**Anomaly Detection in the Cyber-Physical System**

# CPTS 415

**Supervisor: Dr. Yinghui Wu**

**Abstract**

In this project, we use a neural network method for the anomaly detection problem in smart grid dataset. The input data is a 5 features dataset of power grid with normal and anomalous data values. We applied auto encoders and pcap (Wireshark) dataset for detecting the cyber- attacks. All the approaches were discussed above sections in the details. In this project, we coded for the physical smart grid dataset and for the Cyber dataset.

# Introduction: Motivation and Challenges

A common need when analyzing real-world data sets is determining which instances stand out as being dissimilar to all others. Such examples are called as anomalies and the goal of anomaly detection is to determine all such instances is a data-driven fashion. Anomalies can be caused by errors in the data but sometimes are indicative of a new, previously unknown, underlying process; In other words, we can say that an outlier as an observation that deviates signiﬁcation from other observation and that observation arouse suspicion that it generated by diﬀerent procedure.

There are various machine learning techniques to process the anomalies in diﬀerent real world dataset such as Unsupervised, supervised and Reinforcement learning. Unsupervised anomaly detection techniques uncover anomalies in an unlabeled test data, which plays a key role in various application such as, fault-detection, network intrusion detection system, fault diagnosis and ﬁnding the attacks in the smart grid system. I have read few papers, ﬁnd that One-class Support vector machines are widely used, eﬀective unsupervised techniques to identify anomalies. However, comparing the performance of OC-SVM is sub optimal on complex, high dimensional data sets. From recent studies, unsupervised anomaly detection using deep learning is proven to be very eﬀective. Deep learning method for anomaly detection can be broadly classiﬁed into model architecture using auto encoders [3]and hybrid models.

Monitoring and protecting Large Complex Critical Infrastructures (LCCIs) is becoming more and more important, as the growth of structures interdependencies, and their increasing complexity

make them vulnerable to failures or to deliberate attacks. Our goal is to detect anomalies in the dynamics (i.e. evolution over time) of the measure vectors coming from the substations of

an Electric Power System. In this paper, a neural network-based approach for novelty detection is presented, on the same lines proposed by Thompson et al. [1], but in a diﬀerent setting. The use of auto associative neural networks is aimed at learning normal behavior of a LCCIs sub components, for a low level, distributed monitoring approach: dangerous attack or accidental fault within the system would probably bring signiﬁcant deviations at this level, thus causing novelty detection. There are some basics term used in this paper that used in the smart grid system which describe below.

1. Electric Power System (EPS):An Electric Power System (EPS) can be seen as a set of nodes, called substations, connected each other by transmission lines. Each substation, usually monitored by a Remote Terminal Unit (RTU), is composed by several components, each playing a speciﬁc role in the power generation/consuming process. Electric power is generated by generators, distributed through transmission lines, consumed by loads, which demand may usually vary hourly, weekly and monthly.
2. Artiﬁcial Neural Networks: An Artiﬁcial Neural Network (ANN) is built out from simple, non-intelligent units (neurons) which are connected, becoming able to perform complex signal processing. In the learning phase, an ANN is presented with input data set and is trained to ﬁre out the desired values at output layer. The training algorithm iteratively modify weights on connections through which signals are transmitted, in order to minimize gap between network output and desired one. **The Auto encoder Model** - An Auto associative Neural Network Encoder (or simply auto encoder) has two primary features:

-**Auto associative Feature:** the network is trained to reproduce at output layer same values presented as input. For this reason, input and output layer have the same size

(i.e. the same number of neural units).

– **Bottleneck Layer**: at least one of the hidden layers of the network must be smaller than input and output. The architecture selected in this work consists of an input layer, 3 hidden layers, and an output layer (see Fig. 1).The three hidden layers shape a “feature detection” architecture in which the bottleneck layer plays the key role in the identity mapping, as it forces the network to develop a compact representation of the training data that better models the underlying system parameters.

