QUIC Protocol: DoS attack

Anomaly Detection

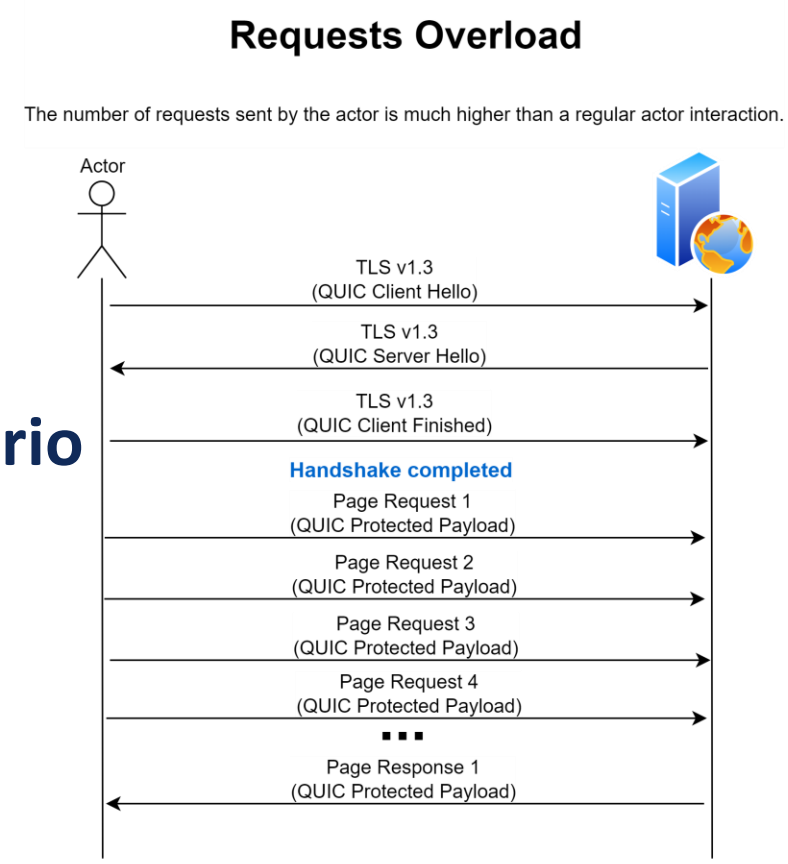
Maria Inês Rocha 93320

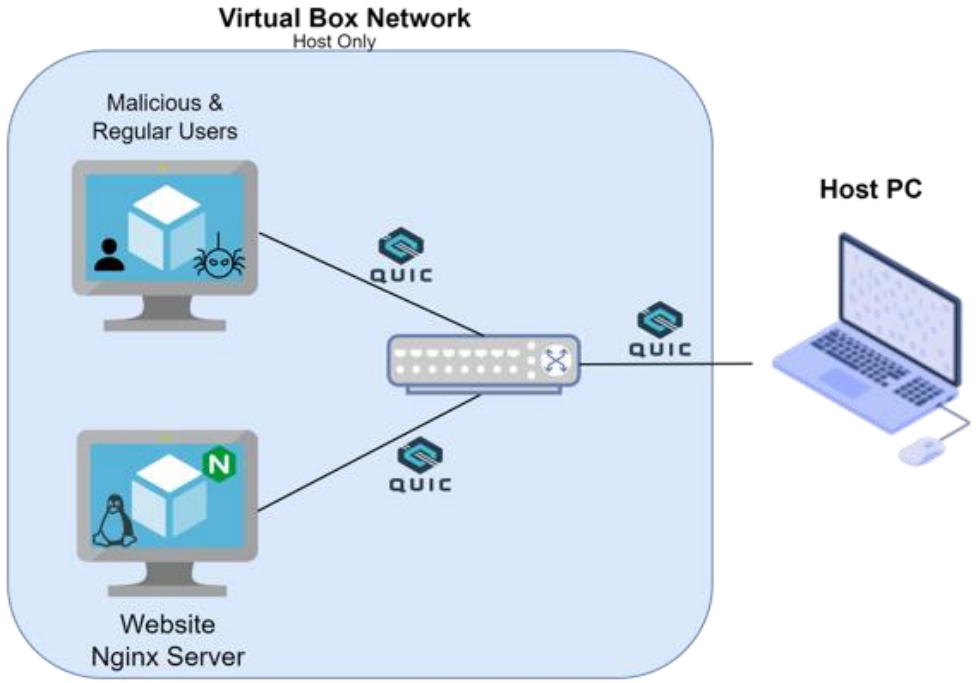
Pedro Abreu 93240

Main Objective

- To detect a **QUIC DoS attack** – service denial attack
- Proposed: 3 different scenarios
- Achieved: only 1 scenario evaluated

Test Scenario





Solution Setup

Data Sources

Network Packets

- Wireshark

Observation Windows Tested

- 10 secs with sliding of 2 secs
- 20 secs with sliding of 5 secs
- 60 secs with sliding of 10 secs

Metrics

Time between consecutive packets

Packet Size

Number of QUIC Packets

Time Independent Features

Average packet length

Median packet length

Standard deviation packet length

95th percentile packet length

Minimum packet length

Maximum packet length

Time Dependent Features

Average of time

Median of time

Standard deviation of time

Nº of upload packets

Two cases:

