**CHAPTER 4 - RESULTS AND ANALYSIS**

**4.1 MATLAB SIMULATION RESULTS**

Matlab simulation plots for the fault conditions and fault types on the WSCC-9 bus system are plotted. The graphs indicate the voltage and current of the three phases in two lines- one in which the fault has occurred and one a neighbouring line which compensates for the fault.

**4.1.1 SINGLE LINE TO GROUND FAULT (L-G)**

**4.1.1.1 Line Containing Fault (Line 4-6, B)**

Chart, line chart

Description automatically generatedA picture containing diagram

Description automatically generated

## Figure 4.2: Phase Current of Line 4-6

Figure 1 : Phase Voltage Plot of line 4-6

**Figure 4.1: Phase Voltage of Line 4-6**

**4.1.1.2 Line Without Fault (Line 5-4, A)**

Chart, line chart

Description automatically generatedChart, line chart

Description automatically generated

## Figure 4.3: Phase Voltage of Line 5-4

## Figure 4.4: Phase Current of line 5-4

**4.1.2 LINE TO LINE FAULT (L-L)**

**4.1.2.1 Line Containing Fault (Line 4-6, B)**Chart, line chart

Description automatically generated

## Figure 4.5: Phase Voltage of Line 4-6

Chart, line chart

Description automatically generated

## Figure 4.6: Phase Current of Line 4-6

**4.1.2.2 Line Without Fault (Line 5-4, A)**

Chart, line chart

Description automatically generated

## Figure 4.7: Phase Voltage of Line 5-4

Chart, line chart

Description automatically generated

## Figure 4.8: Phase Current of Line 5-4

**4.1.3 DOUBLE LINE TO GROUND FAULT (L-L-G)**

**4.1.3.1 Line Containing Fault (Line 4-6, B)**

Chart, line chart

Description automatically generated

## Figure 4.9: Phase Voltage of Line 4-6

Chart, line chart

Description automatically generated

## Figure 4.10: Phase Current of Line 4-6

**4.1.3.2 Line Without Fault (Line 5-4, A)**

Chart, line chart

Description automatically generated

## Figure 4.11: Phase Voltage of Line 5-4

Chart, line chart

Description automatically generated

## Figure 4.12: Phase Current of Line 5-4

**4.1.4 ALL THREE PHASE TO GROUND FAULT (L-L-L-G)**

**4.1.4.1 Line Containing Fault (Line 4-6, B)**

Chart, line chart

Description automatically generated

## Figure 4.13: Phase Voltage of LIne 4-6

Chart, line chart

Description automatically generated

## Figure 4.14: Phase Current of Line 4-6

**4.1.4.2 Line Without Fault (Line 5-4, A)**

Chart, line chart

Description automatically generated

## Figure 4.15: Phase Voltage of Line 5-4

Chart, line chart

Description automatically generated

