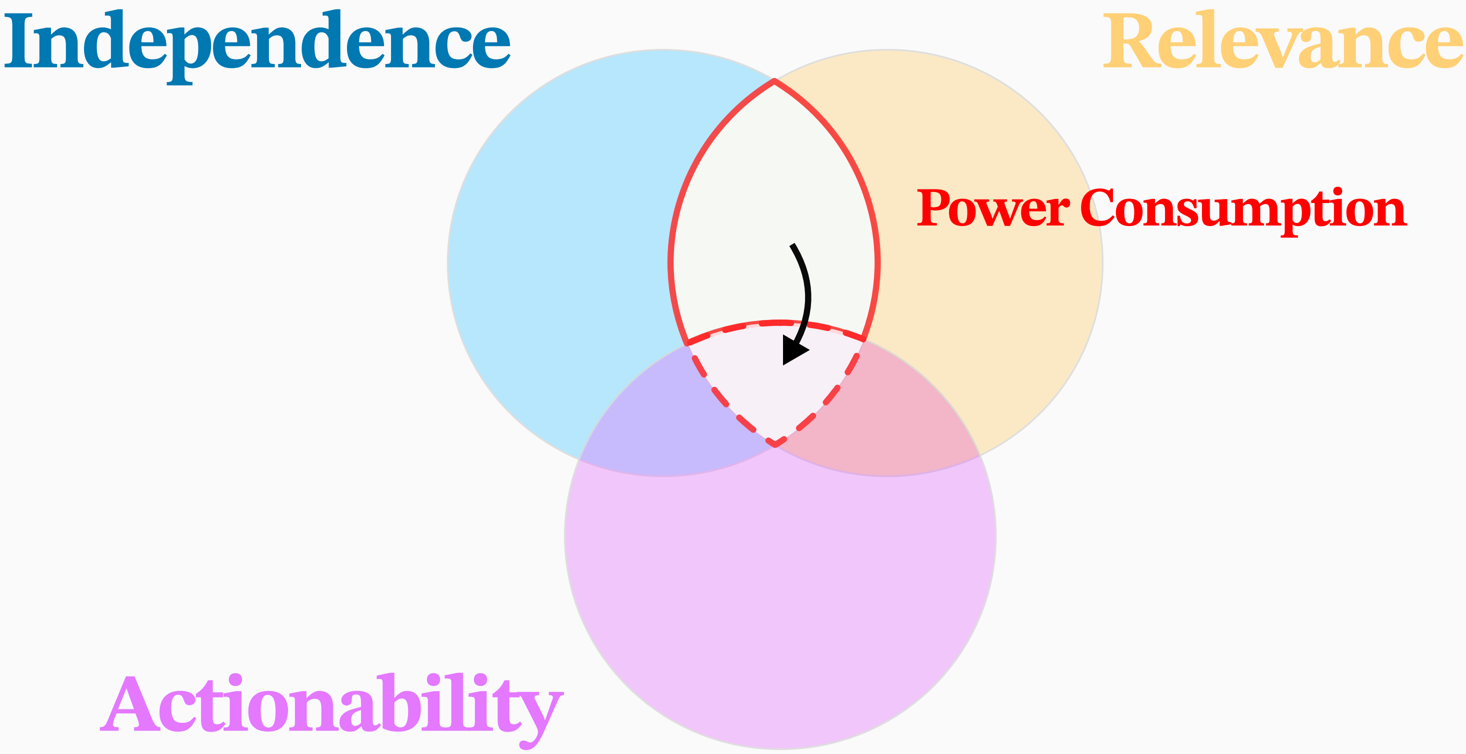
Introduction



Introduction



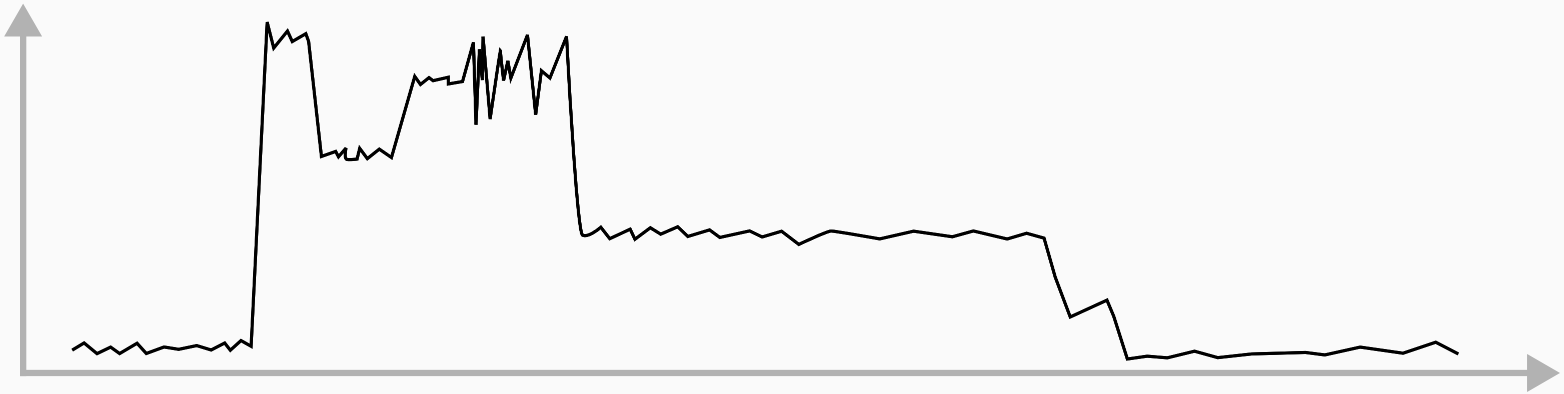
Introduction



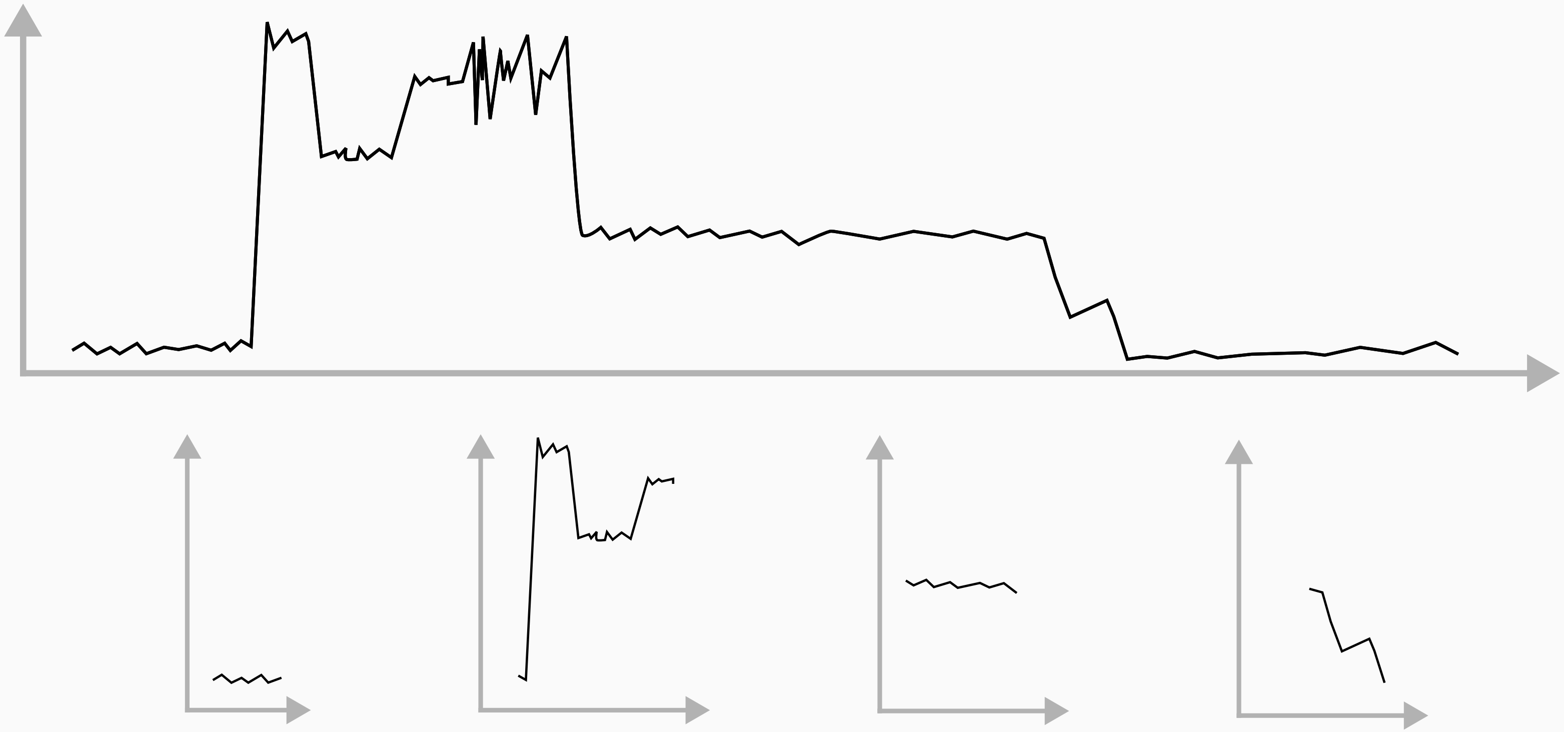
Problem Statement

Given a discretized time series t and a set of patterns $P = \{P_1, \ldots, P_n\}$, identify a mapping $m : \mathbb{N} \longrightarrow P \cup \lambda$ such that every sample $t[i]$ maps to a pattern in $P \cup \lambda$ with the condition that the sample matches an occurrence of the pattern in t.