<1 sec

> 1 sec

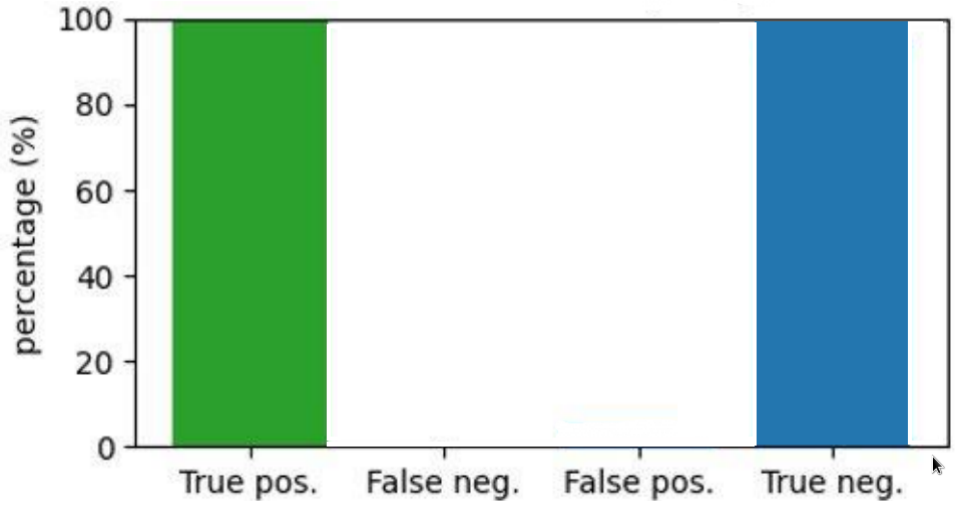
Analysis Context

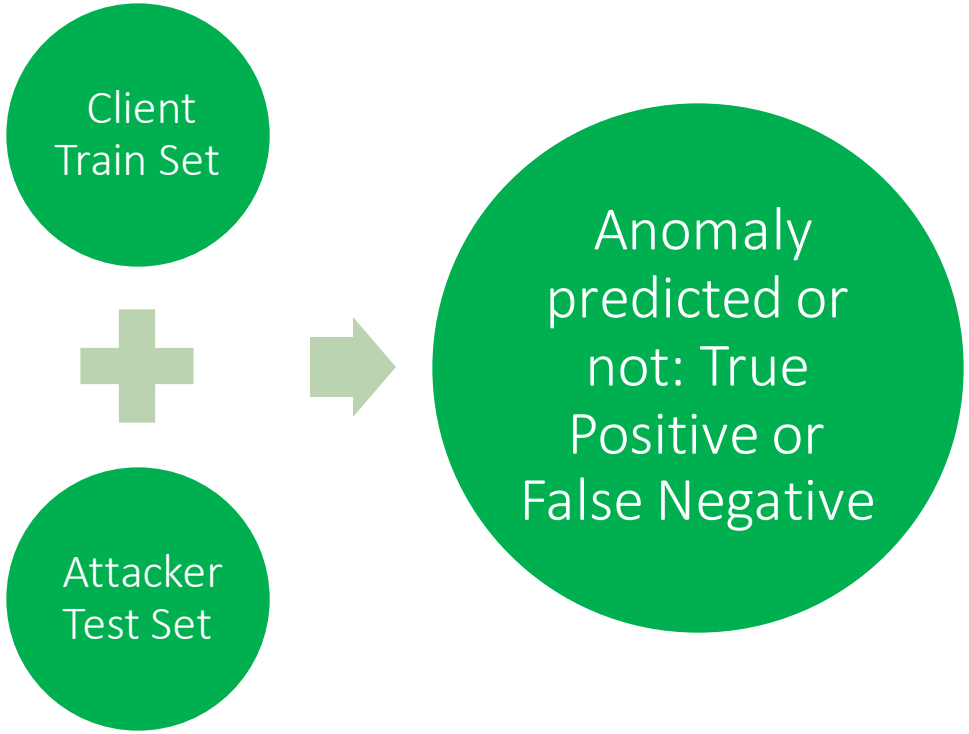
- Detecting anomalies:

