This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

HyRiM

Detection of Cyber-Attacks Against SCADA

An evaluation of anomaly detection techniques

Antonios Gouglidis

Novel Approaches in Risk and Security Management for Critical Infrastructures

Vienna, 19th and 20th September 2017

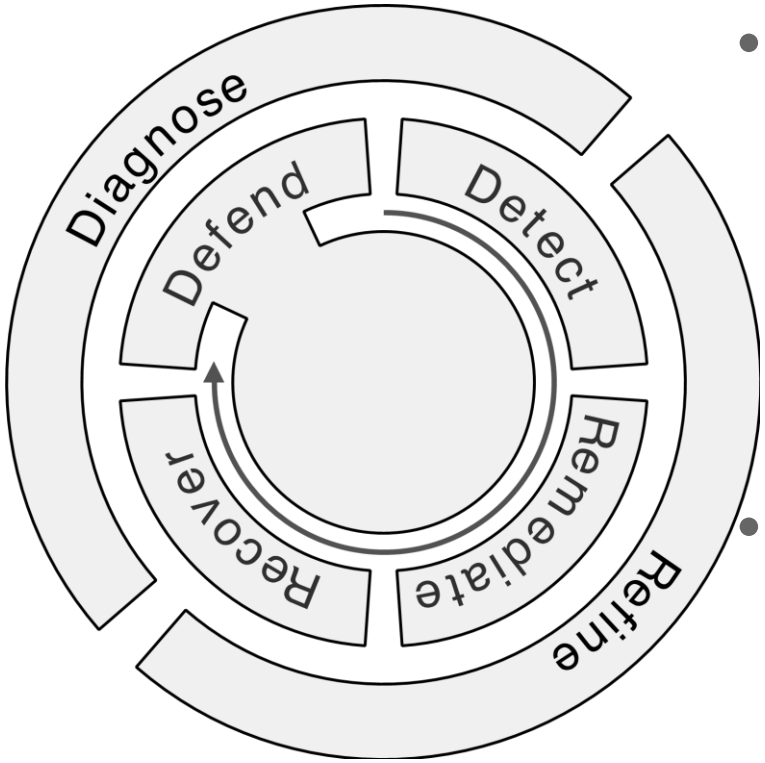
This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Contents

- Resilience reference framework
- Performance analysis of detection techniques
- Concluding remarks

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Resilience and ways of achieving it…



