Operational Data Based Intrusion Detection System for Smart Grid

Dr. Panagiotis Sarigiannidis

University of Western Macedonia

psarigiannidis@uowm.gr

Under SPEAR Project

Authors

European Commission

OINF

Georgios Efstathopoulos

Vasilis Vasilis Argyriou

UOWM

Panagiotis Radoglou Grammatikis

Panagiotis Sarigiannidis

TRSC

Konstantinos Stamatakis

Michail K. Angelopoulos

Solon K. Athanasopoulos

SIDROCO

Antonios Sarigiannidis

Operational Data Based Intrusion Detection System for Smart Grid

Outline

Introduction

Cybersecurity in SG

SCADA

Internet of Things

Advanced Metering Infrastructure

Background

IDS Goal

IDS Architecture

IDS Types

Related Work

Signature-based IDS

Anomaly-based IDS

Operational-data based IDS

Our IDS

Architecture

Data Collection

Pre-processing and Feature Selection

Anomaly Detection

Response

Evaluation

Experimental Results

Conclusions

Cybersecurity in SG

• SG addresses multiple challenges such as centralised generation, one-way communication (only electricity transmission), limited control and manual restoration.

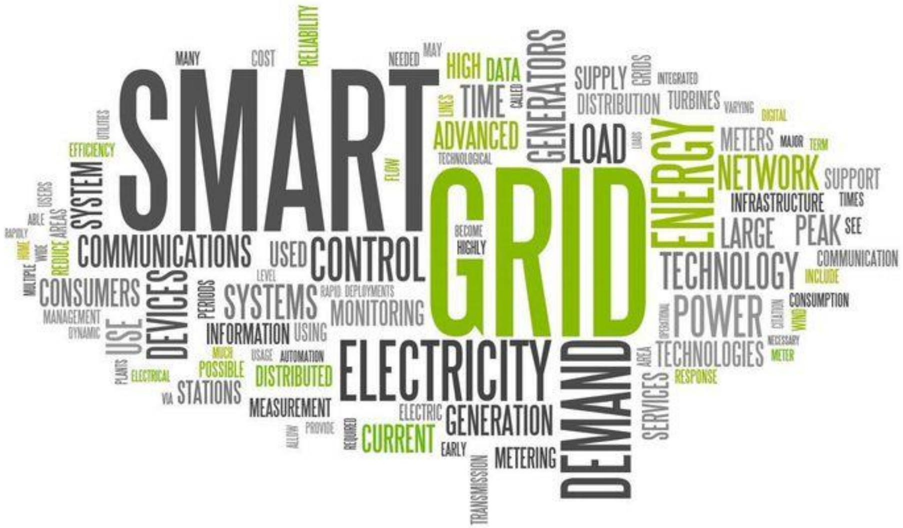
• At the same time, it introduces severe cybersecurity issues due to its interconnected and heterogeneous nature.

• CIA (Confidentiality-Integrity-Availability) : MiTM attacks, False Data Injection, DoS attacks, APTs, etc.

• Example: Cyberattack against Unkranian electric substation - Power blackout for more than 225,000people

Cybesecurity in SG

HAVE A CLOSER LOOK



SCADA Legacy System

SCADA Systems utilise legacy industrial protocols such as Modbus, Profinet, IEC 61850, IEC-104, DNP3, IEC-104 that are characterised by severe cybersecurity flaws since they do not integrate appropriate authentication and authorization mechanisms.

Internet of Things

IoT generates crucial security concerns since it is based on Internet, which is insecure by its nature. Also, it combines novel technologies such as Wire-less Sensor Networks (WSNs) that bring the corresponding cybersecurity issues, such as sinkhole, sybil and wormhole cyberattacks.

Advanced Metering Infrastructure

AMI is composed of several networks (HAN, NAN, WAN) and components (smart meters, data collectors and AMI headend that constitute an attractive target for the cyberattackers). MiTM attacks, DoS, False Data Injection (FDI), ransomware, etc. are characteristic examples.

