Machine Learning for Power Plants Cyber Security

Alessio Vaccaro, **Beatrice Di Sero**
Unit of Computer Systems and Bioinformatics, Department of Engineering, Universita' Campus Bio-Medico di Roma, Rome, Italy
ELIS Innovation Hub, Rome, Italy
a.vaccaro@elis.org, b.disero@elis.org

Abstract

Nowadays, industrial development is in the midst of a transformation to keep up with the increasingly complexity, competitive production and economic needs. Oppositely, the integration and control required by *Industry 4.0* between IT and OT has been raising new challenges, especially in the field of *Cyber Security*. In the area of energy production, there has been attacks that led to the shutdown or even the explosion of power plants areas, e.g. *Davis-Besse* or the infected *Natanz* Iranian nuclear power plant. This has fostered the adoption of Intrusion Detection Systems (IDS) that, however, show an high false positive rate. In this context, this work aims to increase the awareness of what is happening within the plant through the development of a support tool for the plant emergency team. The proposed system was applied to the Santa Barbara ENEL power plant in Italy, showing promising results.

1 INTRODUCTION

Industrial systems, especially power plants, are now designed and operated as living organisms with different layers of information transport networks. It is clear that, while the connection of all production units leads to a better control, it also exposes the company to risks that have been neglected up to now. The problem of detecting and mitigating anomalous behaviors has been studied thoroughly, yet it remained one of the most common problems in Computer Science and industrial field. For this reason, a Proof-Of-Concept has been proposed which, by detecting maintenance and Out-of-Services (OoS), is able to indirectly reduce IDS false alarms in the Santa Barbara ENEL plant. In particular, an unsupervised model for anomaly detection in the OT behavior of the plant has been developed.

2 MATERIALS AND METHODS

We collected OT data from January 2018 to August 2018, sampled every 5 minutes, including values from 1873 probes spread inside the power plant. They consist in temperatures, pressures, activation of cooling pumps, concentration of gas in the exhaust fumes. Hence, because of the huge amount of probes, after a data preprocessing phase, a dimensional reduction stage is proposed. In this paper we propose the following three-steps solution in order to model a system for the detection of OT anomalies in the Santa Barbara ENEL power plant:

(1) Data preparation, in which low variance and low quality variables has been discarded. In this phase we have also distinguished the analog and digital series.
(2) Dimensionality Reduction Model (DRM) that shrinks data through the use of an ensemble of clustering algorithms (DBSCAN, Hierarchical Clustering and SOM) and then by using the ability to measure features' importance of XGboost. This cascade approach allowed reduce the number of variables from 1873 to 191 (10%).
(3) Anomaly Detection Model that, taking as input the prescriptions coming from the DRM, identifies anomalies deviation from forecasted time series using XGBoost. The anomaly scores of the variables have been averaged in order to obtain a plant anomaly score.

The entire solution has been developed in *R* language and in a *Data Science Virtual Machine* from *Microsoft Azure*.

3 RESULTS

The obtained plant anomaly score [0-1] (*Fig.*1) allowed to identify the *OoS* and maintenances with a recall of 99% and precision of 83%. It can be used as a filter to screen all those false positives coming from the IDS and therefore to improve security in the plant. Next steps could involve increasing model accuracy through the use of anomalies labelled by safety operators. In parallel, the integration of an anomaly detection model on network data could lead to a more robust solution.

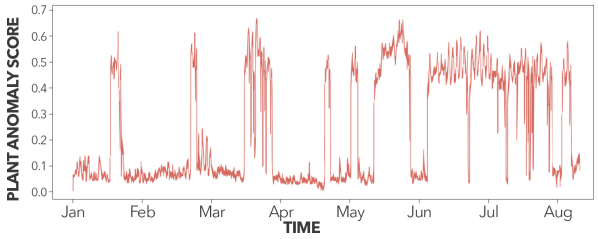

Figure 1: Plant anomaly score: values higher than a choosen tunable threshold (e.g. 0.3) refer to more abnormal behaviors.

NOTE: Due to security reasons and Non-Disclosure Agreements any source code is not publicly available.,

. .
DOI: n.d

BIBLIOGRAPHY

[1] Chandola V., Banerjee A., Kumar V., *Anomaly detection: A survey* , ACM Computing Surveys, Vol. 41 Issue 3, pages 1-58, 2009
[2] T. Chen, C. Guestrin *XGBoost: A Scalable Tree Boosting System*, 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pages 785-794, 2016
[3] Boongoen T., Iam-On N., *Cluster ensembles: A survey of approaches with recent extensions and applications*, Computer Science Review, Vol. 28, pages 1-25, 2018
[4] Toledano M, Cohen I., Ben-Simhon Y., Tadeski I., *Real-time anomaly detection system for time series at scale*, Workshop on Anomaly Detection in Finance, Vol. 71, pages 56-67, 2018