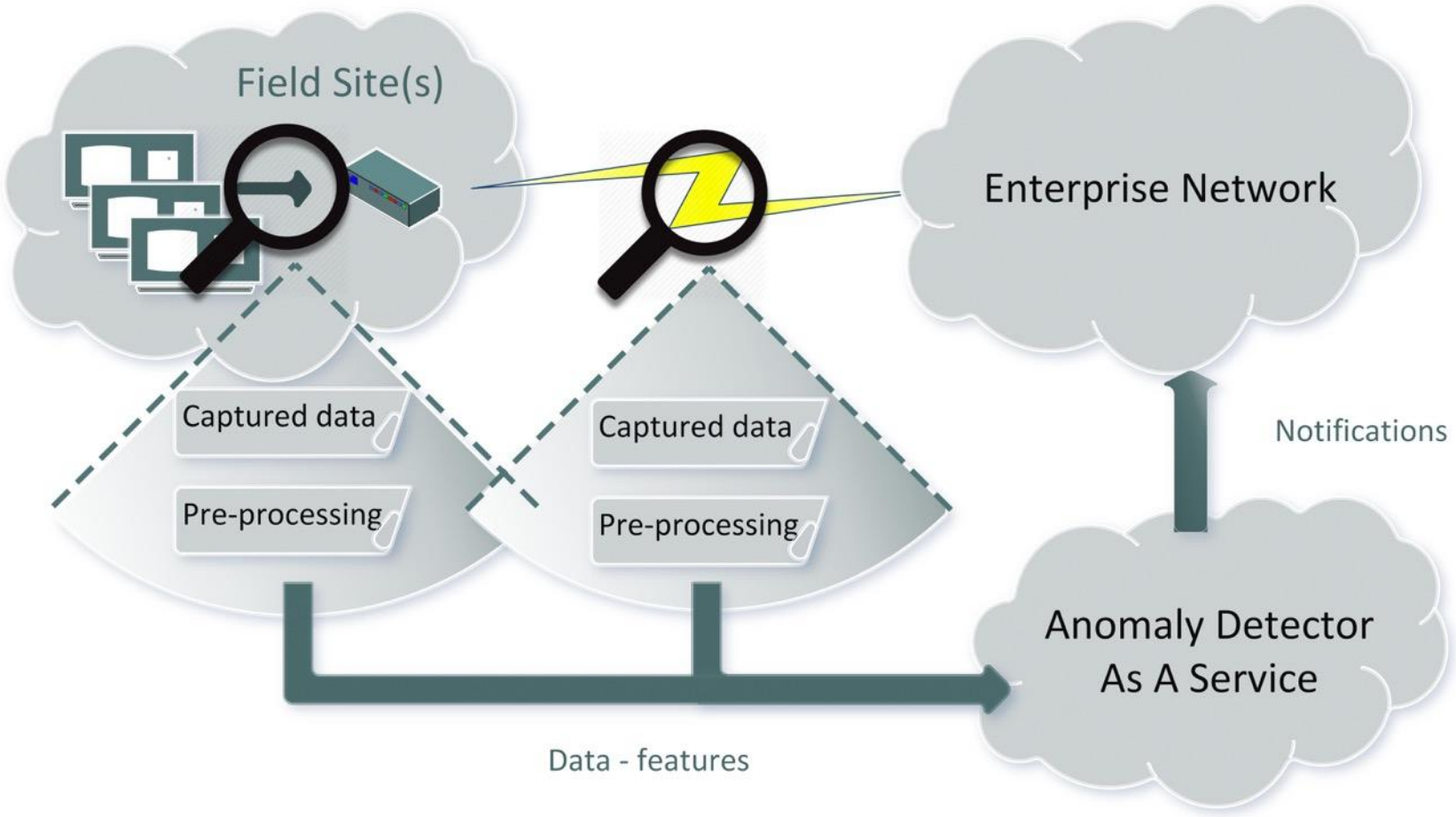
Resilience strategy

- *'… the ability of a network/system to defend against and maintain an acceptable level of service in the presence of challenges.' **
- D^2R^2+DR
  - Real-time control (internal) loop
  - Background (external) loop

* Sterbenz, James PG, et al. "Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines." Computer Networks 54.8 (2010): 1245-1265.