Intrusion Detection

Main Goals

Detecting a wide range of intrusions

Detecting malicious activities that originate from external unauthorised users or malicious insiders. The modern IDS must include mechanisms to deal with zero-day attacks.

Timely intrusion detection

Possible cyberattacks and anomalies should be detected within a reasonable time.

High accuracy rate

Intrusion detection mechanisms should be characterised my a minimum number of False Negatives (FN) and False Positives (FP).

Friendly user interface

The detection results generated by IDS (alerts and warnings) should be presented appropriately to the system administrator or the security administrator.

Intrusion Detection System

Typical Architecture

Agents

Monitor, pre-process and collect useful information, such as network traffic data and operational data.

Analysis Engine

Analyses the collected information and detects cyberattack patterns or possible anomalies

Response

Informs the system/security administrator via alerts and warnings and performs appropriate countermeasures

Intrusion Detection Systems

Detection types

Signature-Based

Matches the information collected by the agents with specific attack signatures.

Anomaly-Based

Attempts to identify possible anomalies by adopting statistical analysis and AI techniques.

Specification-Based

Matches the information collected by the agents with a set determining the legitimate behaviours.

Related Work

IDS systems for SG

2015

Towards a stateful analysis framework for smart grid network intrusion detection

B. Kang et al.

Signature-based IDS for IEC 61850 substations, using the Sricata IDS.

2017

A nifty collaborative intrusion detection and prevention architecture for smart grid ecosystems

A. Patel et al.

Anomaly-based IDS for SG based on SVM, OKB and a fuzzy analyser. It consists of many HIDS and NIDS. Also, it utilises the KDD Dataset.

2019

An anomaly-based intrusion detection system for the smart grid based on cart decision tree

P. Radoglou and P. Sarigiannidis

Anomaly-based IDS based on a CART decision tree capable of detecting network attacks against AMI. It uses the CICIDS2017 dataset.

2019

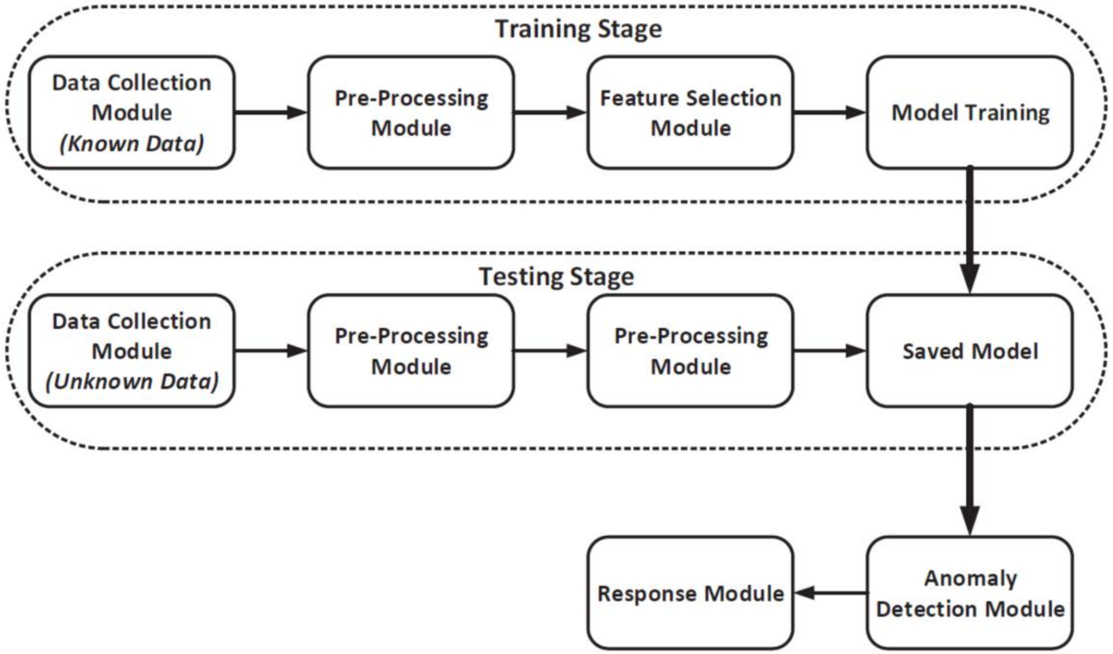
Securing the smart grid: A comprehensive compilation of intrusion detection and prevention systems

P. Radoglou and P. Sarigiannidis

A detailed survey paper about various IDS systems devoted to protecting SG applications

Architecture of the Proposed IDS

The proposed method for anomaly detection using **operational data** is based on a supervised learning framework



Data Collection Module

Responsible for collecting operational data and particularly temperature values that will be analysed for detecting possible anomalies.