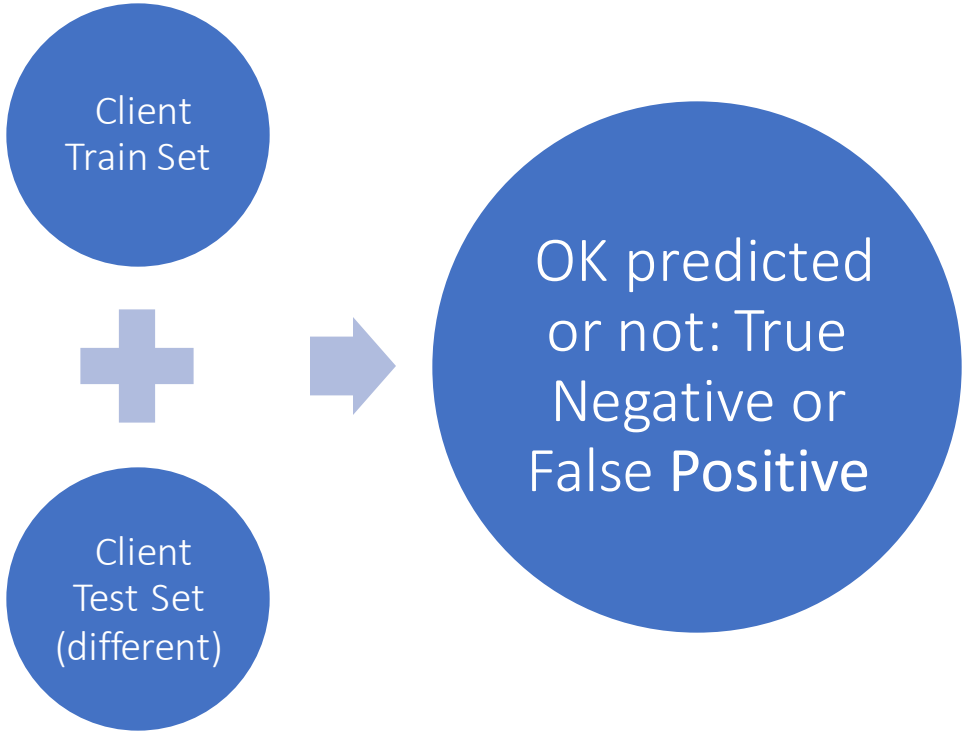
=> Positive Class: Anomaly

=> Negative Class: Ok

Perfect Scenario







Results >> Window: 10 Slide: 2

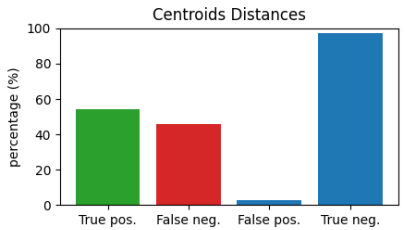
```
-- Analysis of Centroids Distances --
True Positives: 1630, False Negatives: 2827
True Negatives:   83, False Positives: 1397

Accuracy (%):                      28.85
Precision (%):                     53.85
Recall (%):                        36.57
F1-Score:                          43.56
----------------------------------------
-- Analysis of Centroids Distances (PCA) --
True Positives: 1585, False Negatives: 2839
True Negatives:   71, False Positives: 1442

Accuracy (%):                      27.89
Precision (%):                     52.36
Recall (%):                        35.83
F1-Score:                          42.54
----------------------------------------
-- Analysis of Multivariate PDF (PCA) --
True Positives: 1641, False Negatives: 2791
True Negatives:  119, False Positives: 1386

Accuracy (%):                      29.64
Precision (%):                     54.21
Recall (%):                        37.03
F1-Score:                          44.0
----------------------------------------
```

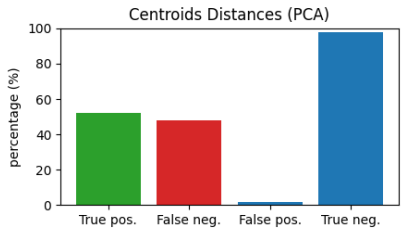
```
-- Analysis of One Class SVM Linear --
True Positives:   73, False Negatives: 1669