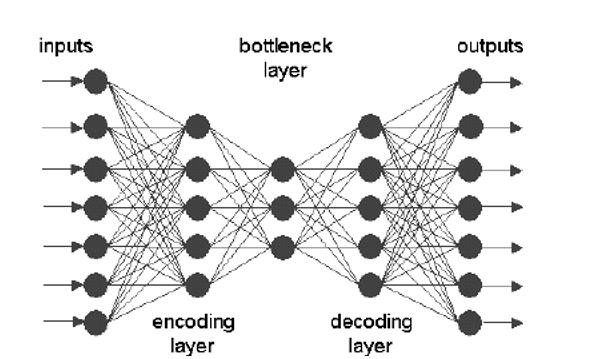


Fig. 1. Sample of auto associative neural network encoder

# Problem Setup

The aim of this project is to build a system able to perform strict on-line monitoring on substations belonging to an electric power network, reading measures by RTUs, and able to shows signiﬁcant changes in case of anomaly detection. One of the major diﬃculties in LCCIs monitoring is due to the non-linear nature of its behavior; the problem become even harder when a large amount of non-predictable abnormal states can arise, due to local or generalized faults. Numerical methods are usually time and resources consuming and could be not proper for an on-line measure monitoring with a small sampling time. Presently, numerical estimation algorithms are often used to rebuild the state of the power system in case of missing and/or corrupted data: however, state estimator approach does not address the problem of giving a normal/abnormal state assessment, and in some cases could tend to hide traces of an ongoing attack or of other anomalies. Moreover, state estimators eﬃciency and accuracy depend on the size of the network, and the estimation of state is often based on prior knowledge about substations sensor reliability. Electric system peculiarities and problem speciﬁc features suggested the use of neural networks as objects able to deal with continuous values coming from physical ﬁelds, with good performances, suitable for on-line data processing, and able to implicitly learn data underlying aspects featuring the system behavior.

# Solution Approach

In December 2015, ﬁrst known successful cyber power grid attack happen in Ukraine. Hackers were able to successfully compromise information system of three energy distribution companies in Ukraine and temporarily disrupt electricity to the end consumers. Wikipedia. This cyber-attack was complex and consist of prior compromise of cooperates network using spear-phishing email with Black Energy malware, also seizing SCADA under control, remotely switching substation oﬀ. From this attack, there are diﬀerent dataset collected to ﬁnd the variations in the normal values. Since, observing the various dataset with the normal and abnormal. Scientist able to deﬁned whether it is an attack or a ﬂuctuation in PMU parameters. The most diﬃcult problem we faced during the ﬂuctuation value and attacks dataset because once the SCADA system has been attacked the values of PMU measurement will change but sometimes ﬂuctuation results into abnormal values. Since, we are diﬀerentiating between the normal and abnormal values, So, it’s Kind of anomaly detection system in the smart grid system. Since there are various algorithms exists to solve the anomaly detection in the machine learning such as one-class SVM, clustering analysis and neural network which is advance version using deep learning. We are using the auto encoder for the anomaly detection. As the auto encoder explain in the introduction, well using this algorithm, we can get an accuracy of 90% in the static dataset we trained and tested. We have the 24 hours dataset with the normal and abnormal values. Considering the algorithm and getting this accuracy gave me the conﬁdence to continue with this approach. Since, Its beginning of the detection of anomaly in the smart grid. The biggest drawbacks we faced in this approach or the dataset, diﬀerentiate between the ﬂuctuation and attack value because in both the situation, the values either drop or raise at some constant levels. Doing more analysis, we can elaborate this project as much more advance, since, currently, we are focusing on detecting the cyber-attack on smart grid and not how we can create defense strategies. If we solve this problem using the reinforcement learning, we can deﬁne the defense and detection strategies based on the current knowledge using Q-learning. Since, we don’t have any model information yet or we need to create an environment for smart grid to solve this problem which is little hard because values and variation in the smart grid are not deﬁned yet. I have tried to solve this problem in the summer vocation but unable to create an environment. However, I end up with developing Q-learning method and strategies for the smart cyber-attack. Please ﬁnd a Link If you want to check the progress(https://github.com/sukhjindermultani/Cyber-Physical- Attackdefense-system). Well, there many diﬀerent systems exist to solve this problem but overall, I found this reinforcement learning approach could be better which create defensive strategies against those cyber physical attacks.