Proposed Approach

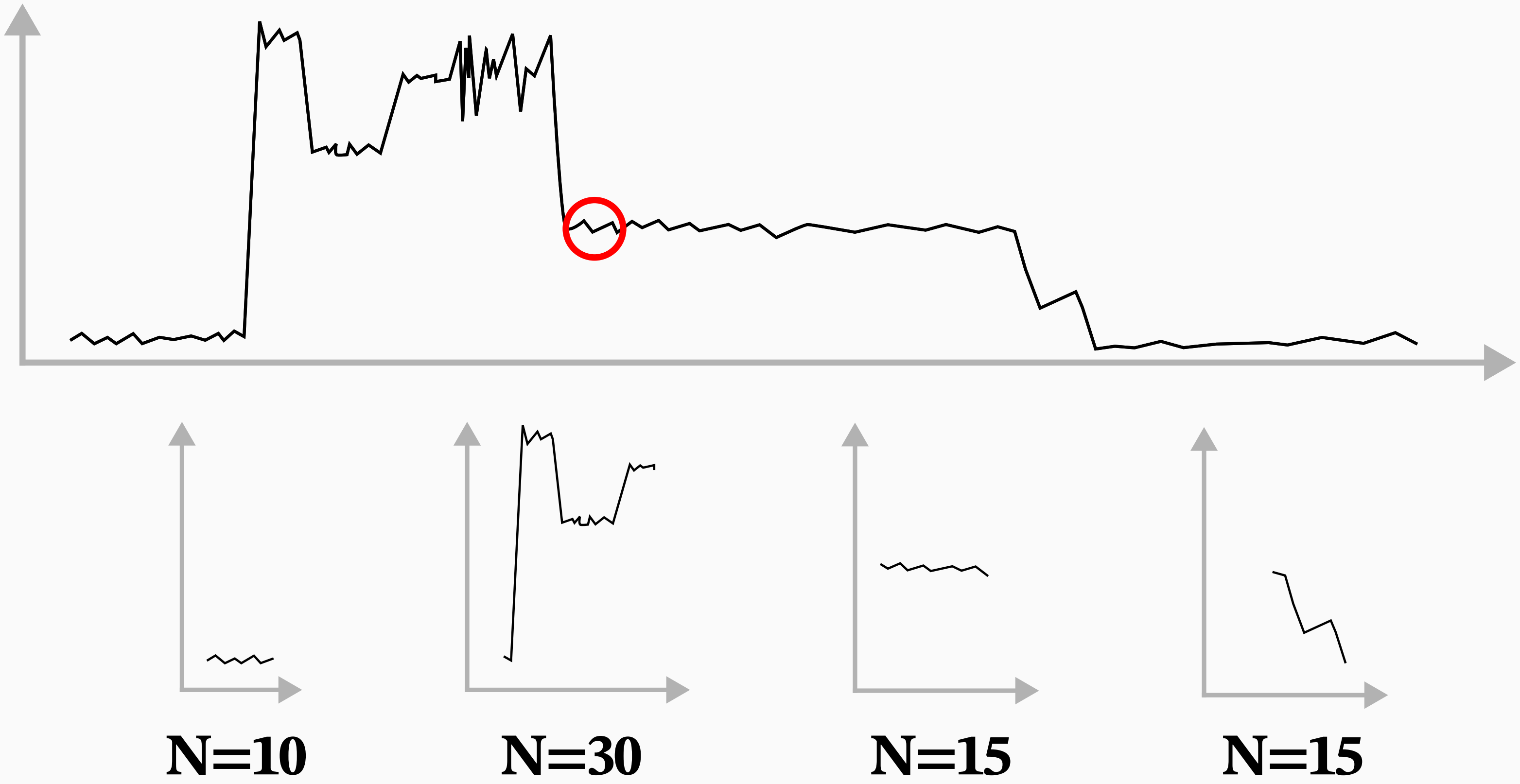


Proposed Approach

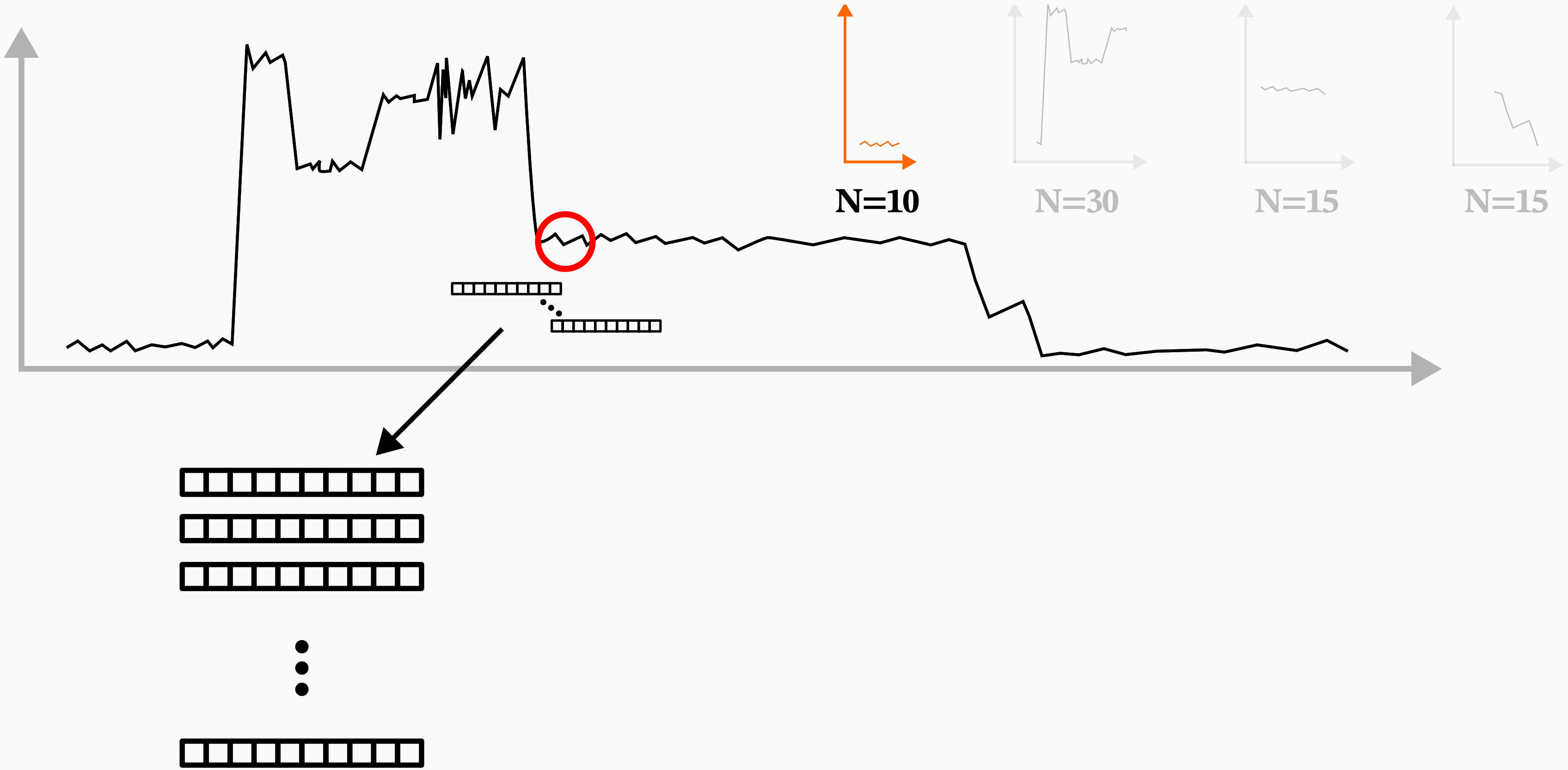


N=10 N=30 N=15 N=15

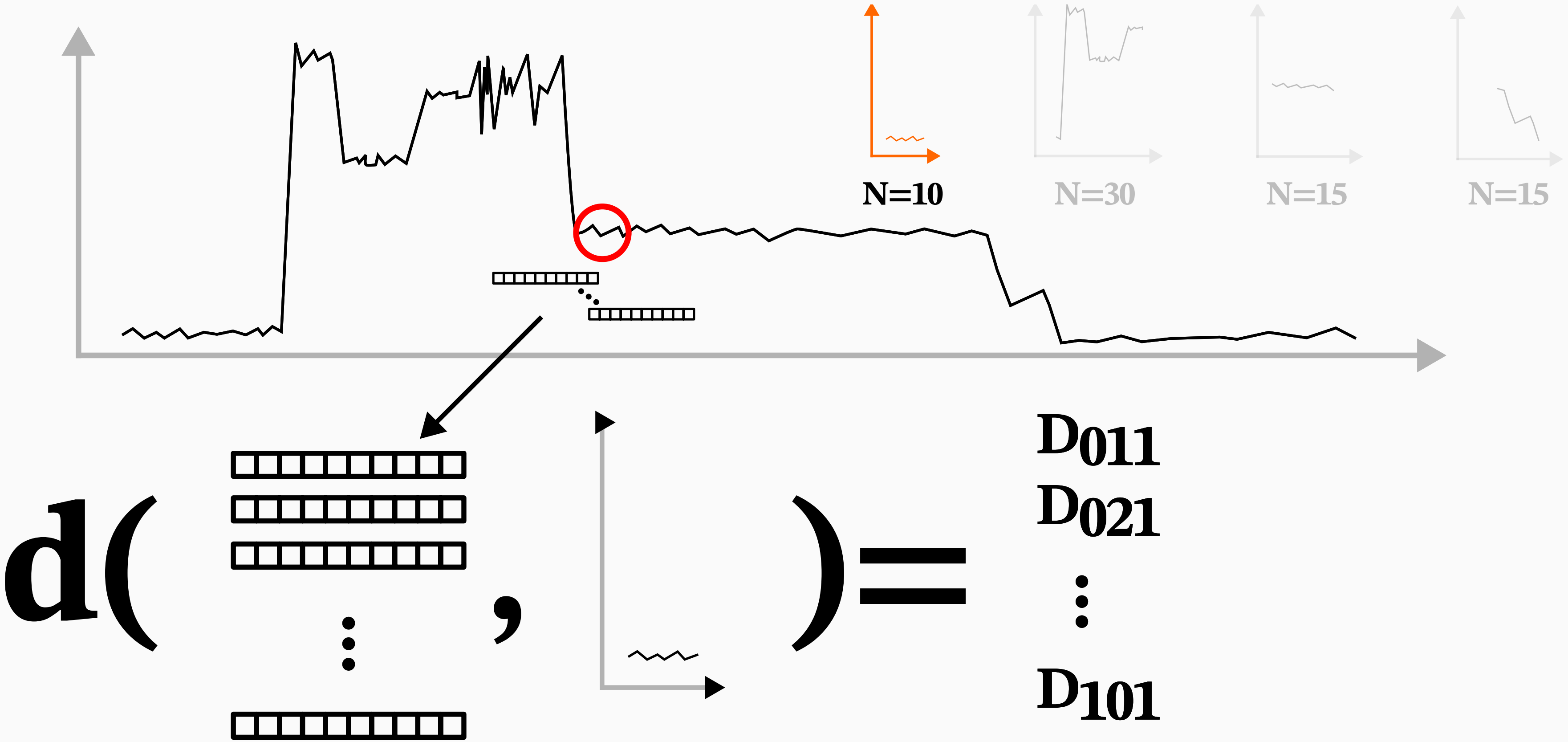
Proposed Approach



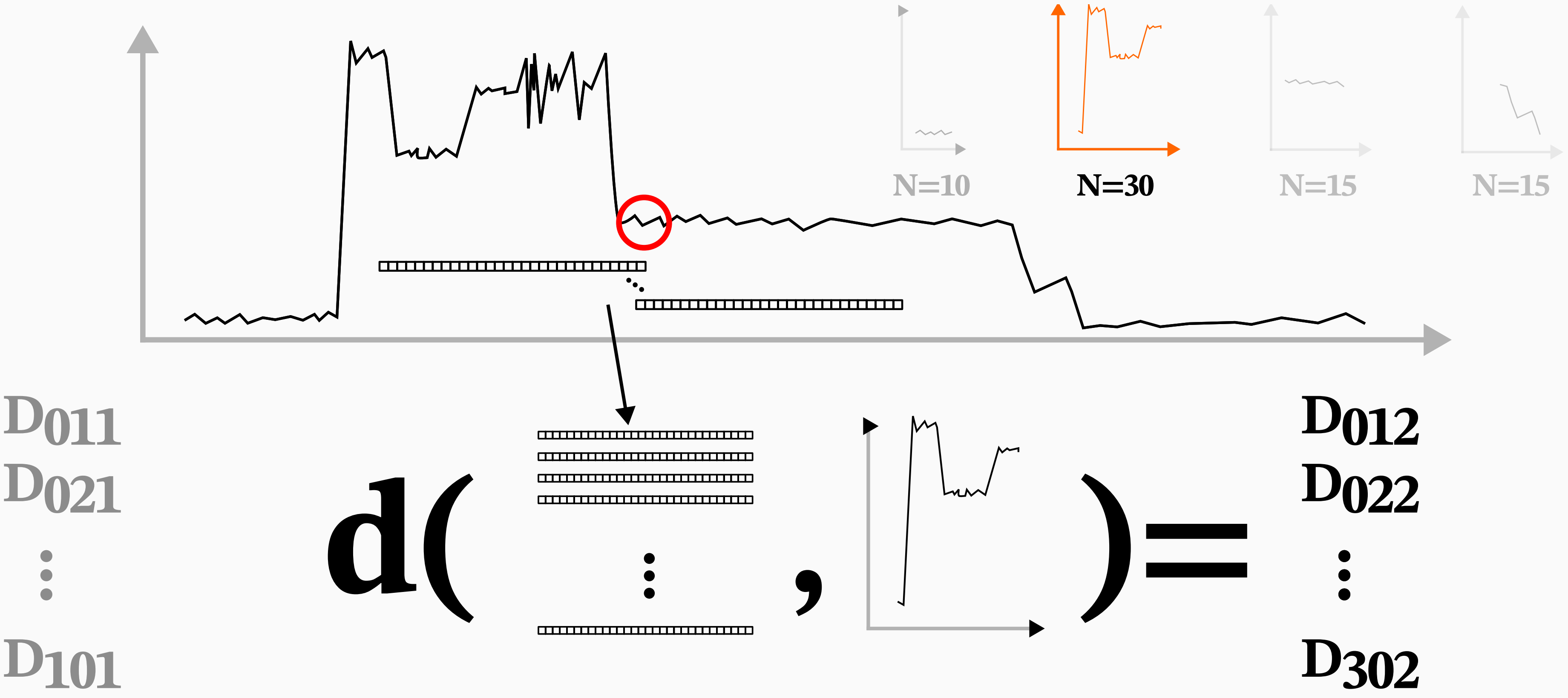
Proposed Approach



Proposed Approach



Proposed Approach



N=10

N=30

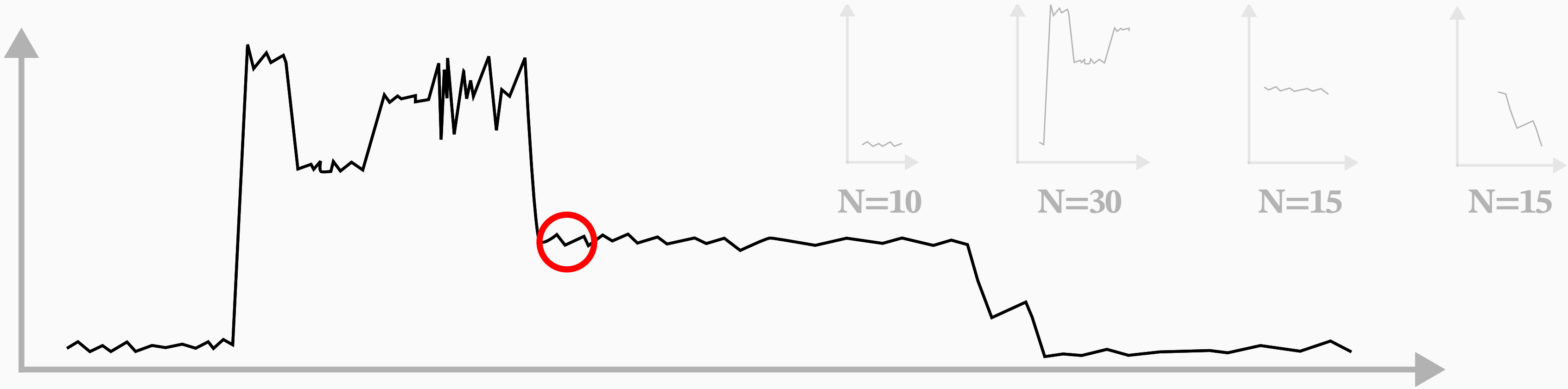
N=15

N=15

D011
D021
⋮
D101