True Negatives: 1241, False Positives: 2954

Accuracy (%):                      22.13
Precision (%):                      2.41
Recall (%):                         4.19
F1-Score:                           3.06
----------------------------------------
-- Analysis of One Class SVM Linear (PCA) --
True Positives: 1154, False Negatives: 2848
True Negatives:   62, False Positives: 1873

Accuracy (%):                      20.48
Precision (%):                     38.12
Recall (%):                        28.84
F1-Score:                          32.84
----------------------------------------
```

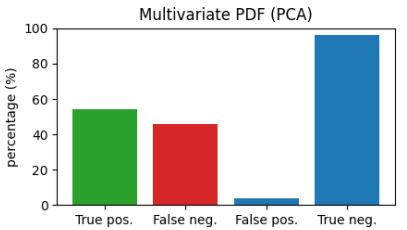
```
-- Analysis of One Class SVM RBF --
True Positives: 3027, False Negatives: 1344
True Negatives: 1566, False Positives:    0

Accuracy (%):                      77.36
Precision (%):                     100.0
Recall (%):                        69.25
F1-Score:                          81.83
----------------------------------------
-- Analysis of One Class SVM RBF (PCA) --
True Positives: 3027, False Negatives: 1450
True Negatives: 1460, False Positives:    0

Accuracy (%):                      75.58
Precision (%):                     100.0
Recall (%):                        67.61
F1-Score:                          80.68
----------------------------------------
```

