

## SIL765 : Networks and System Security

### Assignment – 4

1) There are 27 different message identifiers which are recorded on this CAN bus, these are :

```
['0316', '018f', '0260', '02a0', '0329', '0545', '0002', '0153',  
'02c0', '0130', '0131', '0140', '0350', '043f', '0370', '0440',  
'04f0', '0430', '04b1', '01f1', '05f0', '00a0', '00a1', '0690',  
'05a0', '05a2', '0000']
```

```
(base) Nikitas-MacBook-Air:SIL_Assign4 nikitabhamu$ python can.py  
Different message identifiers : 27  
['0316', '018f', '0260', '02a0', '0329', '0545', '0002', '0153', '02c0', '0130',  
'0131', '0140', '0350', '043f', '0370', '0440', '04f0', '0430', '04b1', '01f1',  
'05f0', '00a0', '00a1', '0690', '05a0', '05a2', '0000']
```

2) All the messages are read till the time the first anomaly shows up, i.e., the time when the first message with label with 'T' comes up.

We found that mean of the inter message arrival times of the some message ids is 10 times the standard deviation, rest all the message ids have standard deviation quite less than the mean. So, if we consider a message to be periodic if the standard deviation of the inter message arrival times is 10 or more times lesser than the mean of the inter message arrival time, then all the messages will turn out to be periodic

#### DoS\_dataset :

```
(base) Nikitas-MacBook-Air:SIL_Assign4 nikitabhamu$ python periodic.py DoS_dataset.csv
```

MessageId	Mean_InterMsgTime	StdDev_InterMsgTime
0316	0.01	0.0002
018f	0.01	0.0001
0260	0.01	0.0001
02a0	0.01	0.0001
0329	0.01	0.0001
0545	0.01	0.0002
0002	0.01	0.001
0153	0.01	0.0005
02c0	0.01	0.0005
0130	0.01	0.001
0131	0.01	0.001
0140	0.01	0.001
0350	0.01	0.0001
043f	0.01	0.0004
0370	0.01	0.0002
0440	0.01	0.0002
04f0	0.02	0.0002
0430	0.02	0.0
04b1	0.02	0.0
01f1	0.02	0.0
05f0	0.0501	0.0004
00a0	0.0999	0.0001
00a1	0.0999	0.0001
0690	0.1	0.0001

### gear\_dataset :

```
(base) Nikitas-MacBook-Air:SIL_Assign4 nikitabhamu$ python periodic.py gear_dataset.csv
MessageId      Mean_InterMsgTime  StdDev_InterMsgTime
0140            0.0101            0.0019
02c0            0.0101            0.001
0350            0.0103            0.0021
0370            0.0104            0.0034
043f            0.0101            0.0012
0440            0.0102            0.0019
0316            0.0103            0.003
018f            0.0104            0.0039
0002            0.0101            0.0016
0153            0.0101            0.0013
0260            0.0101            0.0011
0130            0.0101            0.0019
0131            0.0101            0.0019
02a0            0.0101            0.0013
0329            0.0101            0.0014
0545            0.0101            0.0013
04f0            0.02            0.0002
0430            0.02            0.0002
04b1            0.0203            0.0027
01f1            0.0203            0.0027
05f0            0.05            0.0005
00a0            0.0999            0.0001
00a1            0.0999            0.0001
0690            0.1            0.0
```

### 3) IDS for DOS attacks :

#### How to execute?

--> python ids\_dos.py DoS\_dataset.csv

--> Classifier used :- Logistic Regression

--> Features of the message used :