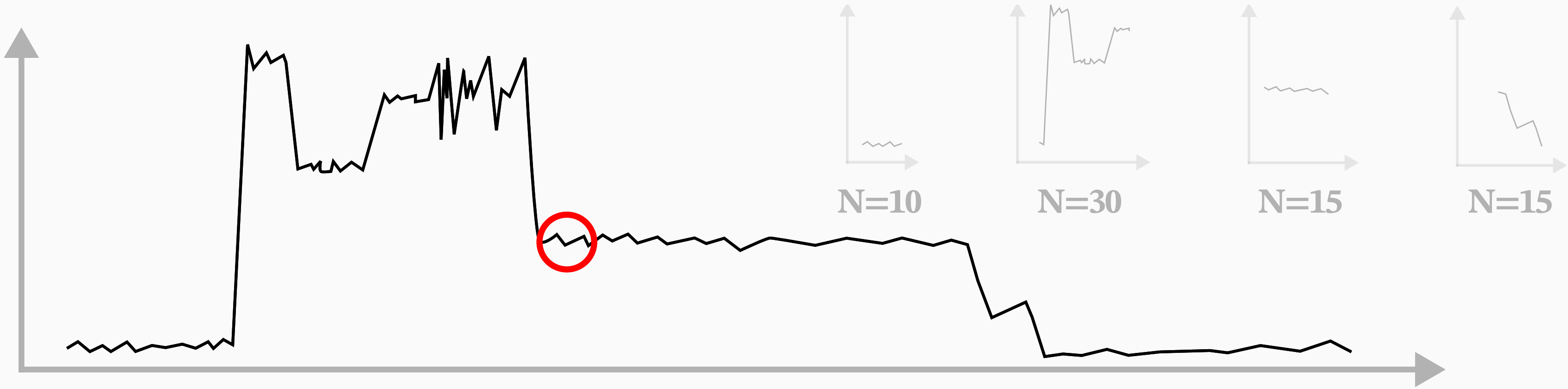
d(⋮ ,) = D012
D022
⋮
D302

Proposed Approach



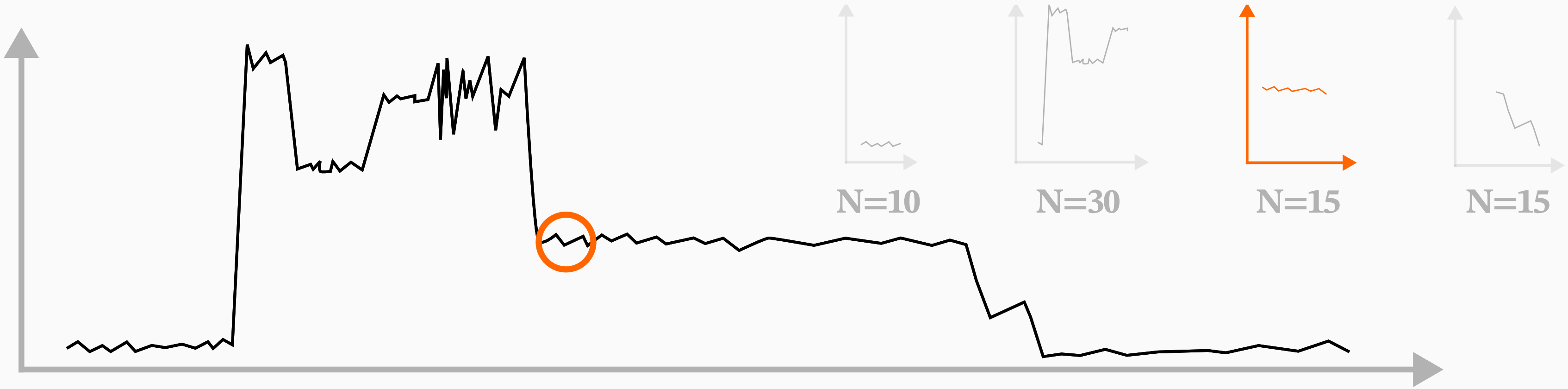
D011	D012	D013	D014
D021	D022	D023	D024
⋮	⋮	⋮	⋮
D101	D302	D153	D154

Proposed Approach



D011	D012	D013	D014
D021	D022	D023	D024
⋮	⋮	⋮	⋮
D101	D302	D153	D154
/10	**/30**	**/15**	**/15**

Proposed Approach



D011	D012	D013	D014
D021	D022	D023	D024
⋮	⋮	⋮	⋮
D101	D302	D153	D154