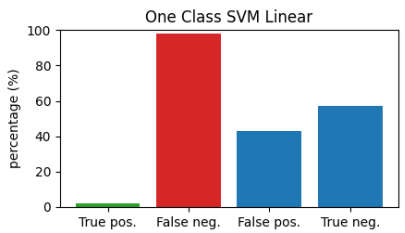
```
-- Analysis of SVM Poly --
True Positives:   55, False Negatives: 1670
True Negatives: 1240, False Positives: 2972

Accuracy (%):                      21.81
Precision (%):                      1.82
Recall (%):                         3.19
F1-Score:                           2.31
----------------------------------------
-- Analysis of One Class SVM poly (PCA) --
True Positives: 1385, False Negatives: 1366
True Negatives: 1544, False Positives: 1642

Accuracy (%):                      49.33
Precision (%):                     45.75
Recall (%):                        50.35
F1-Score:                          47.94
----------------------------------------
```

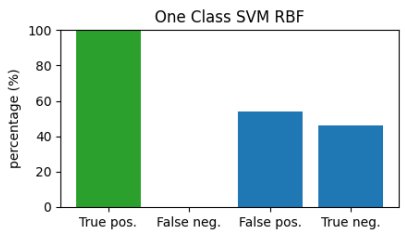
```
- Total of Anomalies for each method -
Num. Observações test dataset:     4424
Num. entrys from browsing:         2910
Num. entrys from DoS:              1514
Percentage of DoS entrys:          34.2
Expected anomalys:               1513.0


Centroids Distance:                 583
Centroids Distance PCA:             526
Multivariate PCA:                   630
SVM Linear:                        1314
SVM Linear PCA:                      86
SVM RBF:                           3080
SVM RBF PCA:                       2974
SVM Poly:                          1295
SVM Poly PCA:                      2547
----------------------------------------
```

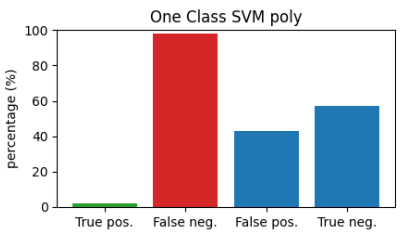


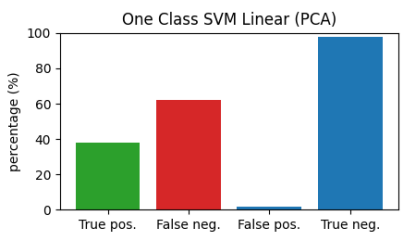


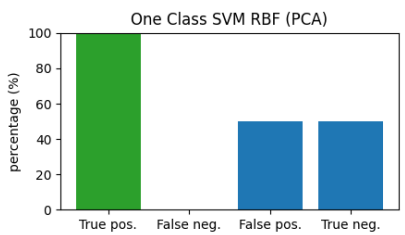


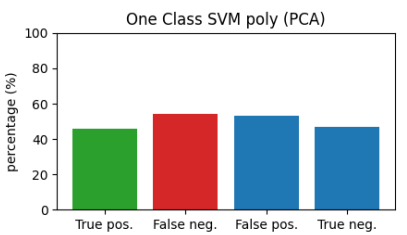












Results >> Window: 20 Slide: 5

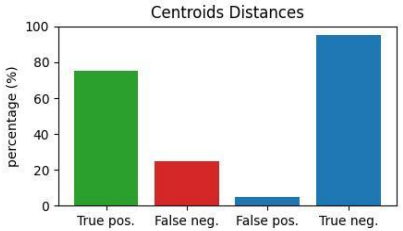
```
-- Analysis of Centroids Distances --
True Positives:  906, False Negatives: 1109
True Negatives:   53, False Positives:  300

Accuracy (%):                          40.5
Precision (%):                        75.12
Recall (%):                           44.96
F1-Score:                             56.26
----------------------------------------
-- Analysis of Centroids Distances (PCA) --
True Positives:  654, False Negatives: 1114
True Negatives:   48, False Positives:  552

Accuracy (%):                          29.65
Precision (%):                        54.23
Recall (%):                           36.99
F1-Score:                             43.98
----------------------------------------
-- Analysis of Multivariate PDF (PCA) --
True Positives: 1206, False Negatives: 1101
True Negatives:   61, False Positives:    0

Accuracy (%):                          53.51
Precision (%):                        100.0
Recall (%):                           52.28
F1-Score:                             68.66
----------------------------------------
```

