Bird Consortium Workshop – a bit about us

- Dr. Nir Nissim, Lecturer in IEM at BGU
- Head of the Malware Lab
- Malware Lab uniqueness:
  - Experience of over 17 years in Research & Development of Malware Detection Methods
    - Variety of platforms: PC, Cloud & VMs, Smartphones, Medical devices etc.
    - Variety of Analysis techniques: Static, Dynamic , Hybrid, Trusted
    - Variety of OSSs: Windows, Linux, Debian etc.
  - Experience of over 15 years in Research & Development of Machine Learning Methods
    - Classic ML methods
    - Advanced ML methods: Temporal Analysis, Deep Learning, Complex data types analysis
  - 12 Active Research students:
    - 4 Ph.D. , 7 M.Sc. , 1 Postdoc.
  - We have a designated malware analysis lab, allowing a full investigation of malware
  - Our research is published in Top Scientific Journals and evaluated by worldwide experts

Task 10: Multi-layer anomaly detection framework

Goal: **Improving the detection of an attacks and anomalous Behavior based on time interval mining of MTSD originated from multiple utility sources and layers exist int ICS.**

Past Methods:

- **There is no timer interval based temporal pattern (TPs) mining algorithm adjusted to ICS data characteristics**
  - **noise in data**
  - **missing values**
  - **varying frequencies**

- **There is no multiplicity of abstraction levels**

- **There is no designated ML algorithm to leverage TPs**

Our Proposed Method: TPF Algorithm = Temporal probabilistic Profiles and Time-Interval Patterns

Task 10: Multi-layer anomaly detection framework

Exploiting the raw time data from variety of ICS sensors

A. Temporal Abstraction to cope with
- **noise in data,**
- **missing values,**
- **varying frequencies**

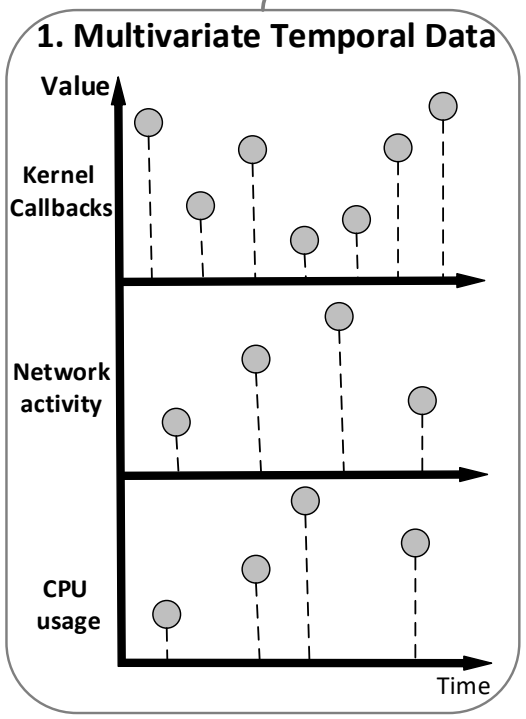
B. Combining multiple Abstraction levels to better capture behaviors

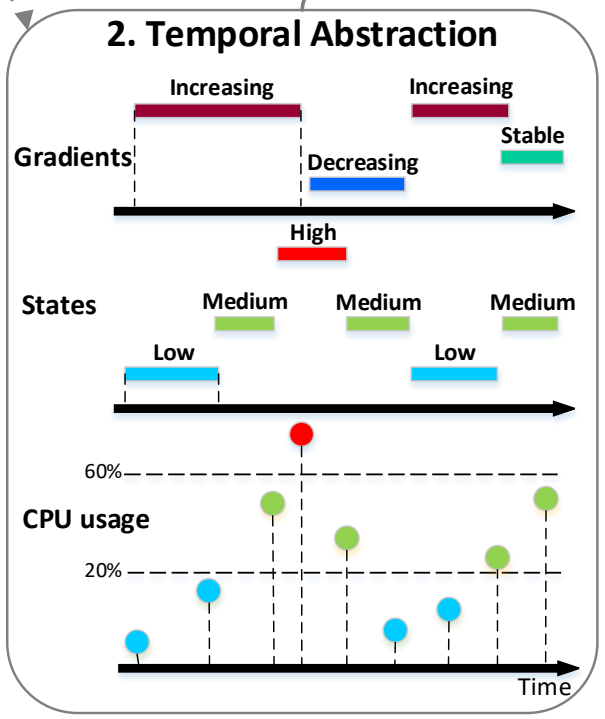
Mining time interval Patterns and Combining them from multiple layers in the ICS ecosystems