/10	/30	/15	/15

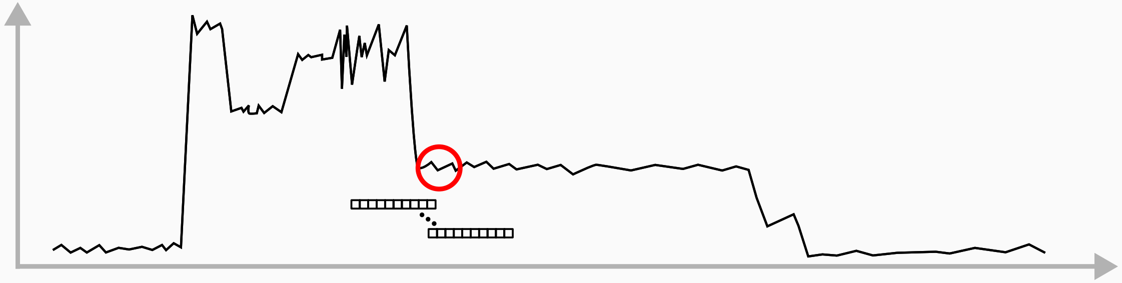
$\xrightarrow{\text{min}}$ D_{153}

Proposed Approcah

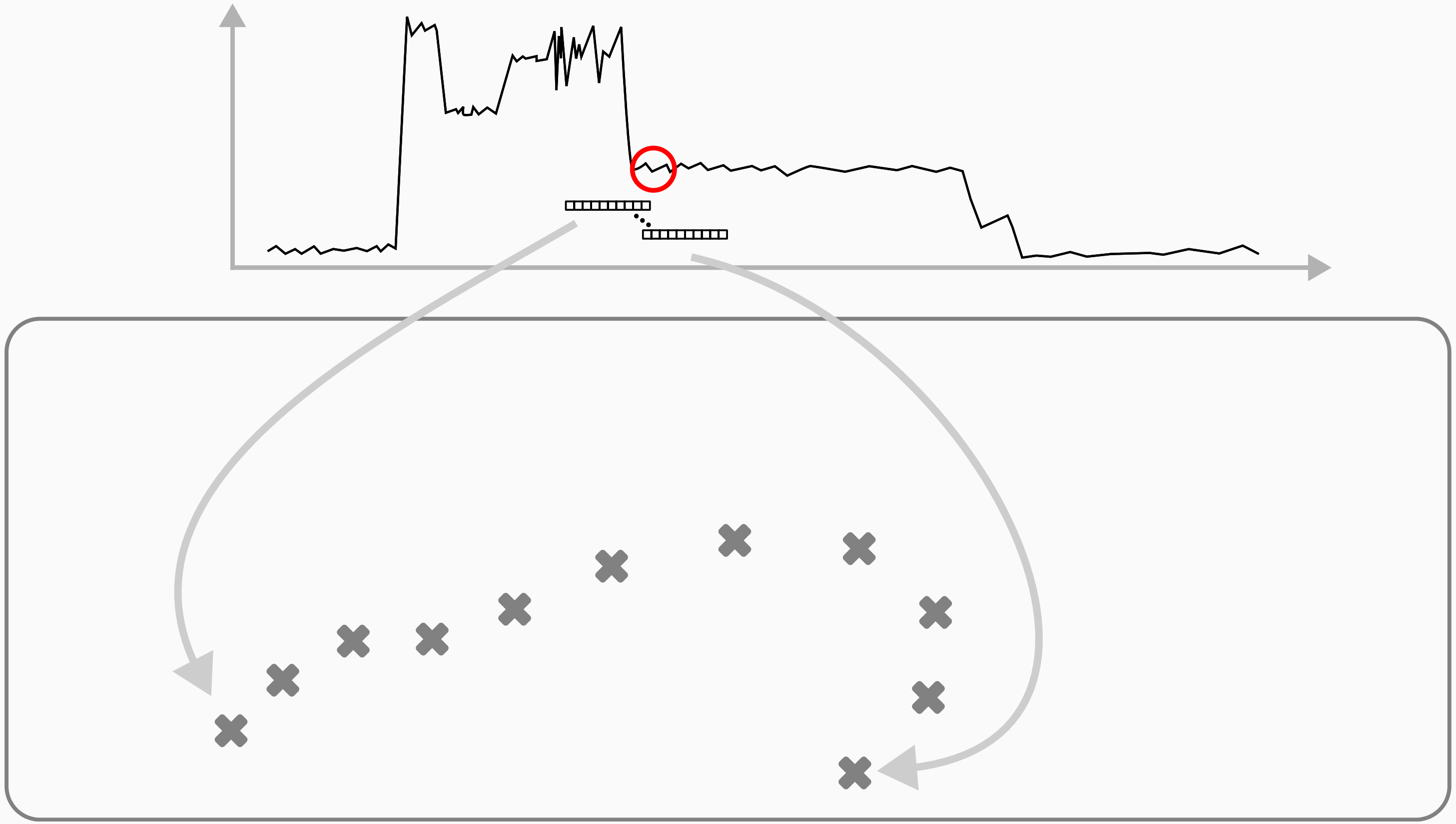
Metric: The distance between a sample and a pattern is the minimum normalized distance between the pattern and any pattern-length substring that includes the samples.

Decision: Each sample receives the label of the closest training pattern.