Pre-Processing and Feature Selection Modules

Responsible for pre-processing the data and selecting specific features that are utilised by the Anomaly Detection Module.

Anomaly Detection Module

Responsible for implementing the anomaly detection process by considering a plethora of machine learning and deep learning methods.

Response Module

Responsible for informing the system administrator or the security administrator about the possible cyberattacks and anomalies.

Data Collection Module

CORE VALUE

Operational Data

Temperature values coming from the incoming cooling water and the generator winding

Power Plant

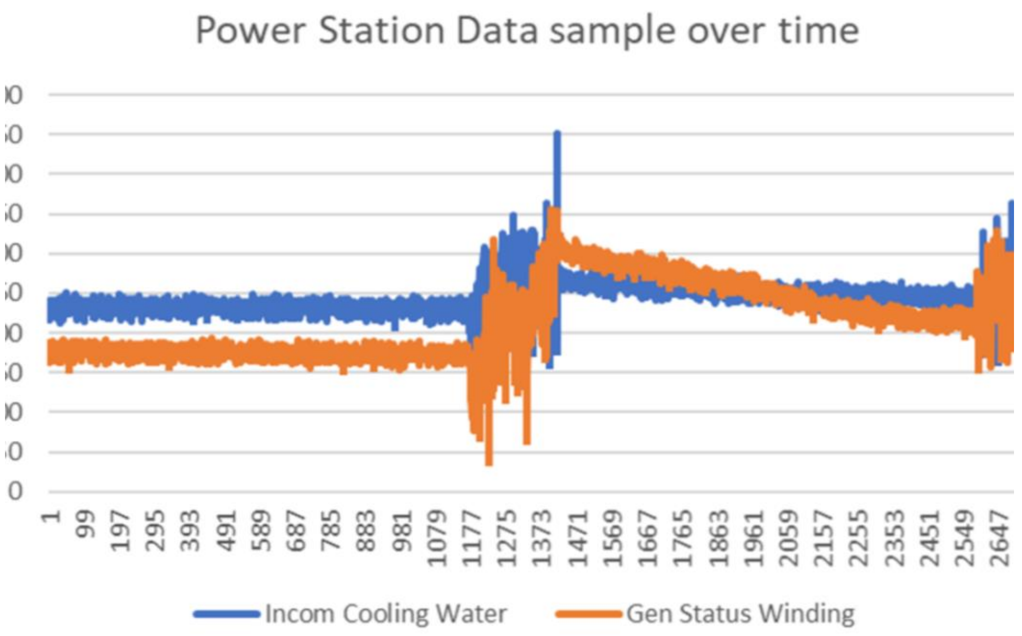
Lavrio Unit 5 that consists of PLCs & RTUs, sampled every minute.

Ground Truth

The data was annotated by the power plant engineers, indicating the anomalies and the events that triggered them.

Sample of the Dataset

The figure shows a sample of the dataset utilised.



Pre-processing and Feature Selection Modules

CORE VALUE

- Feature standardisation was considered making the values of each feature in the data have zero-mean and unit variance

- Where *f′* is the original feature vector, $\dot{f}$ is the mean of that feature vector, and σ is its standard deviation

- Let f(**m**);m = [x; y]^{T}εR denote the feature vector with *x* and *y* to represent the **water** and **generator temperature** respectively. A complex representation of these features allows better correlation between them [28-30].

