Electronics and Computer Science

Faculty of Physical Sciences and Engineering

University of Southampton

Author: Emiliyan Veselinov Hristov – evh1u20

Date: 07.06.2023

COMP3217

Assignment 2: Detection of Attacks on Power System Grids

GitHub Link - https://github.com/emiliyanhristov/coursework2

Part A

Problem: In Part A we are given 6000 system traces for our Power System Grid. Each one is labelled with either 0 for a normal event or 1 indicating a data injection attack. Using these traces an AI must be trained on the 128 features of each trace (4 Phasor Measurement Units (PMUs) with 29 features = 116 features and additional 12 features for control panel logs), to label the trace as normal or data injection event. Then the AI must predict the labels of another 100 system traces.

Machine Learning Technique: The Random Forest Classifier method was used for the machine learning AI. This method makes a prediction based on the data by using several decision trees, in this case, 100. This technique is extremely accurate, able to handle vast amounts of data, can indicate which features are more important, and also is less prone to overfitting. This method was chosen after trying out various scikit-learn algorithms and deciding on the best one based on its coefficient of determination and mean square error regression loss. For the training of the model, the 6000 traces were split into 80% training and 20% testing shuffled data and then used to make predictions on the 100 testing traces.

Computed Labels: These are the computed labels for every row in the 100 test system traces for Part A - [1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0] in the same order.

Training Error and Accuracy: The training accuracy for the Random Forest Classifier technique for Part A is the coefficient of determination R2 = 0.985 (with a best possible score of 1.0) and the training error is calculated using mean square error regression loss RMSE = 0.035.

Part B

Problem: In Part B we are given 6000 system traces for our Power System Grid. Each one is labelled with 0 for a normal event, 1 indicating a data injection attack, and 2 standing for a command injection attack. Using these traces an AI must be trained on the 128 features of each trace (4 Phasor Measurement Units (PMUs) with 29 features = 116 features and additional 12 features for control panel logs), to label the trace as normal, data injection, or command injection event. Then the AI must predict the labels of another 100 system traces.

Machine Learning Technique: The Random Forest Classifier method was again used for the machine learning AI. As discussed in Part A, this method makes a prediction based on the data by using several decision trees, in this case again, 100. This technique is extremely accurate, able to handle vast amounts of data, can indicate which features are more important, and also is less prone to overfitting. This method was again chosen after trying out various more complex scikit-learn algorithms and deciding on the best one based on its coefficient of determination and mean square error regression loss. For the training of the model, the 6000 traces were split into 80% training and 20% testing shuffled data and then used to make predictions on the 100 testing traces.

Computed Labels: These are the computed labels for every row in the 100 test system traces for Part B - [2, 2, 2, 2, 2, 2, 1, 1, 2, 2, 2, 1, 1, 1, 1, 1, 2, 1, 1, 1, 1, 1, 2, 1, 1, 1, 2, 2, 2, 2, 2, 2, 2, 1, 1, 1, 1, 1, 2, 1, 1, 1, 1, 2, 2, 2, 2, 2, 2, 1, 2, 2, 2, 2, 2, 2, 2, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0] in the same order.

Training Error and Accuracy: The training accuracy for the Random Forest Classifier technique for Part B is the coefficient of determination R2 = 0.98 (with a best possible score of 1.0) and the training error is calculated using mean square error regression loss RMSE = 0.095.