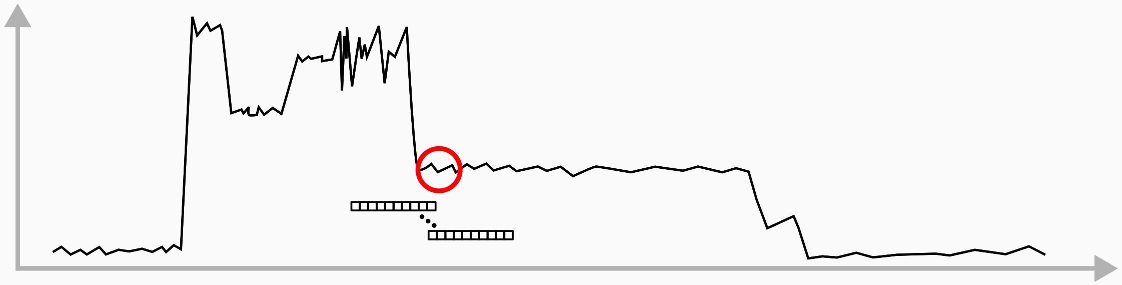
2D Interpretation

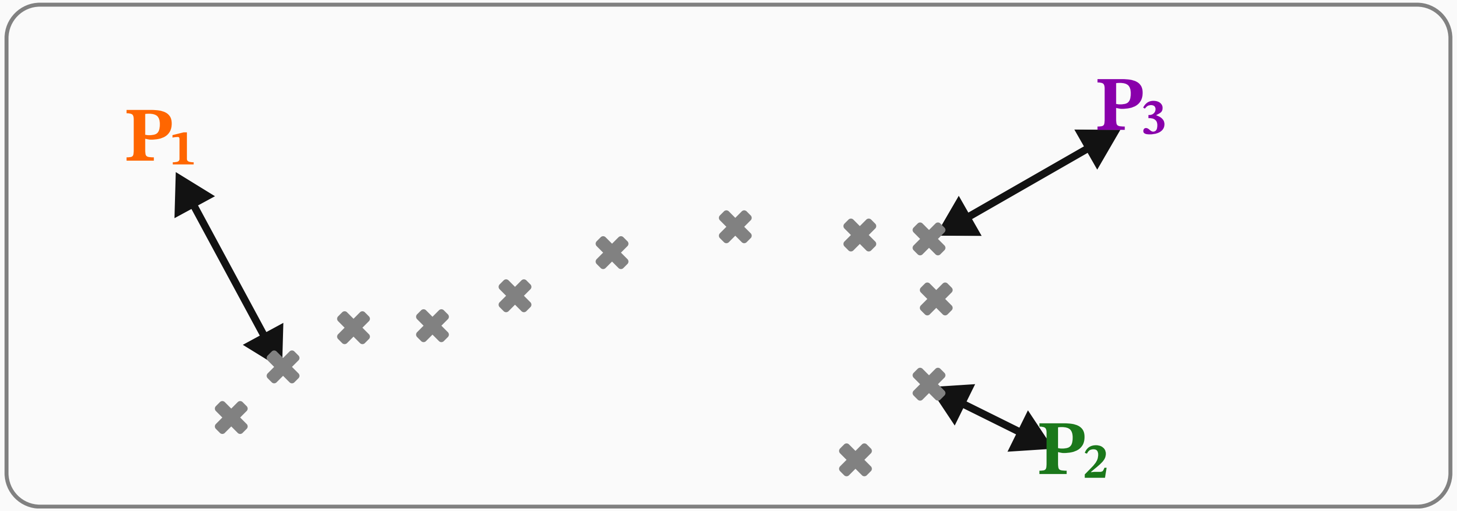


2D Interpretation

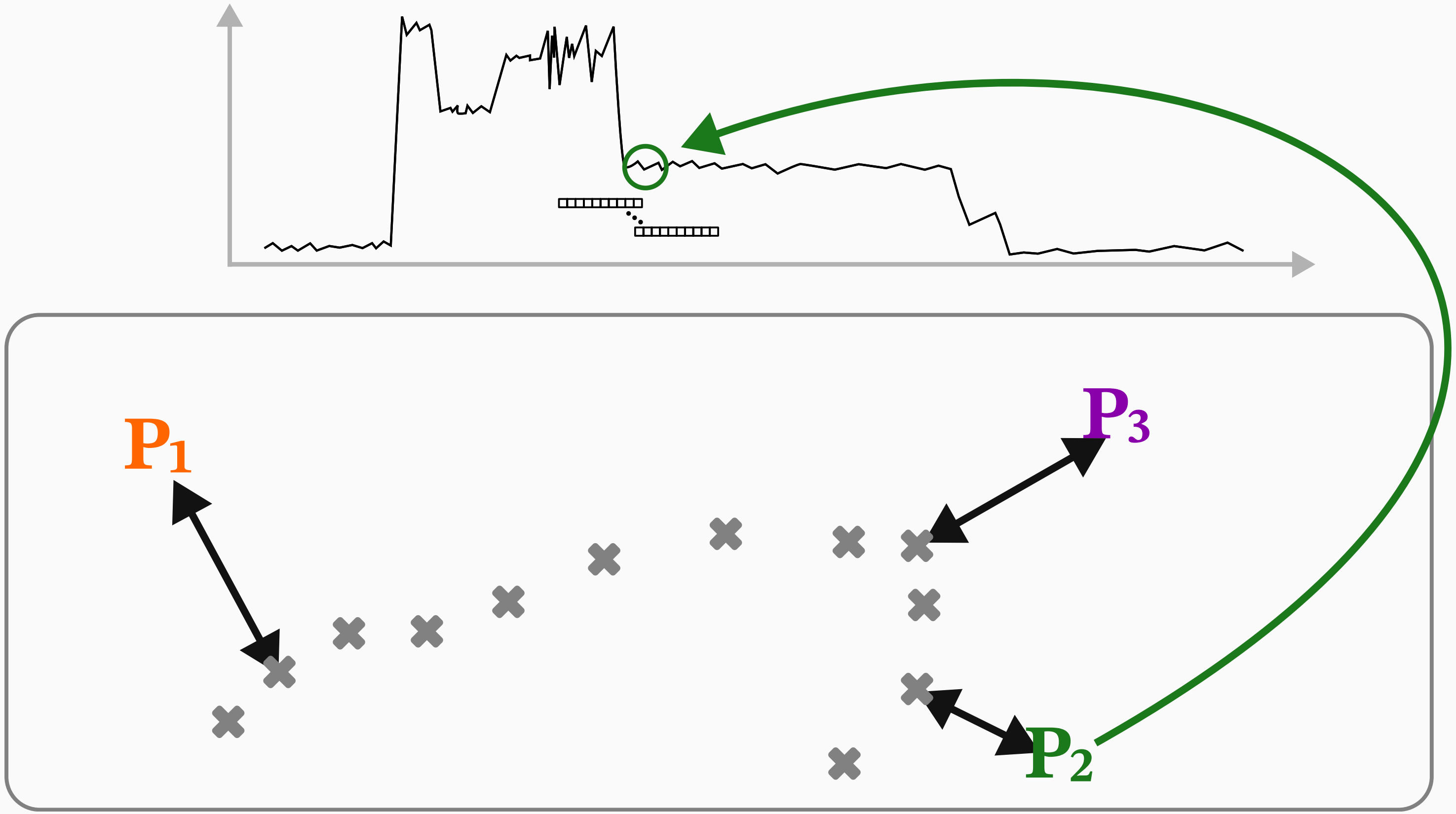


2D Interpretation

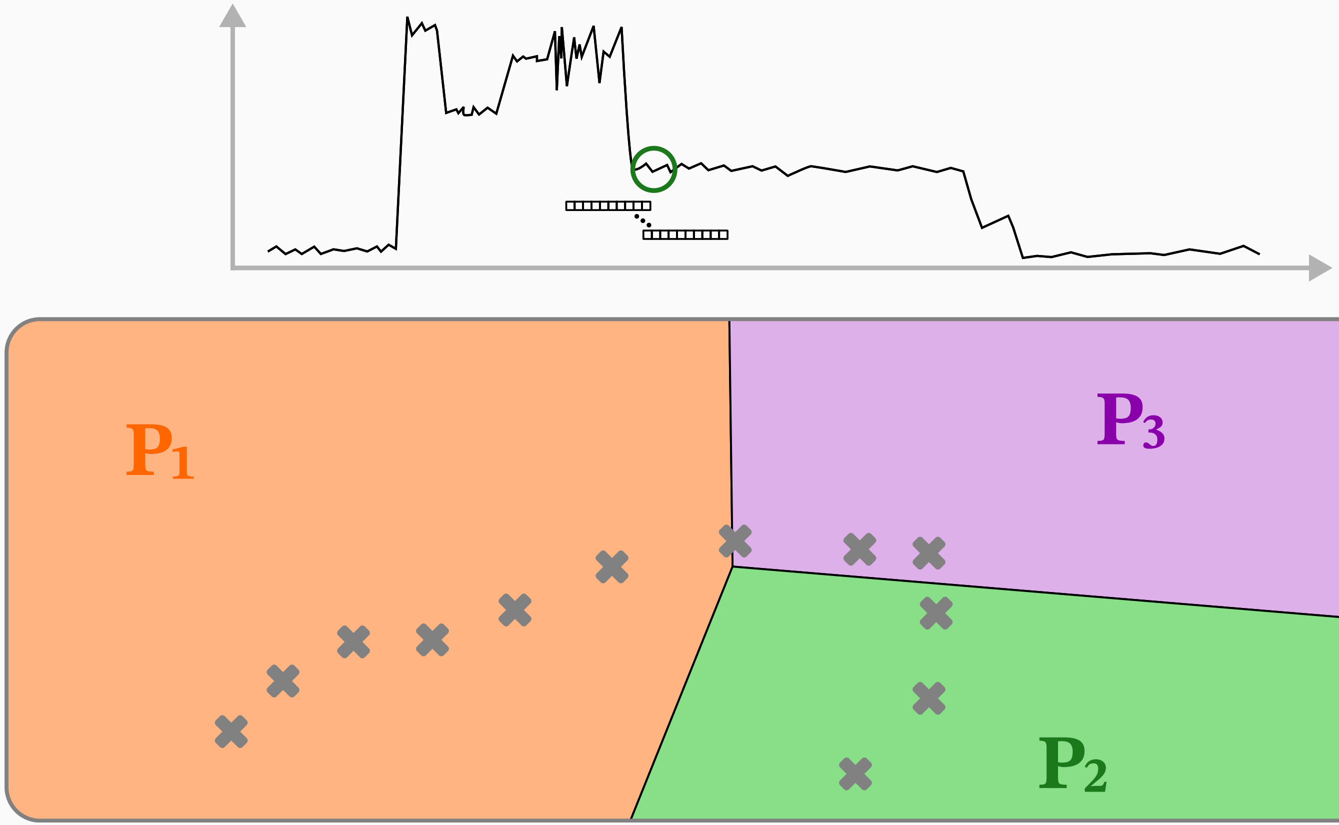




2D Interpretation



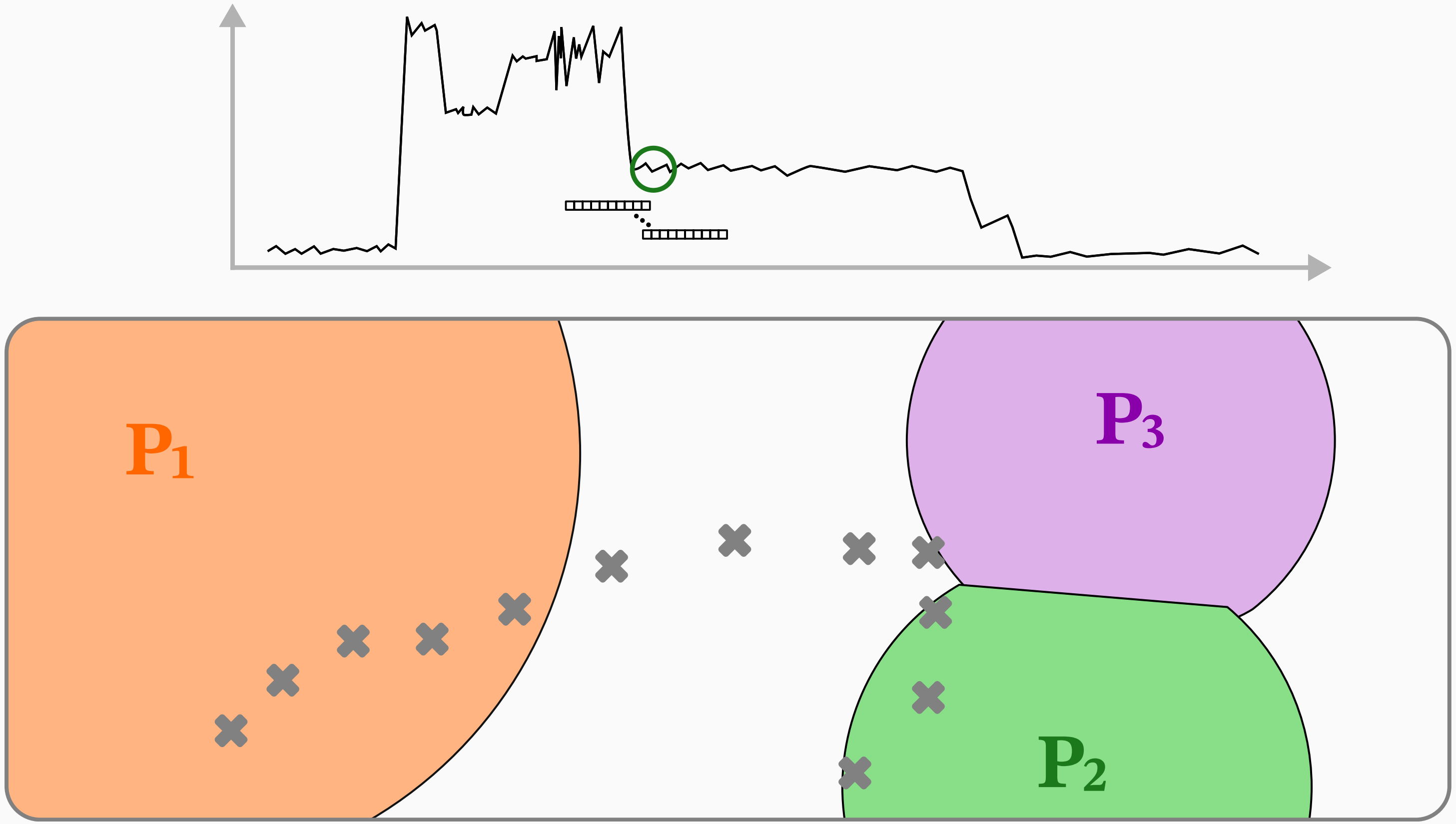