- Considering a **complex vector** *z* representation for the pre-processed features we have f(z); *z = x + iy* ε C that can be also denoted using the Euler representation z = $re^{i\varphi}$ where *r = |z|= sqrt(x² + y²)* is the magnitude of z and ϕ = argz = atan2(y; x).

$$f' = \frac{f - \bar{f}}{\sigma}$$

Pre-processing and Feature Selection Modules

CORE VALUE

- The proposed **complex descriptor** does **not** affect the overall performance if the components are **independent**
- This complex representation considers and takes advantage of that improving the performance, if there is a **correlation**.
- The proposed method capturing the dependencies within the two temperature sensors exploits the complex representation.

Anomaly Detection Module

CORE VALUE

- **Several machine learning methods were considered**

  One Class-SVM, Isolation Forest, Angle-Base Outlier Detection (ABOD), Stochastic Outlier Selection (SOS), Principal Component Analysis (PCA), Deep fully connected AutoEncoder

- The proposed complex feature vectors over a **sliding time window** were used as input for all these approaches.

- The input is a time-series and the training is performed only with normal data.

- For the proposed machine learning approaches the dataset was split to training and testing subsets and simple k-fold Cross Validation (CV) was also used.

Anomaly Detection Module

Details about the anomaly detection methods

PCA and One Class SVM

Linear kernels were used

SOS

Euclidean distance was used to obtain the dissimilarity matrix and T-distributed Stochastic Neighbor Embedding (tSNE) to calculate the affinity matrix

ABOD

The angle based outlier factor was defined as the variance over the angles between the feature vectors weighted by their distance

Isolation Forest

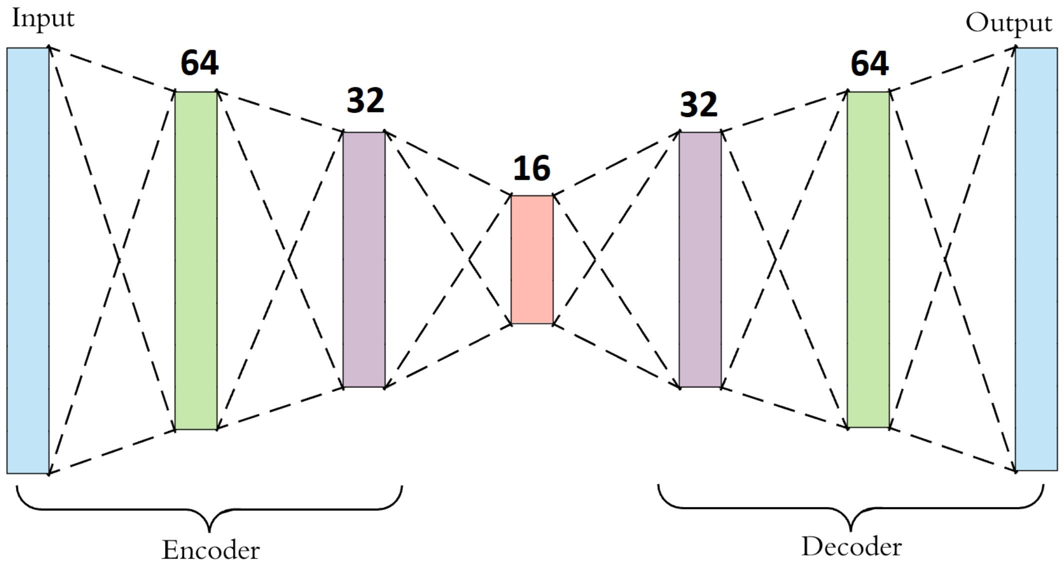
The average path length between the root and each leaf (feature point) was used with the abnormal data points to be the ones with relatively short average path.