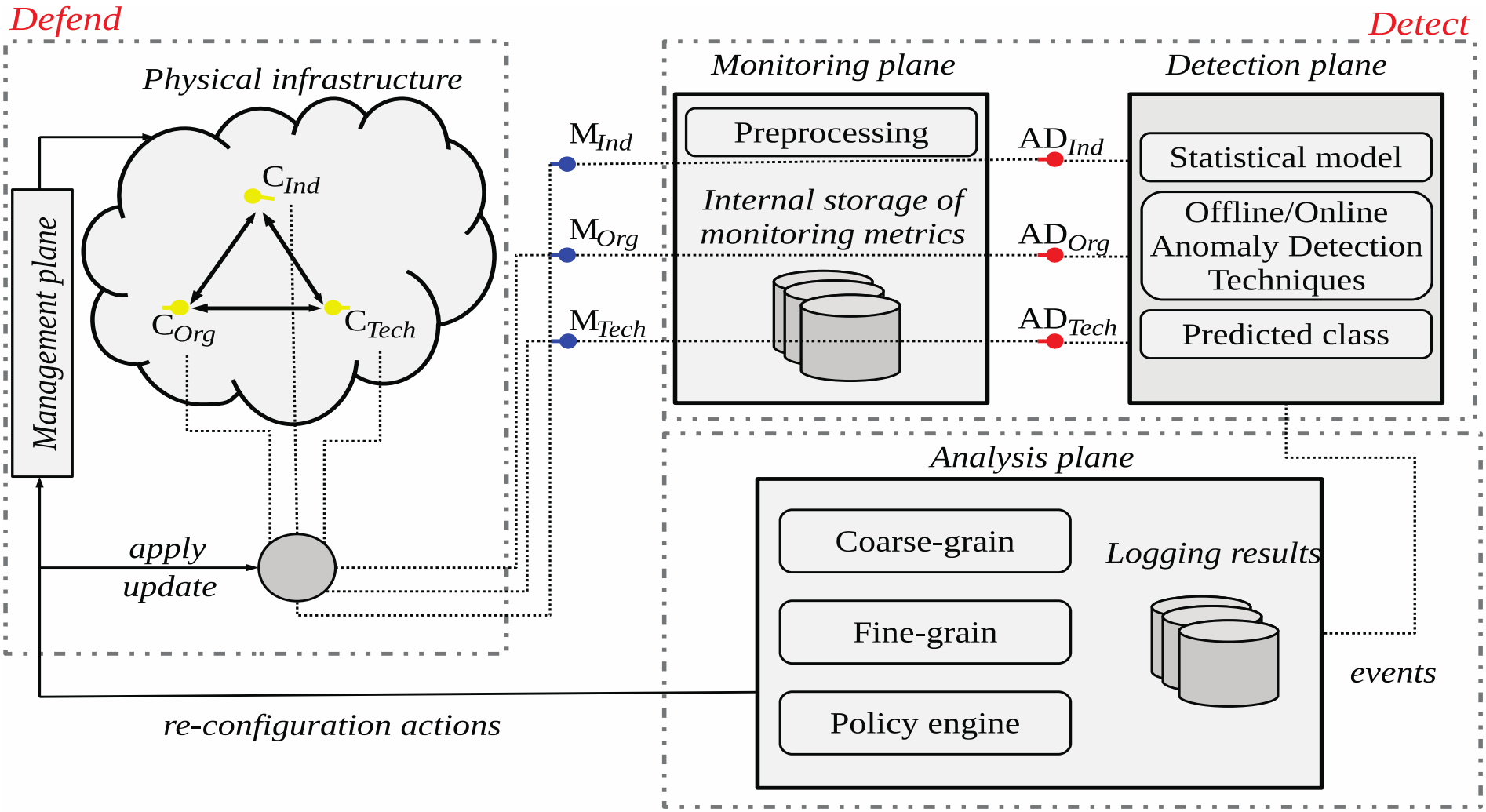
This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Overall concept



This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090

Resilience architecture



This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Dataset and techniques

HyRiM

- Dataset*
  - Simulated traffic on a gas pipeline
  - Modbus traffic including read/write command for a PLC
  - Attacks included: Response injection (naïve, complex), reconnaissance, DoS, command injection (state, parameters, function code)
- Detection techniques
  - Supervised: K-Means, Naïve Bayesian
  - Unsupervised: PCA – Singular value decomposition, GMM, Data Density

* Mississippi State University lab

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Method for evaluating techniques