2D Interpretation



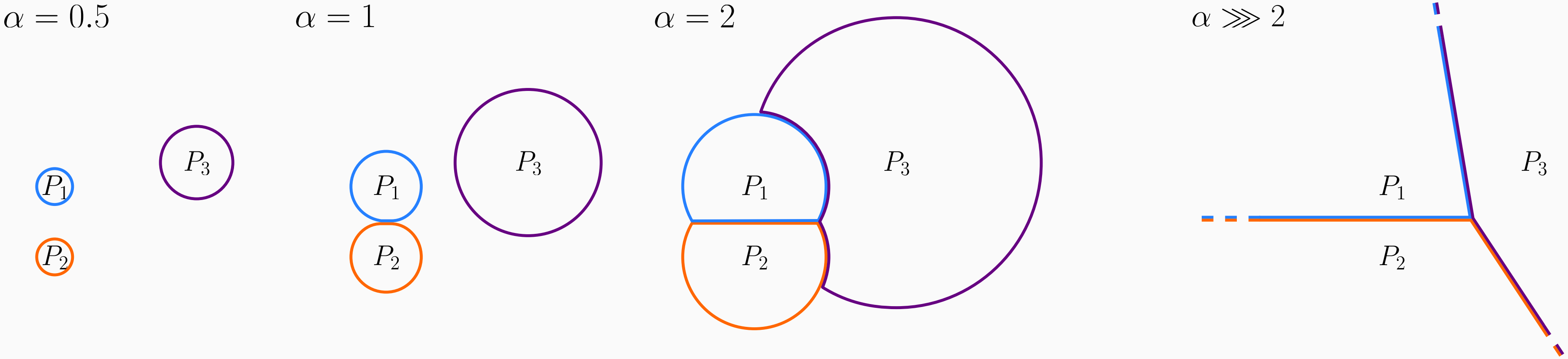
Question

Should the algorithm **always** choose a label?

2D Interpretation

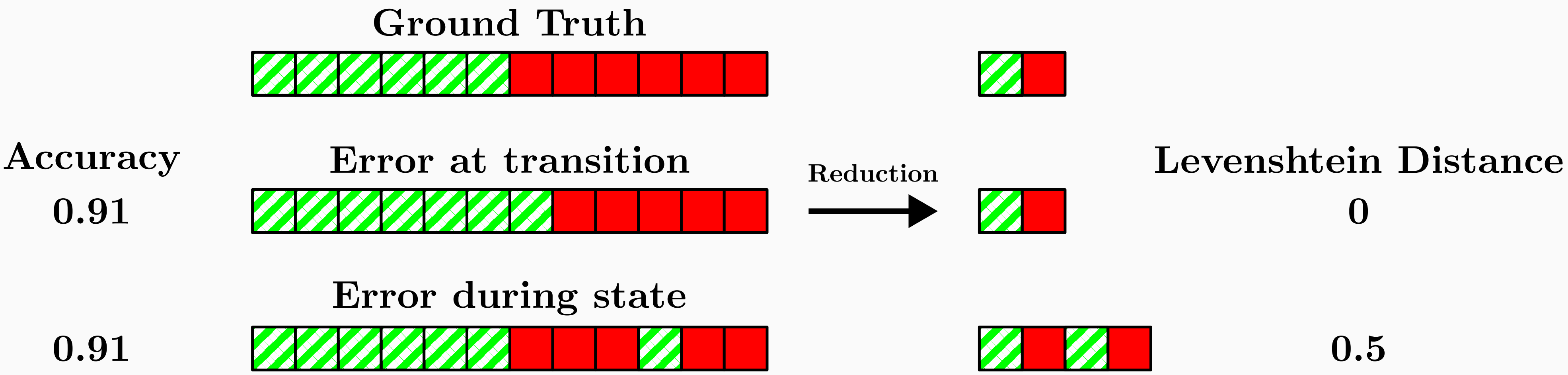


Parameter α



With α⋘2, the algorithm acquire novelty-detection capability.