# Experiment and Results

In this section we represent the experimental results of the Auto encoder neural network which mentioned in the previous sections. There are several performance metrics we have used in

this project such as model loss, evaluating algorithm on smote using synthetic data, roc curve, shows the diﬀerent between recall vs precision and show diﬀerent results based on threshold values. I have described the experiment results in diﬀerent sections.

# Data

The dataset used in this section contains 37,550 PMU readings for the last 24 hours based on the smart grid lab. The reading contains attributes of Current, Voltage magnitude and Real Power. In the ﬁrst reading ﬁle, we have 37,550 normal values and in other reading ﬁle, we have abnormal values. For the cyber dataset, we have PCP (Wireshark) ﬁle which is also collected from smart grid lab for testing the cyber-attack such as DOS, physical trip, authentication failure.

# Features

We have 12 features in this dataset for the abnormal and normal readings. The features in these reading is such as 151A-ang,151A-mag,151Bang,151B-mag,151C-ang,151C-mag, V5A-ang, V5A-mag, V5B-ang, V5B-mag, V5Cang, V5C-mag and label for the fault. these are the values for the current and voltage in the diﬀerent angle and magnitude for the diﬀerent phase.

# Evaluation Methodology

1. . Model Loss

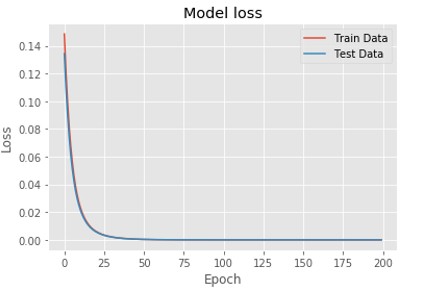
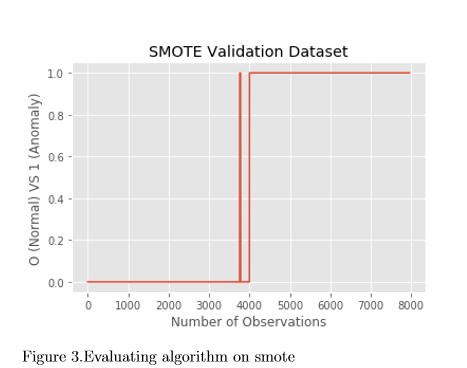
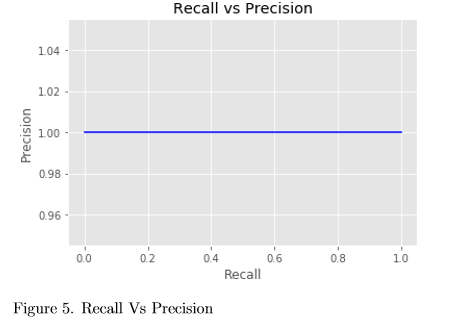
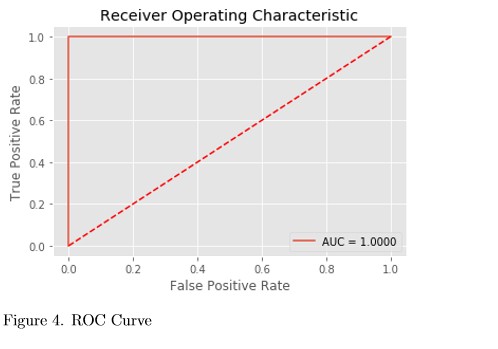