## Figure 4.16: Phase Current of Line 5-4

**4.1.5 ALL THREE PHASE SHORT CIRCUITED (L-L-L)**

**4.1.5.1 Line Containing Fault (Line 4-6, B)**

Chart, line chart

Description automatically generated

## Figure 4.17: Phase Voltage of Line 4-6

Chart, line chart

Description automatically generated

## Figure 4.18: Phase Current of Line 4-6

**4.1.5.2 Line Without Fault (Line 5-4, A)**

Chart, line chart

Description automatically generated

## Figure 4.19: Phase Voltage of line 5-4

Chart, line chart

Description automatically generated

## Figure 4.0: Phase Current of Line 5-4

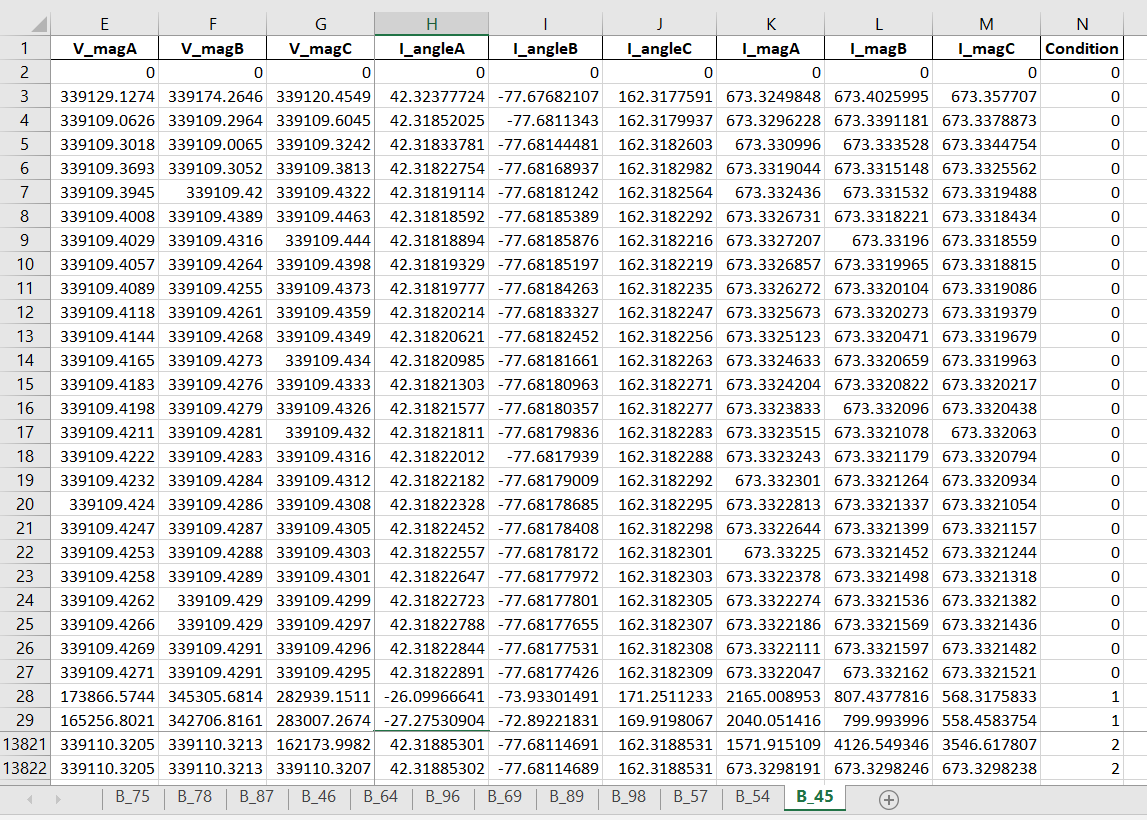


Figure 2 Consolidated dataset

Figure 2 provides an example of the consolidated dataset. Three types of condition are indicated as – Normal Operation (0), Faults (1) and Cyber Attacks (2). The following features were sent from across from the circuit breaker to the main control substation, indicated in Table x.

|  |
| --- |
| Features extracted |
| Phase A voltage magnitude |
| Phase B voltage magnitude |
| Phase C voltage magnitude |
| Phase A voltage angle |
| Phase B voltage angle |
| Phase C voltage angle |
| Phase A current magnitude |
| Phase B current magnitude |
| Phase C current magnitude |
| Phase A current angle |
| Phase B current angle |
| Phase C current angle |

**4.2 CYBER-ATTACK RESULTS**

**4.2.1 Modbus TCP Server**

The server code will be running at the Control Centre and will be responsible for listening and responding to requests as well interacting with the database to store data values. A screenshot of the server code is attached below, and the same source code can be found in the appendix

Graphical user interface, text, application

Description automatically generated

Figure : Modbus TCP Server Code

**4.2.2 Modbus TCP Client**

The client code will be running in the PLCs and RTUs. The client code allows the devices to send data and requests to the server. A screenshot of the client code is attached below, and the same source code can be found in the appendix.

Graphical user interface, text, application

Description automatically generated

Figure 2 : Modbus TCP Client Code

**4.2.3 Encode data to Modbus format**

The raw data is converted to Modbus format and is sent to the server. When the payload is fetched it is then finally decoded back to raw data using PyModbus. A screenshot of the payload encoder - decoder code is attached below, and the same source code can be found in the appendix.