Performance Metric



Ground Truth

Accuracy

0.91

Error at transition

Reduction

Levenshtein Distance

0

Error during state

0.91

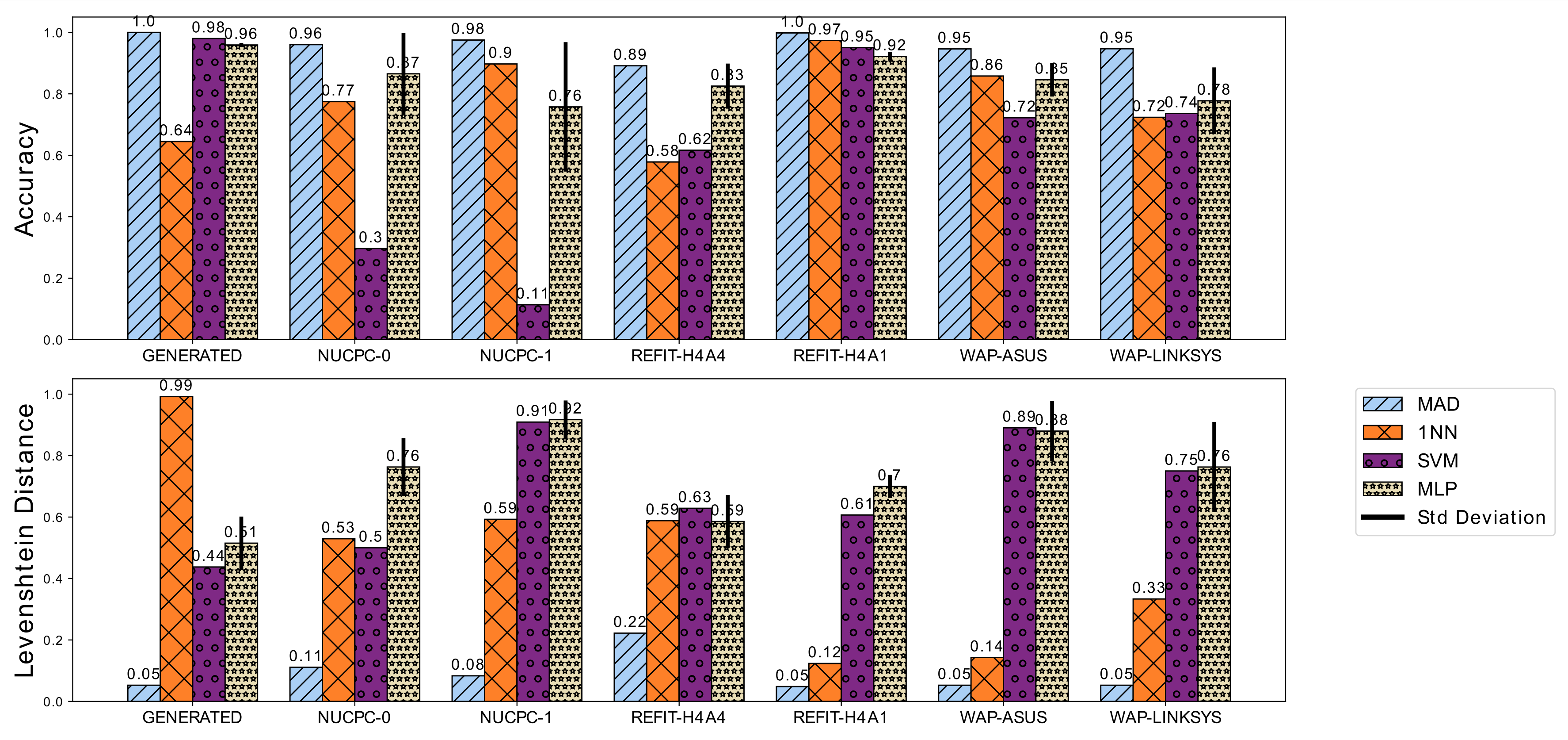
0.5

Case Study 1

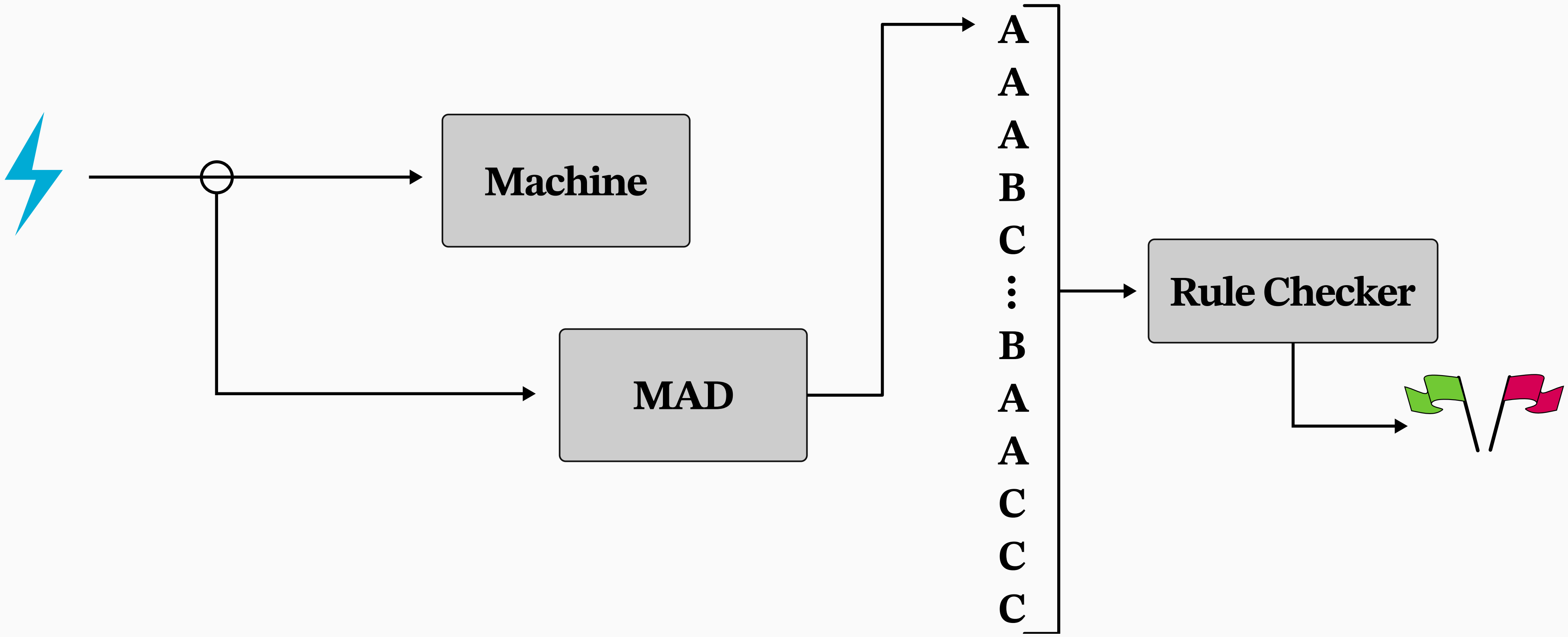
Dataset	Length	Number of Occurences
NUCPC-0	22700	11
NUCPC-1	7307	8
Generated	15540	18
WAP-ASUS	26880	18
WAP-LINKSYS	22604	18
REFIT-H4A4	5366	17
REFIT-H4A1	100000	142