Anomaly Detection Module

Details about the anomaly detection methods

Deep fully connected AutoEncoder

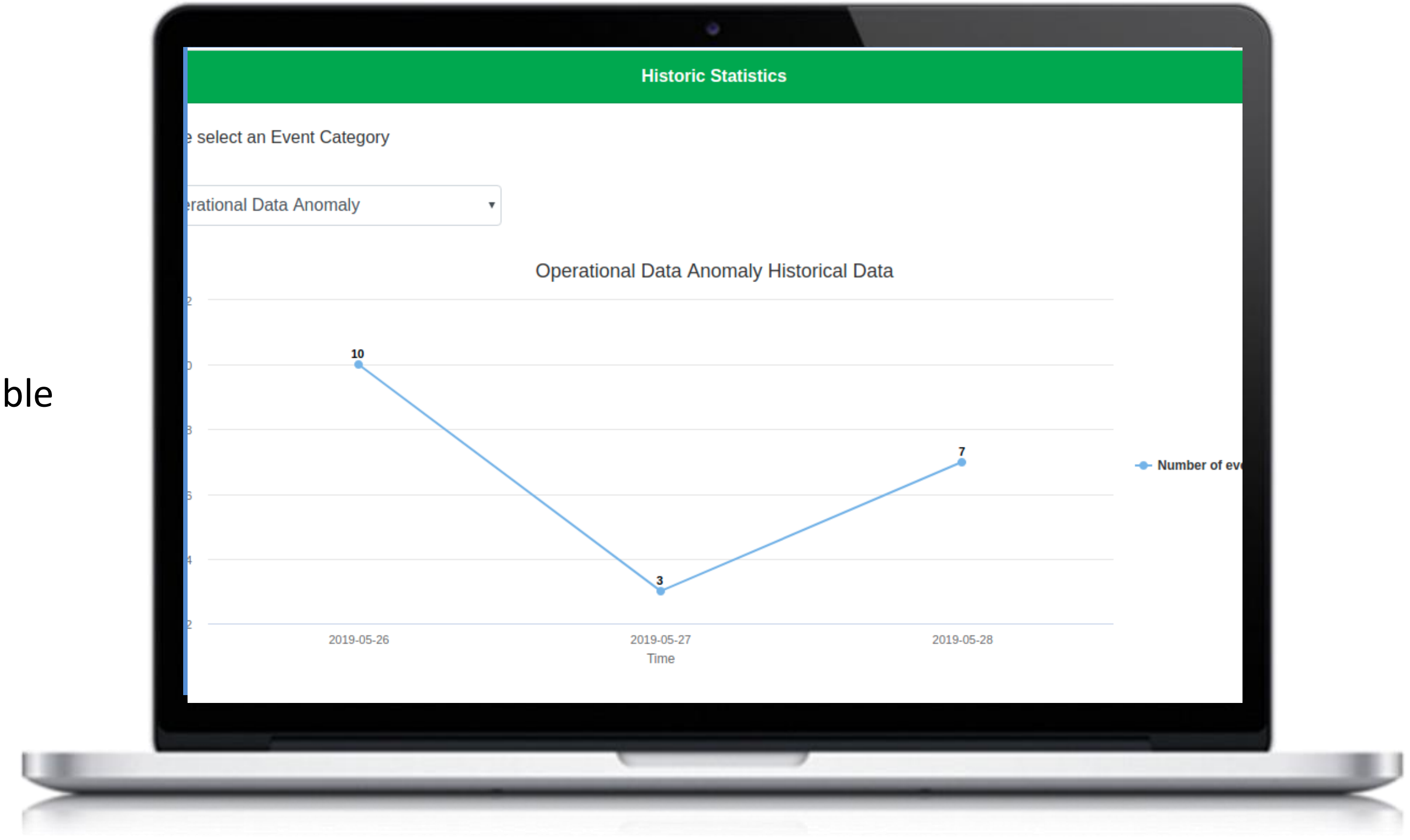
The following autoencoder was designed with six fully connected layers as it is shown below



Response Module

Core Value

- Receives the output of the Anomaly Detection Module and undertakes to inform the security operator or the security administrator about the possible cyberattacks by extracting the appropriate security events.
- A web-based platform was developed for this purpose, providing also related statistics.



Evaluation Analysis

All the methods and features were tested for three different sliding time windows of 20, 30 and 50 minutes

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

$$F1 = \frac{2 \times Precision \times Recall}{Precision + Recall}$$

$$AUC = \int_a^b TPR\left(FPR^{-1}(X)\right) dx = P(X_1 > X_0)$$

Where X_1 is the score for a positive instance and X_0 is the score for a negative instance.