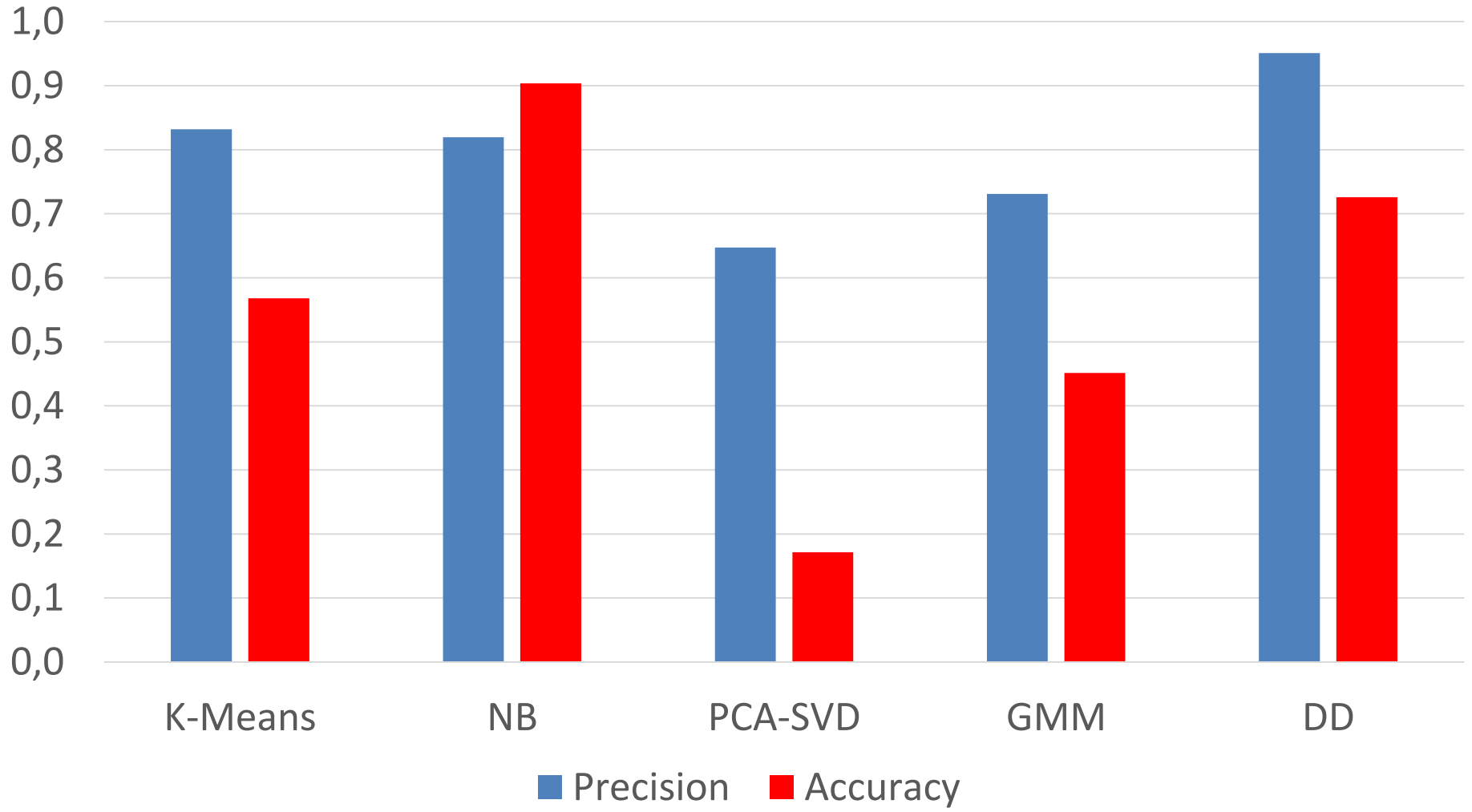
HyRiM

- Obtain most significant features from the dataset
  - Normalization of data
- Split dataset in 8 trace files
  - Combined dataset (1 file)
  - Attack trace plus normal data (7 files)
- Submit each trace file to the detector
- Compare the output against ground truth