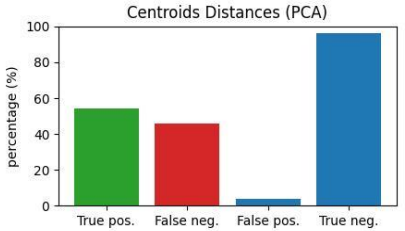
```
-- Analysis of One Class SVM Linear --
True Positives:    0, False Negatives:  650
True Negatives:  512, False Positives: 1206

Accuracy (%):                          21.62
Precision (%):                          0.0
Recall (%):                             0.0
F1-Score:                                 0
----------------------------------------
-- Analysis of One Class SVM Linear (PCA) --
True Positives:  654, False Negatives: 1110
True Negatives:   52, False Positives:  552

Accuracy (%):                          29.81
Precision (%):                        54.23
Recall (%):                           37.07
F1-Score:                             44.04
----------------------------------------
```

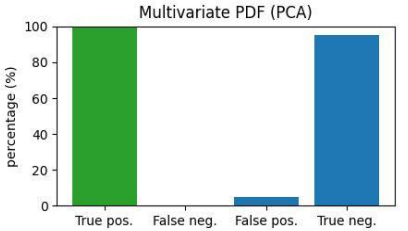
```
-- Analysis of One Class SVM RBF --
True Positives: 1206, False Negatives:  541
True Negatives:  621, False Positives:    0

Accuracy (%):                          77.15
Precision (%):                         100.0
Recall (%):                           69.03
F1-Score:                             81.68
----------------------------------------
-- Analysis of One Class SVM RBF (PCA) --
True Positives: 1206, False Negatives:  537
True Negatives:  625, False Positives:    0

Accuracy (%):                          77.32
Precision (%):                         100.0
Recall (%):                           69.19
F1-Score:                             81.79
----------------------------------------
```

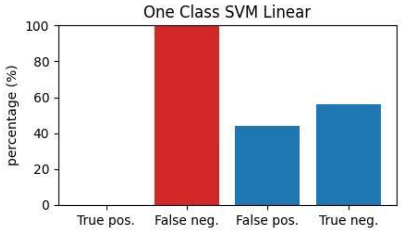
```
-- Analysis of SVM Poly --
True Positives:    0, False Negatives:  650
True Negatives:  512, False Positives: 1206

Accuracy (%):                          21.62
Precision (%):                          0.0
Recall (%):                             0.0
F1-Score:                                 0
----------------------------------------
-- Analysis of One Class SVM poly (PCA) --
True Positives:   14, False Negatives:  516
True Negatives:  646, False Positives: 1192

Accuracy (%):                          27.87
Precision (%):                         1.16
Recall (%):                            2.64
F1-Score:                              1.61
----------------------------------------
```

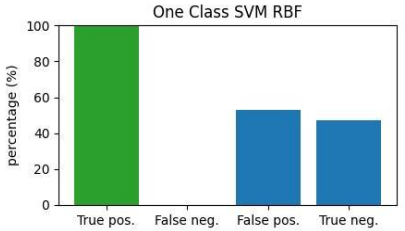
```
- Total of Anomalies for each method -
Num. Observações test dataset:     1765
Num. entrys from browsing:         1162
Num. entrys from DoS:               603
Percentage of DoS entrys:          34.2
Expected anomalys:                603.6


Centroids Distance:                 468
Centroids Distance PCA:             251
Multivariate PCA:                   664
SVM Linear:                         512
SVM Linear PCA:                     255
SVM RBF:                           1224
SVM RBF PCA:                       1228
SVM Poly:                           512
SVM Poly PCA:                       653
----------------------------------------
```