Figure 2. Model loss

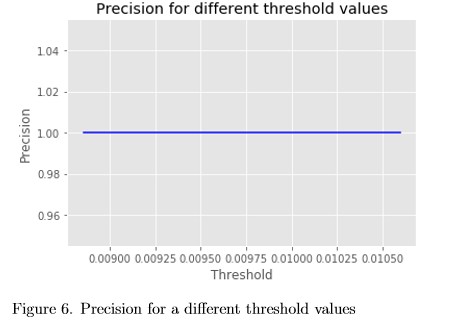


**3. ROC Curve** Receiver operating characteristic curves are an expected output of most

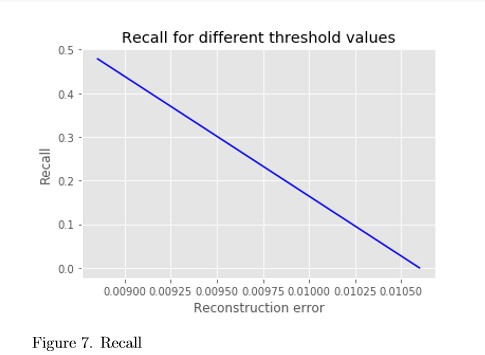
binary classiﬁers. Since we have an imbalanced data set, they are somewhat less useful



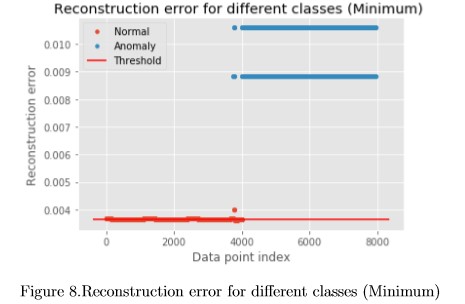
# Precision for diﬀerent threshold values



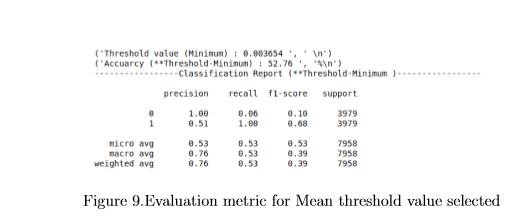
1. **Recall for diﬀerent threshold values**



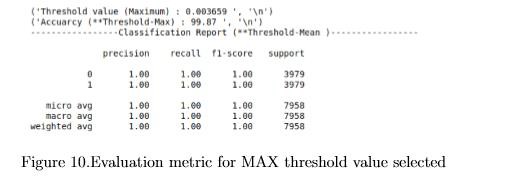
1. **Reconstruction error for diﬀerent classes (Minimum)**



1. **Evaluation metric for Mean threshold value selected above**



1. **Evaluation metric for MAX threshold value selected above**



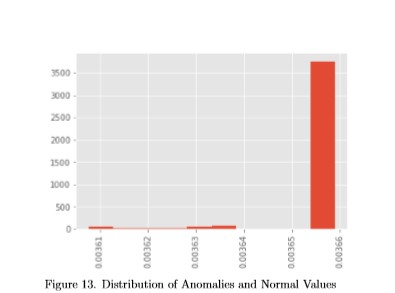
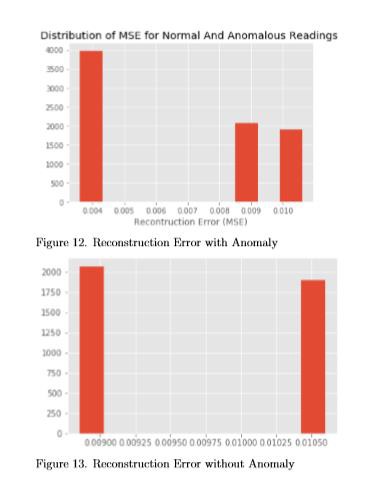
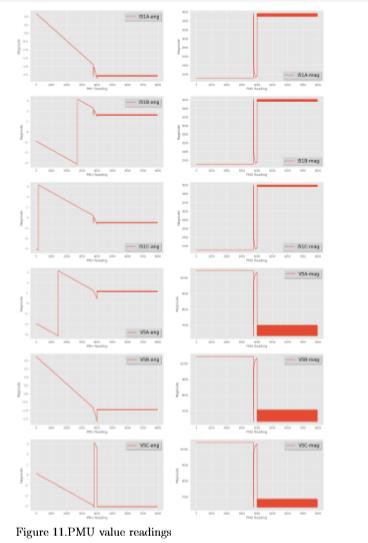
* 1. **Baseline Approach**

Since, in this project we are using only auto encoder for the anomaly detection. Well, there are other unsupervised and ensemble methods exists for the anomaly detection we can use but due to limited period we have used only this algorithm and this algorithm gave us the 90% accuracy for the static dataset and on maximum threshold value which is really good for the anomaly detection.