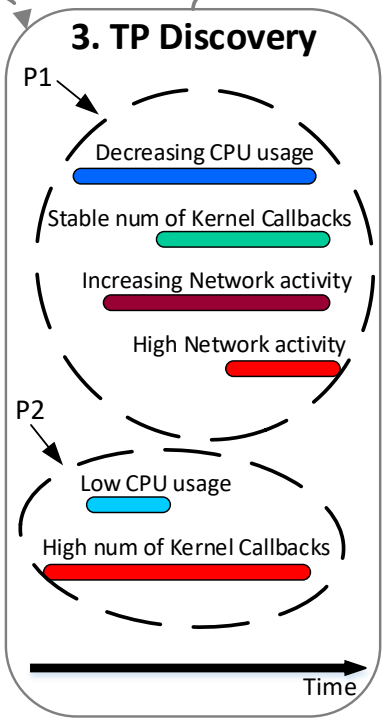
Profiling the normal ICS behavior and known attacks

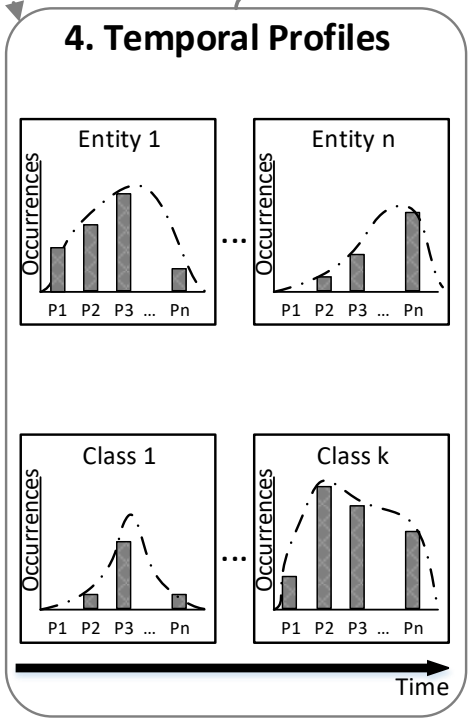
- Each class
- Each entity

Similarity calculation for attacks and Anomalous state detection









5. Similarity Scores

	Class 1	Class 2	Class 3
Entity 1	0.5	0.7	0
Entity 2	0.1	0.25	0.45
Entity 3	0	0.3	0.15
Entity 4	0.9	0.4	0
Entity 5	0.2	0.5	0.6
Entity 6	0.05	0.85	0.3

Task 12: Explainable cyber AI analytics - Temporal Explainability

Goal: Develop a temporal explainability algorithm, **clear to human operators,** via improved utilization of **multivariate time series data (MTSD) that are produced in Energy ICS**

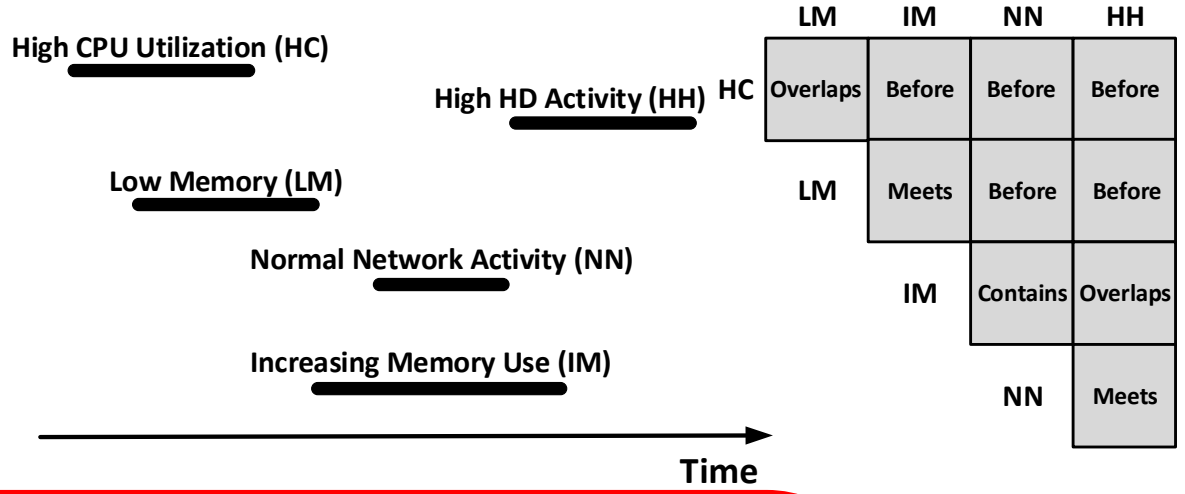
Existing Methods:

- **State of the art algorithms for MTSD lack clear temporal explainability (e.g. RNNs, DTW, Shapelets, HMM etc.)**
- **There is no human defined temporal abstraction method for ICS data**

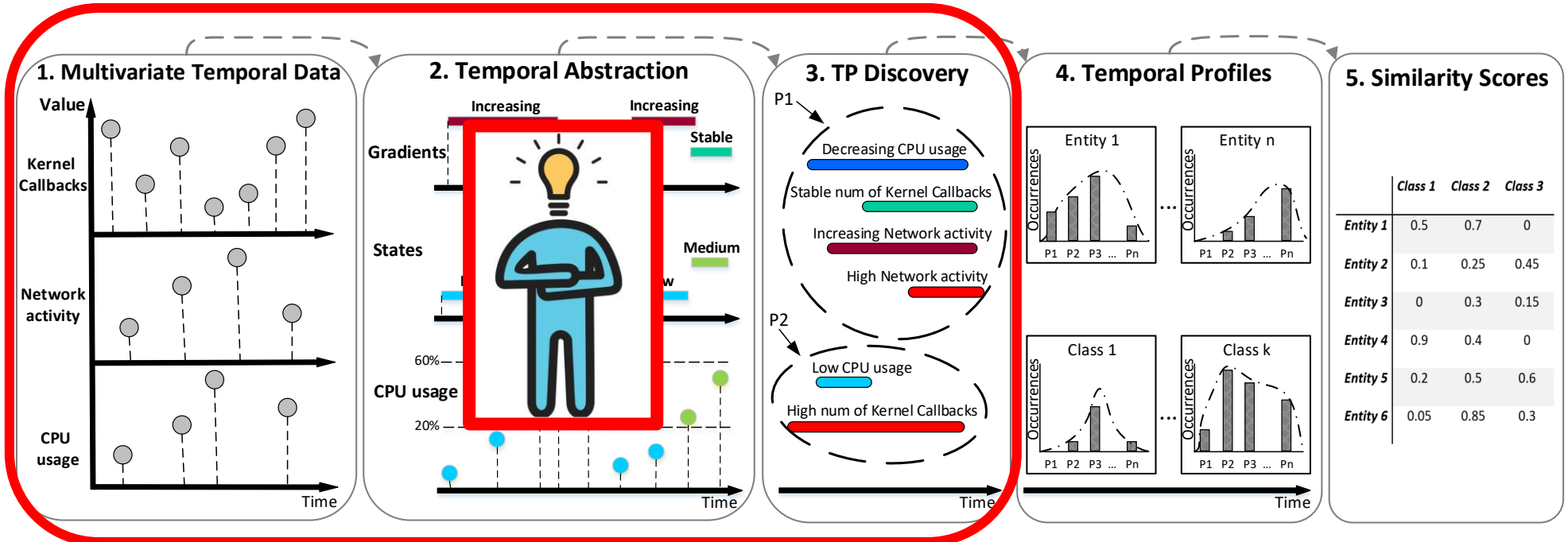
Our Proposed Method:

- The first Knowledge-based Temporal Abstraction for ICS sensors
- Mining Time-Interval Patterns
- Developing exploration tool for Temporal Explainability using the mined patterns

Task 12: Explainable cyber AI analytics - Temporal Explainability



	LM	IM	NN	HH
HC	Overlaps	Before	Before	Before
LM		Meets	Before	Before
IM			Contains	Overlaps
NN				Meets



	Class 1	Class 2	Class 3
Entity 1	0.5	0.7	0
Entity 2	0.1	0.25	0.45
Entity 3	0	0.3	0.15
Entity 4	0.9	0.4	0
Entity 5	0.2	0.5	0.6
Entity 6	0.05	0.85	0.3