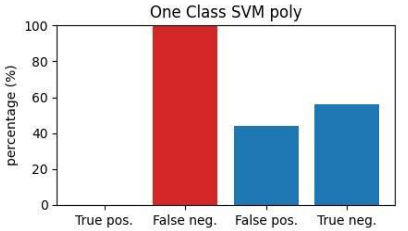


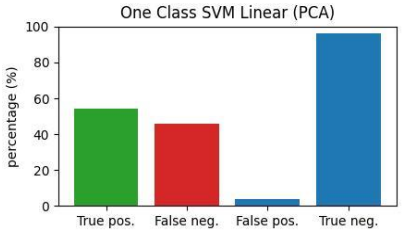


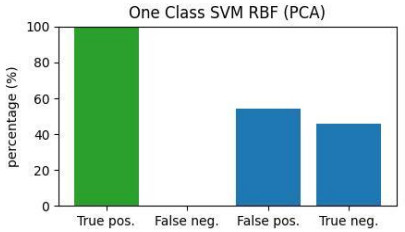


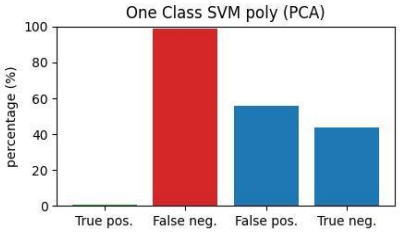












Results >> Window: 60 Slide: 10

```
-- Analysis of Centroids Distances --
True Positives:  592, False Negatives:  544
True Negatives:   32, False Positives:    0

Accuracy (%):                          53.42
Precision (%):                         100.0
Recall (%):                            52.11
F1-Score:                              68.52
----------------------------------------
```

```
-- Analysis of One Class SVM Linear --
True Positives:    0, False Negatives:  321
True Negatives:  255, False Positives:  592

Accuracy (%):                          21.83
Precision (%):                           0.0
Recall (%):                              0.0
F1-Score:                                  0
----------------------------------------
```

```
-- Analysis of One Class SVM RBF --
True Positives:  592, False Negatives:  232
True Negatives:  344, False Positives:    0

Accuracy (%):                          80.14
Precision (%):                         100.0
Recall (%):                            71.84
F1-Score:                              83.62
----------------------------------------
```

```
-- Analysis of One Class SVM Poly --
True Positives:    0, False Negatives:  321
True Negatives:  255, False Positives:  592

Accuracy (%):                          21.83
Precision (%):                           0.0
Recall (%):                              0.0
F1-Score:                                  0
----------------------------------------
```

```
-- Analysis of Centroids Distances (PCA) --
True Positives:  654, False Negatives: 1114
True Negatives:   48, False Positives:  552

Accuracy (%):                          29.65
Precision (%):                         54.23
Recall (%):                            36.99
F1-Score:                              43.98
----------------------------------------
```

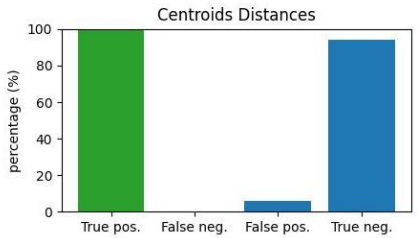
```
-- Analysis of One Class SVM Linear (PCA) --
True Positives:  273, False Negatives:  531
True Negatives:   45, False Positives:  319

Accuracy (%):                          27.23
Precision (%):                         46.11
Recall (%):                            33.96
F1-Score:                              39.11
----------------------------------------
```

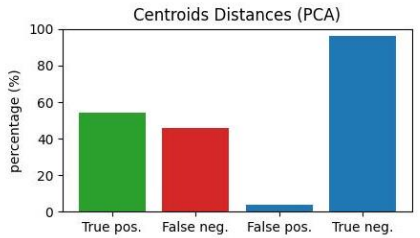
```
-- Analysis of One Class SVM RBF (PCA) --
True Positives:  592, False Negatives:  258
True Negatives:  318, False Positives:    0

Accuracy (%):                          77.91
Precision (%):                         100.0
Recall (%):                            69.65
F1-Score:                              82.11
----------------------------------------
```