A screenshot of a computer

Description automatically generated with medium confidence

Figure3 : PyModbus Payload Code

Text

Description automatically generated

Figure 4 : The decoded payload data, as received back by the client device.

**4.2.4 Setup cyber-attack architecture**

For this thesis, we started with two Windows devices which served as the client and server for Modbus communication. This was accompanied by a third device running Kali Linux on it. It utilised Ettercap v0.8.2 for sniffing and launching ARP Poisoning attacks.

**4.2.5 Perform man-in-the-middle attacks**

A MITM attack was performed with an Ettercap tool that maliciously modified the Modbus TCP commands between the Master and PLC workstations. An Ettercap filter within the Ettercap tool was then created to modify Modbus TCP communications.



Figure 5 : Loading a filter in Ettercap

**4.2.6 Gather Cyber Attack data**

Generate and gather the data produced from conducting cyber-attacks on the network. Perform data wrangling, feature extraction, etc on the gathered data to prepare it for the machine learning model.

**4.3 Machine Learning Results**

Both supervised and unsupervised machine learning techniques were applied for the classification of events. K-Means clustering (unsupervised), Random Forest (supervised) and Decision Tree Classifier (supervised) were the three machine learning algorithms used. Results for each are shown in Table x,y,z.

K-Means

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Fault Line | Accuracy | Precision | Recall | F1 Score |
| a | 86.9 | 82 | 88 | 87 |
| b | 87.5 | 83 | 87 | 89 |
| c | 86.5 | 84 | 86 | 85 |
| d | 86.9 | 83 | 87 | 86 |
| e | 87.3 | 87 | 88 | 85 |
| f | 87.2 | 89 | 82 | 85 |

Random Forest

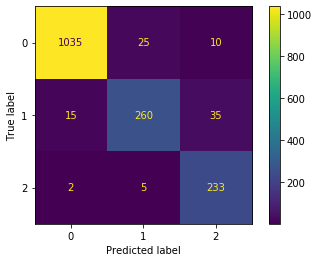
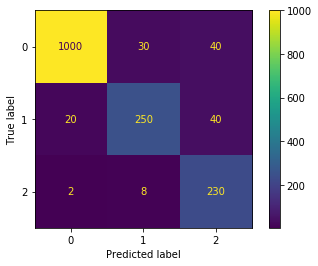
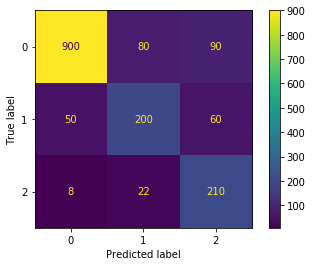
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Fault Line | Accuracy | Precision | Recall | F1 Score |
| a | 95.1 | 95 | 96 | 94 |
| b | 95.6 | 96 | 95 | 95 |
| c | 96.3 | 96 | 97 | 94 |
| d | 95.8 | 96 | 95 | 92 |
| e | 95.3 | 96 | 94 | 95 |
| f | 95.9 | 94 | 96 | 95 |

Decision Tree Classifier

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Fault Line | Accuracy | Precision | Recall | F1 Score |
| a | 96.1 | 96 | 93 | 95 |
| b | 96.6 | 98 | 94 | 96 |
| c | 97.3 | 98 | 96 | 96 |
| d | 96.8 | 95 | 95 | 95 |
| e | 96.3 | 96 | 94 | 94 |
| f | 96.9 | 97 | 96 | 95 |

Figure 3 : Confusion Matrices for Line C obtained from K-Means, Random Forest and Decision Tree Classifier respectively 0 - Natural Operation , 1 – Fault, 2- Cyber Attack

(



From tables x,yz, the performance of each machine learning algorithm was seen on each line in the system. It was observed that Decision Tree algorithm performs the best out of the three with an average accuracy of 96%. In general, supervised learning algorithms perform slightly better than unsupervised algorithms in this case.

The confusion matrices for each of the algorithms on line C are shown in Figure f. Despite the high accuracy of the algorithms, there are few cases where the cyber attacks mimic natural events and are misclassified.