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

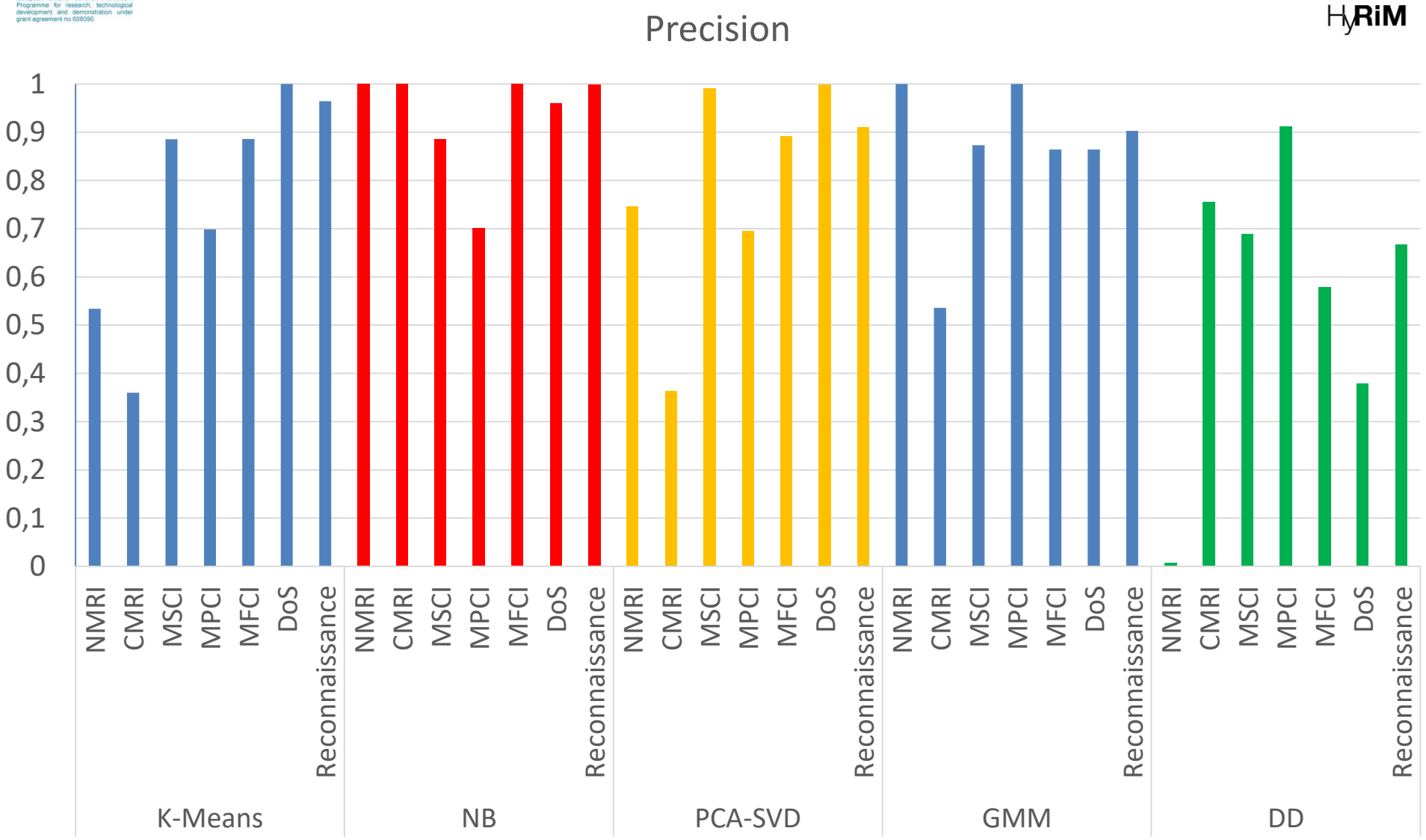
Combined dataset

Comparison of techniques



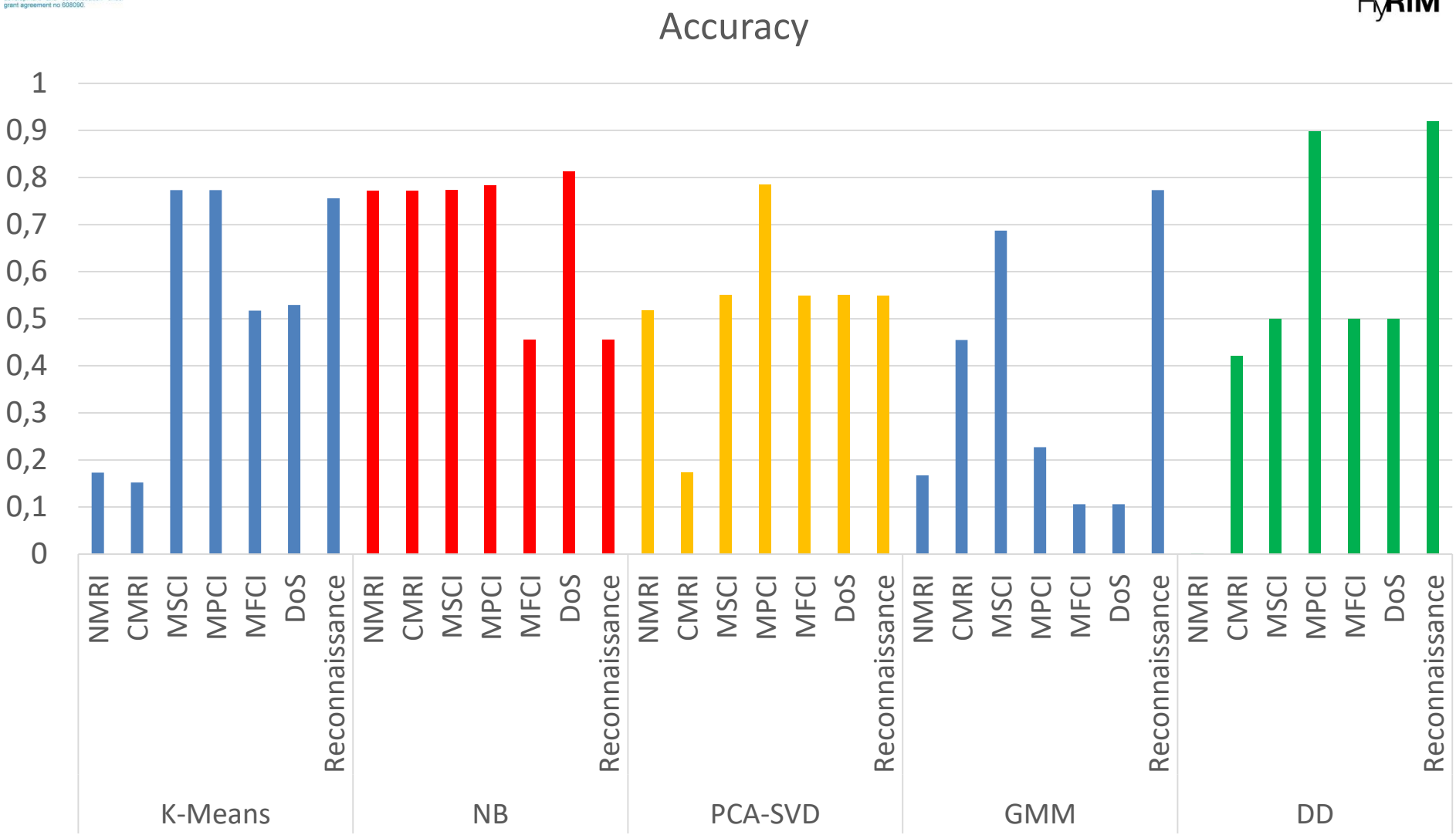
This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Precision of techniques per attack



This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Accuracy of techniques per attack



This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Concluding remarks

- Detection rate differs with respect to the
  - Type of attack
  - How different anomalous data packets are from normal traffic, intensity of the attack
- Supervised techniques perform better
- Is a dataset always available for training?

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Thank you!