# Results

To show the process of successfully anomaly detection in the smart grid we have used several performance evaluation techniques as shown in the section 4.3. Figure 11. shows that the value of the features taken in the dataset which corresponds to the variation of the values. X-axis represent the PMU values and Y-axis represent the magnitude of the values. To show the anomalies in the dataset, we plotted reconstruction error with anomaly and without anomalies which shows in the ﬁgure 12. As we calculated the precision, recall, f-score and support using the minimum threshold value and maximum threshold value which shows in the ﬁgures. These performance metrics shows that using the auto encoder based neural network successfully detected anomalies in the smart grid system. From this project I found the interesting approach

for detecting the anomalies in the smart grid dataset. The implementation of the encoder can be seen as below.



# 4.6. How we achieved the accuracy?

In this project, we evaluate algorithms on test data using two method which are autoencoder

and synthetic modelling. ﬁrst, we calculated threshold values for the test data and try to plot

w.r.t data point index. Based on those we got three diﬀerent values which are minimum, mean and maximum threshold values. Now, using these values, we can easily calculate anomalies value which corresponds to the accuracy of detecting anomalies in the static dataset. When we get threshold value in the dataset, we use those values to get the classiﬁcation report. In this project, threshold-mean corresponds to threshold value (min,max and mean) when we get 99% which mean we have threshold max value which corresponds to the accuracy however this values are for the static dataset.

# Conclusions and Future Work

In this project, we consider a general framework for anomaly detection for cyber-physical systems security. Place of using classical anomaly detection tools, we apply a formal methods approach to the problem. We designed and implemented an algorithm which is able to infer a data classiﬁer in the form of a signal temporal logic formula from unlabeled data. The inferred formula can be interpreted in natural language and can be used in the future for online monitoring. We demonstrated our approach using two case studies, including a model of a train under attack. Our approach was able to classify the attacked and normal outputs for both case studies with low misclassiﬁcation rates.In this project, detecting anomalies in the smart grid system is hard problem due to non-linearity of the dataset problem.The result given by auto encoder could be eﬀectively used by the applications that care only the right order of the

encoder and decoder. Since, we detected attack based on the static dataset but if this work online and on changing the variation of voltage the results may be defer. But we believe that setting the voltage and current variation will give us better performance as we achieved in this project. The study of an auto encoder can aﬀect its performance greatly. variation in PMU reading may aﬀect the performance more than unit layout does. One important future study of this project is to study the reason that how we can defense the attack system. Since, we have the detection algorithms and only thing we can do is how to do defense in the smart grid. We have tried to implement reinforcement learning to do defense but still we are lacking in few things such as what if there’s fault in the system then the PMU reading changes and it will converge according to the performance of the devices. So, detecting and creating defensive strategies will be the future study for the advancement of the cyber-physical system.

1. **References**

[1][https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-](https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/) [power-grid/](https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/)

[2]V. P. Illiano, E. C. Lupu, Detecting malicious aata injections in wireless sensor networks: a survey, ACM Computig Surveys 48, 2 (2015).)103, 104

[3]https:/[/www.rese](http://www.researchgate.net/publication/220565847-Anomaly-Detection-A-)a[rchgate.net/publication/220565847-Anomaly-Detection-A-](http://www.researchgate.net/publication/220565847-Anomaly-Detection-A-)

Survey

[4] M. A. Rassam, A. Zainal, M. A. Maarof, Advancements of data anomaly detection research in wireless sensor networks: a survey and open issues, Sensors 13, 8 (2013) 10087{10122. )103, 104

[5]<http://yann.lecun.com/exdb/publis/pdf/lecun-90c.pdf>

[6]V. Chandola, A. Banerjee, V. Kumar, Anomaly detection: a survey, ACM Computing Surveys 41, 3 (2009). )103, 108, 114