The evaluation results for time window 20.

Win20	Accuracy Norm	Accuracy Comp	F1s Norm	F1s Comp	AUC Norm	AUC Comp
PCA	0.554	**0.975**	0.608	**0.975**	0.710	**0.967**
OneClass	0.595	**0.893**	0.648	**0.869**	**0.735**	0.657
Iforest	0.575	**0.875**	0.628	**0.884**	0.729	**0.851**
ABOD	0.521	**0.688**	0.584	**0.718**	**0.586**	0.547
SOS	0.951	**0.975**	0.947	**0.975**	0.842	**0.967**
Auto	0.560	**0.619**	0.614	**0.669**	0.718	**0.763**

Evaluation Analysis

All the methods and features were tested for three different sliding time windows of 20, 30 and 50 minutes

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

$$F1 = \frac{2 \times Precision \times Recall}{Precision + Recall}$$

$$AUC = \int_a^b TPR\left(FPR^{-1}(X)\right) dx = P(X_1 > X_0)$$

Where X_1 is the score for a positive instance and X_0 is the score for a negative instance.

The evaluation results for time window 30.

Win30	Accuracy Norm	Comp	F1s Norm	Comp	AUC Norm	Comp
PCA	0.527	**0.597**	0.585	**0.652**	0.687	**0.736**
OneClass	0.553	**0.905**	0.611	**0.885**	**0.702**	0.681
Iforest	0.548	**0.791**	0.606	**0.819**	0.697	**0.864**
ABOD	0.530	**0.799**	0.591	**0.791**	**0.642**	0.568
SOS	0.976	**0.989**	0.976	**0.990**	0.921	**0.994**
Auto	0.538	**0.603**	0.596	**0.658**	0.693	**0.740**

Evaluation Analysis

All the methods and features were tested for three different sliding time windows of 20, 30 and 50 minutes

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

$$F1 = \frac{2 \times Precision \times Recall}{Precision + Recall}$$

$$AUC = \int_a^b TPR\left(FPR^{-1}(X)\right) dx = P(X_1 > X_0)$$

Where X_1 is the score for a positive instance and X_0 is the score for a negative instance.

The evaluation results for time window 50.

Win50	Accuracy Norm	Accuracy Comp	F1s Norm	F1s Comp	AUC Norm	AUC Comp
PCA	0.459	**0.550**	0.523	**0.614**	0.627	**0.684**
OneClass	0.516	**0.913**	0.581	**0.909**	0.659	**0.773**
Iforest	0.480	**0.617**	0.545	**0.675**	0.637	**0.757**
ABOD	0.574	**0.739**	0.640	**0.765**	**0.603**	0.598
SOS	0.989	**0.995**	0.989	**0.995**	0.960	**0.997**
Auto	0.466	**0.553**	0.530	**0.617**	0.628	**0.684**

Evaluation Analysis

All the methods and features were tested for three different sliding time windows of 20, 30 and 50 minutes

- The overall performance of the machine learning and deep learning methods with and without the proposed complex feature representation and the affect of the size of the sliding time window.
- The overall average accuracy was increased by 29%, the F1 score by 22% and the AUC by 8%.

Conclusions

1. A novel approach for cyberattacks detection on SGs has been introduced based on anomaly detection over operational data.

2. A complex representation of the input data was suggested aiming to exploit the correlation in between the data values improving the overall accuracy of anomaly detection.

3. Several machine learning and deep learning methods were used in a comparative study demonstrating the improved performance of the proposed methodology.

4. Real operational data from a power plant was used and different parameters were considered.

European Commission

This project has received funding from the European Union Horizon 2020 research and innovation programme under grant agreement No. 787011 (SPEAR)

Questions ?

CONTACT US

psarigiannidis@uowm.gr

https://www.spear2020.eu/

https://www.linkedin.com/company/spear2020/

https://www.youtube.com/channel/UCw6-d5G01ToBhCmaUnHIcpw

Thank You