1. Message identifier
2. Data length
3. Inter message arrival time

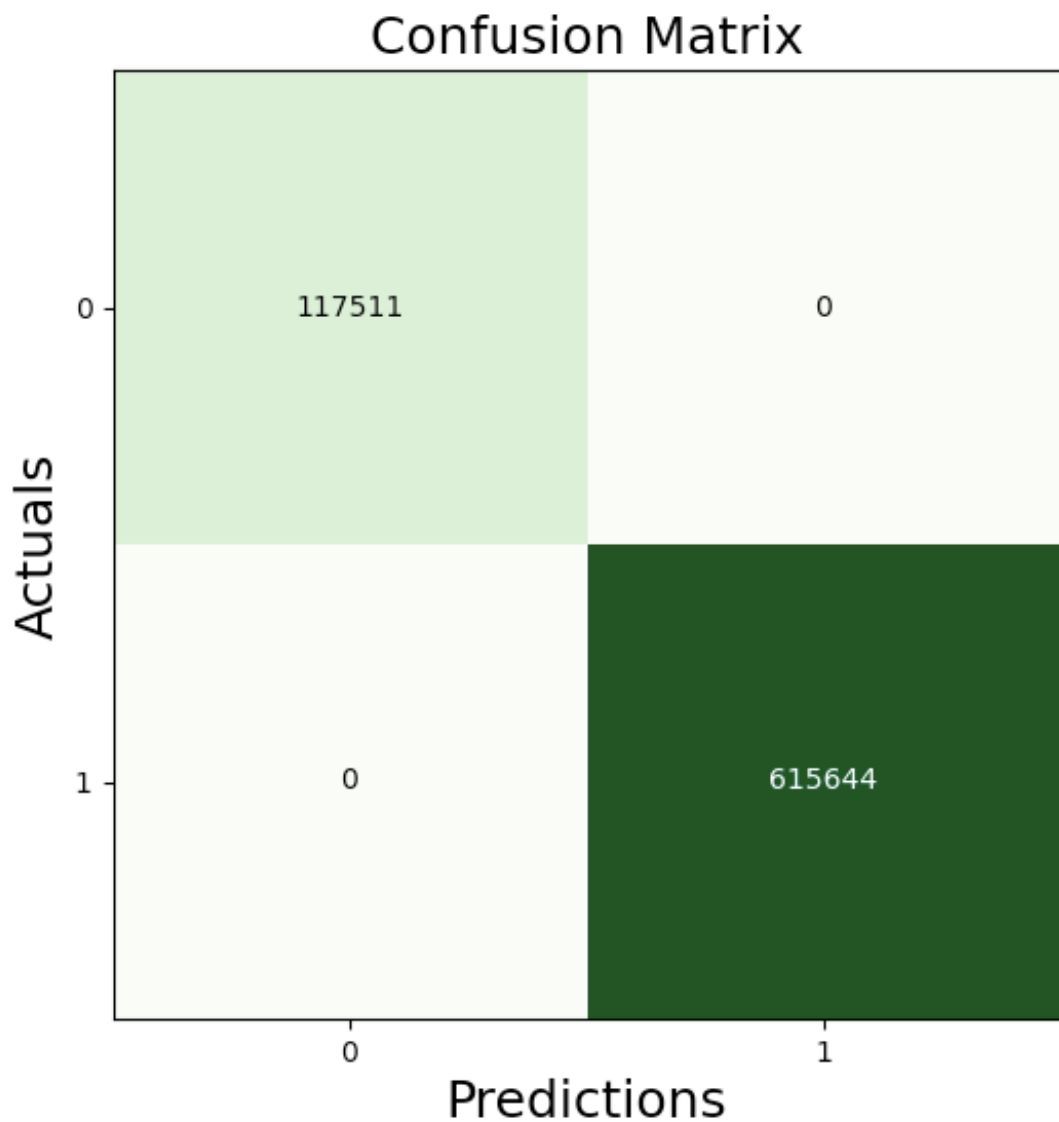
This model is trained on 80% of the dataset given and tested on 20% of the dataset

The accuracy which this model is giving is : 100%

```
(base) Nikitas-MacBook-Air:SIL_Assign4 nikitabhamu$ python ids_dos.py DoS_dataset.csv
Accuracy : 1.0
      precision    recall  f1-score   support

     0         1.00      1.00      1.00     117511
     1         1.00      1.00      1.00     615644

   accuracy          1.00      1.00      1.00     733155
  macro avg          1.00      1.00      1.00     733155
weighted avg          1.00      1.00      1.00     733155
```



'R' labeled messages correctly identified : 615644

'R' labeled messages wrongly identified : 0

'T' labeled messages correctly identified : 117511

'T' labeled messages wrongly identified : 0

Detection rate of this model : 100%

False alarm rate : 0%

#### 4) IDS for Impersonation attacks :

##### How to execute?

--> `python ids_dos.py DoS_dataset.csv`

--> Classifier used :- Logistic Regression

--> Features of the message used :

1. Message identifier
2. Data length

3. Mean of the inter message arrival times
4. Standard deviation of the inter message arrival times
5. Inter message arrival time