Results of the case study 1

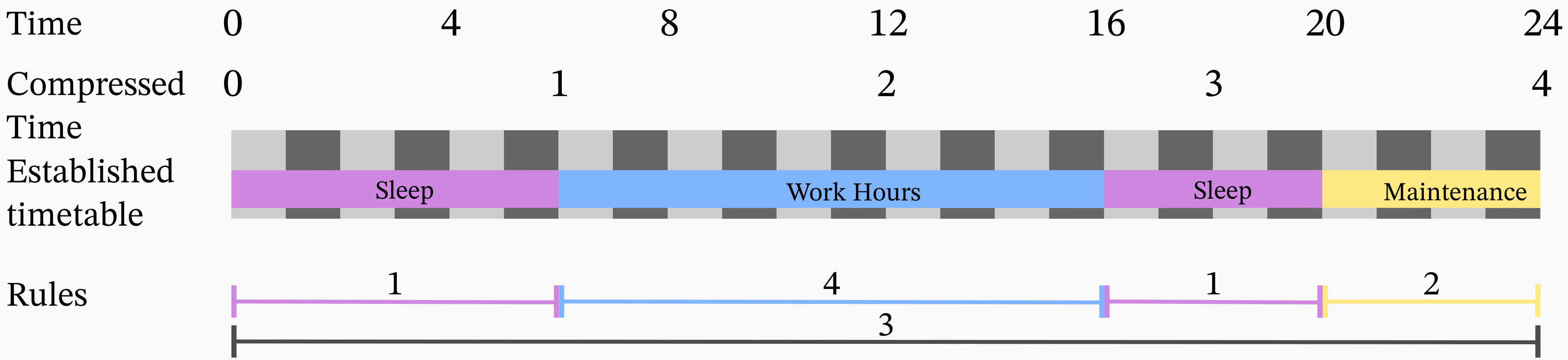
Case Study 1 - Results



Case Study 2

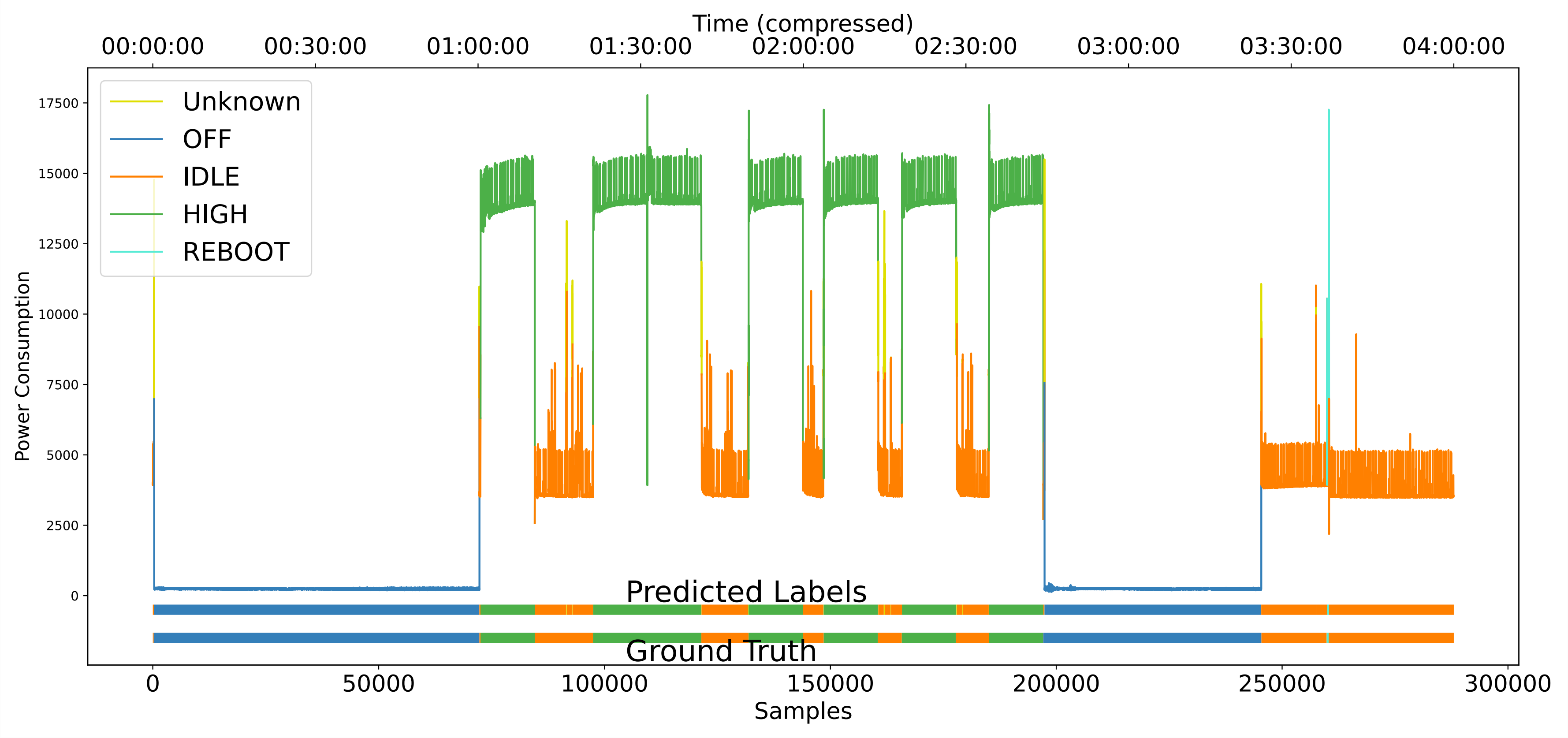


Case Study 2



Rule ID	Rule	Threat
1	“SLEEP” state only	Machine takeover, Botnet, Rogue employee
2	No “SLEEP” for more than 8m	System malfunction
3	One “REBOOT”	APT, Backdoors
4	No “HIGH” for more than 30s	Crypto mining, Ransomware, Botnet

Case Study 2


Time (compressed)
00:00:00
00:30:00
01:00:00
01:30:00
02:00:00
02:30:00
03:00:00
03:30:00
04:00:00
Power Consumption
17500
15000
12500
10000
7500
5000
2500
0
Unknown
OFF
IDLE
HIGH
REBOOT
Predicted Labels
Ground Truth
0
50000
100000
150000
200000
250000
300000
Samples

Case Study 2 - Results

Rule	**Violation Ratio**	**Micro-**F_1
Night Sleep	0.33	1.0
Work Hours	0.3	1.0
Reboot	0.48	1.0
No Long High	0.75	1.0

Results of the case study 2

Futur Work

- Automatic Training (Patterns Extraction)

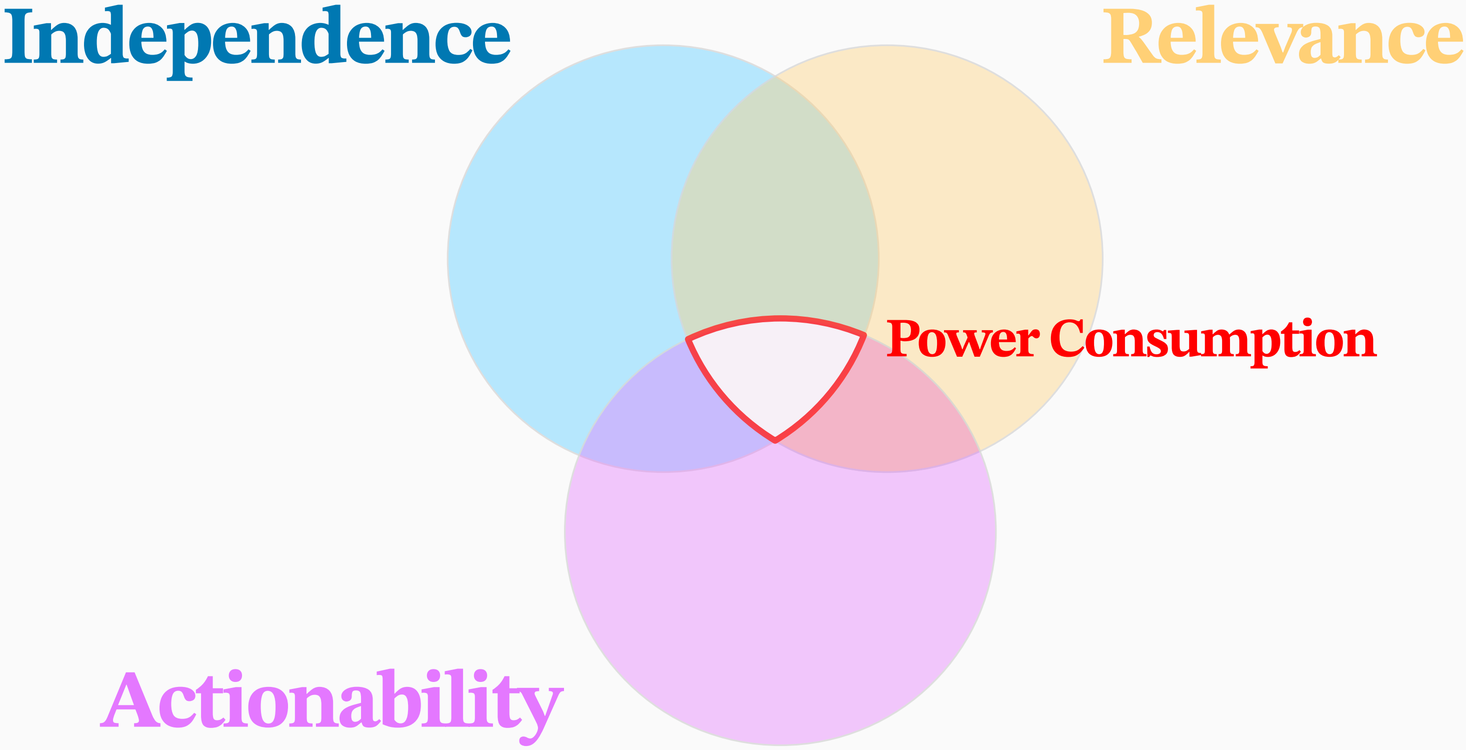
Futur Work

- Automatic Training (Patterns Extraction)
- Multivariate Support

Futur Work

- Automatic Training (Patterns Extraction)
- Multivariate Support
- More Experiments

Conclusion


Independence
Relevance
Power Consumption
Actionability

Thank you for your attention.