Towards Automatic Critical Infrastructure Protection through Machine Learning

Lorena Cazorla, Cristina Alcaraz, and Javier Lopez

Outline

- Introduction
- Machine Learning
- Automation
- Levels of Automation
- Background
- Conclusions

Introduction

- Need to protect the Critical Infrastructures
  - Creating a preparedness and prevention status [COM(2011) 163]
  - Through detection and response mechanisms [COM(2011) 163]
- Intrusion Detection Systems (IDS)
  - Prevention solutions
  - Traditionally designed for general-purpose networks
  - Need to adapt their application for CIP
  - Need to provide them with intelligence and automatic capabilities

Introduction

- Make the IDS the first tool to provide response in emergency situations:
  - IDS will be capable of responding autonomously and intelligently in the presence of failures and attacks
  - Specially useful in the CIP environment
    - Isolated scenarios
    - Legacy equipment
    - Continuous threats
    - Critical assets to society
- Systems based on automatic methods will be capable of performing automatically, and will serve as powerful tools of *reaction,* providing methods of *prevention of cascading failures,* other than only detection of anomalies and intrusions

Machine Learning

- Machine Learning: disciplines that design and construct automatic systems capable of learning from examples
  - Prediction
  - Leveraging knowledge
- Knowledge scheme:
  - *Prior knowledge-based systems*, fed with the knowledge and experience of an expert
  - *Prior knowledge free systems* based on the knowledge extracted through an automatic (or semi-automatic) procedure of training
- Supervision scheme:
  - *Supervised learning,* where the system has knowledge about the variables learned
  - *Unsupervised learning,* where no knowledge is provided to the system when training it

Machine Learning

- Machine Learning – based IDS solutions for CIP provide them intelligence and automation
- Each one of the different techniques available provides advantageous and disadvantageous characteristics to the resulting system
- Main techniques:

Supervised techniques	Unsupervised techniques
Decision trees Rule learners Bayesian networks Artificial neural networks	Association rule learning Clustering Markov chains

Automation

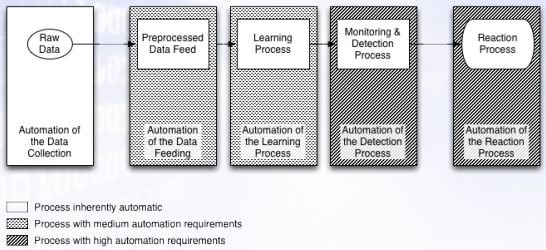
- *Automation:* introduction of automatic equipment or processes within a system, to assist or replace human operators, mostly when the tasks involved are intensive in computations or the working conditions are extreme
- In CIP, there are systems that are usually deployed in distant and isolated locations, where the automation of the tasks is of paramount importance
- Proven need of making certain processes automatic, and thus assisting the human operators in these complex tasks

Levels of Automation

- We define the five levels of automation as a methodology to determine the degree of automation of an IDS:
  - *Automation of the data collection*: collection of the raw data, capturing and recording vast amounts of data involving measurements, logs, etc. for later processing and training - Inherently automatic
  - *Automation of the data feeding*: preprocessing, normalizing and preparing the raw data to feed the inputs of the system. Difficult and costly process – Usually (semi-) manually
  - *Automation of the learning process*: steps of training, tuning and validation. The training of the system is usually automatic, but the process of tuning and validation normally needs the participation of an operator in order to set the system to a correct functioning for a context
  - *Automation of the detection process* – Automatic – but the need to tune the model in a later stage of the deployment of the system can impact negatively the performance of the system

Levels of Automation

  - *Automation of the reaction process*: **passive reaction** (raising alarms or logging off the system) and **active reaction** (react against the anomaly or the intrusion in order to avoid the system failure). – Semi-automatic and highly dependent on the presence and accuracy of the operators



Background

- Survey of the literature that review the characteristics of the systems
- Classification of the degree of automation provided, according to the previous methodology

System	Method	Prior Knowledge	Automation					Technique
			Data Collection	Preprocessing	Learning	Detection	Reaction	
[9]	Sup.	Free	Auto	No	Auto	Auto	Passive	Statistics, ML and Rules
[8]	Sup.	Required	N/A	N/A	N/A	N/A	N/A	Rules
[11]	Sup.	Free	Auto	No	Auto	Auto	Passive	Statistics
[12]	Unsup.	Mixed	Auto	No	Auto	Auto	N/A	Pattern Discovery
[13]	Sup.	Required	N/A	N/A	N/A	Auto	Passive	Rules
[14]	Sup.	Required	Auto	N/A	N/A	Auto	Passive	Rules, Statistics
[10]	Unsup.	Free	Auto	Auto	Auto	Auto	N/A	Statistics, ML and Rules
[15]	Sup.	Required	N/A	N/A	N/A	Auto	Passive	Rules, ML
[16]	N/A	Required	N/A	N/A	N/A	Auto	Passive	Specifications
[17]	Unsup.	Free	Auto	No	Auto	Auto	Passive	Clustering

Conclusions and Future Work

- We review the challenges present in the area of detection and reaction
- We support the use of Machine Learning techniques for IDS solutions in Critical Infrastructures:
  - status of readiness and prevention
  - active and intelligent reaction against threats
- We outline a methodology to evaluate the degree of automation of a given solution
  - there is a need to provide automated reaction mechanisms
- We review the literature and identify the needs of automation in the current solutions
- We want to continue exploring the advantages provided by Machine Learning, to automate the IDS solutions in CIP and build prevention systems

Thank You