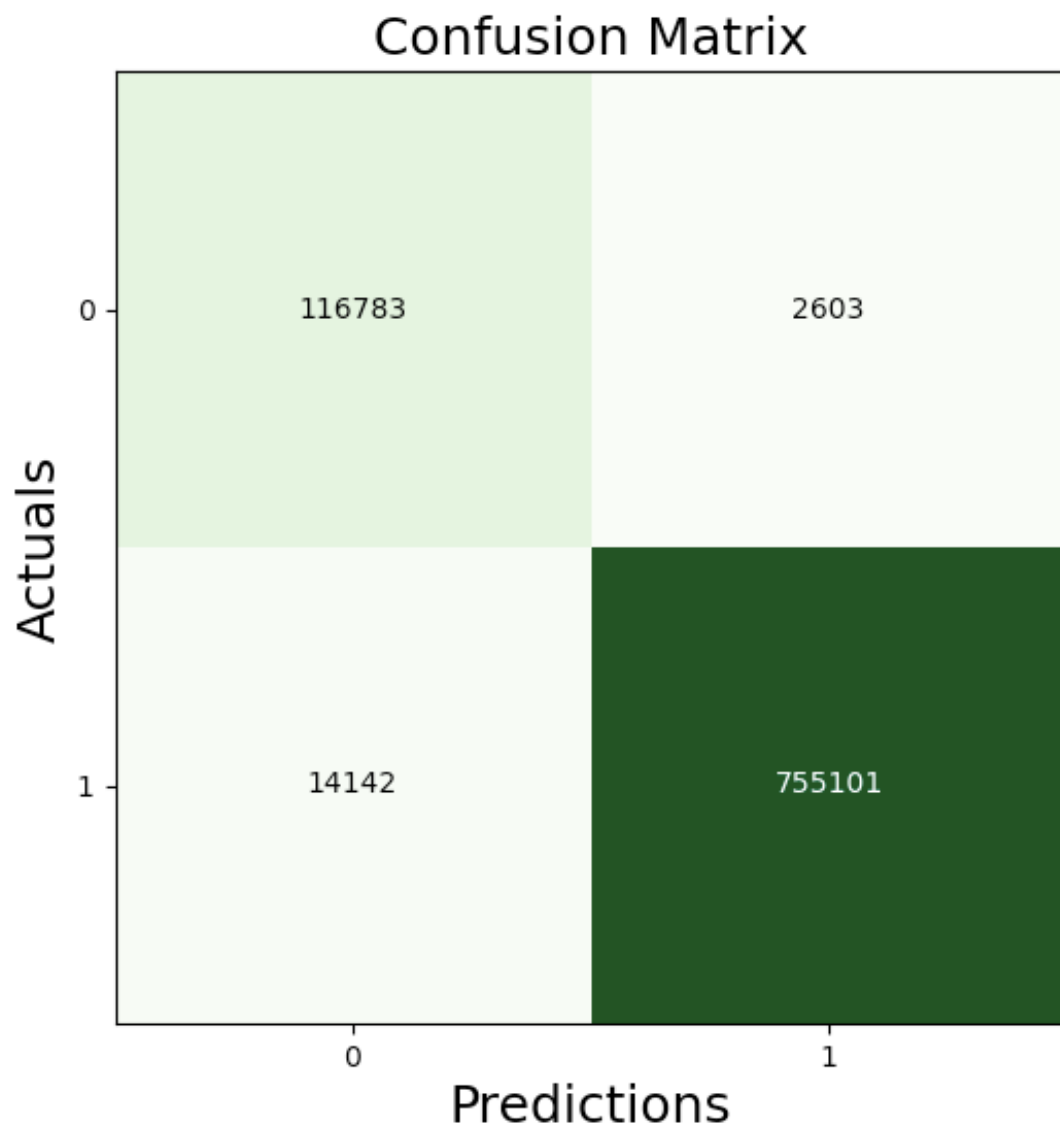
This model is trained on 80% of the dataset given and tested on 20% of the dataset

The accuracy which this model is giving is : 98.115%

```
(base) Nikitas-MacBook-Air:SIL_Assign4 nikitabhmu$ python ids_impersonation.py gear_data.csv
Accuracy : 0.9811563655923901
          precision    recall  f1-score   support

     0       0.89       0.98       0.93     119386
     1       1.00       0.98       0.99     769243

   accuracy          0.98     888629
  macro avg       0.94       0.98       0.96     888629
 weighted avg       0.98       0.98       0.98     888629
```



'R' labeled messages correctly identified : 755101

'R' labeled messages wrongly identified : 14142

'T' labeled messages correctly identified : 116783

'T' labeled messages wrongly identified : 2603

Detection rate of this model : 98.115%

False alarm rate : **1.8%**

**Submitted By :-**

→ **Nikita Bhamu**

→ **2018CS50413**