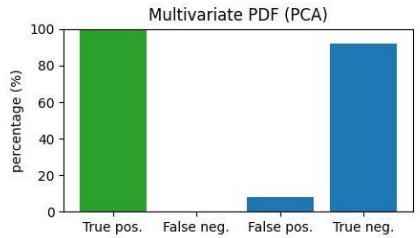
```
-- Analysis of One Class SVM poly (PCA) --
True Positives:    0, False Negatives:  298
True Negatives:  278, False Positives:  592

Accuracy (%):                          23.8
Precision (%):                          0.0
Recall (%):                             0.0
F1-Score:                                 0
----------------------------------------
```

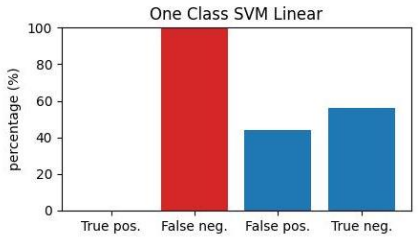
```
-- Analysis of Multivariate PDF (PCA) --
True Positives:  590, False Negatives:  529
True Negatives:   47, False Positives:    2

Accuracy (%):                          54.54
Precision (%):                         99.66
Recall (%):                            52.73
F1-Score:                              68.97
----------------------------------------
```

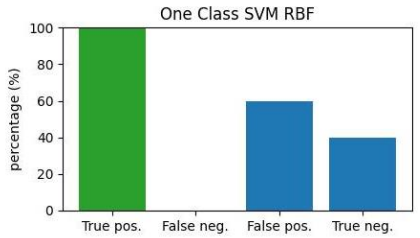
```
- Total of Anomalies for each method -
Num. Observações test dataset:     872
Num. entrys from browsing:         576
Num. entrys from DoS:              296
Percentage of DoS entrys:         33.9
Expected anomalys:               295.6


Centroids Distance:                328
Centroids Distance PCA:            122
Multivariate PCA:                  341
SVM Linear:                        255
SVM Linear PCA:                    243
SVM RBF:                           640
SVM RBF PCA:                       614
SVM Poly:                          255
SVM Poly PCA:                      278
----------------------------------------
```

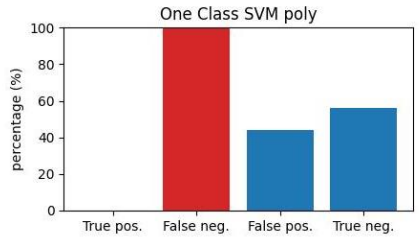


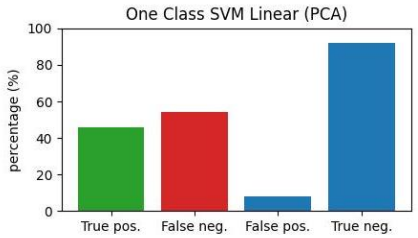


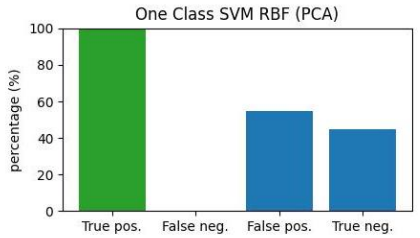


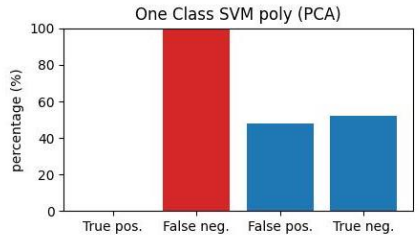






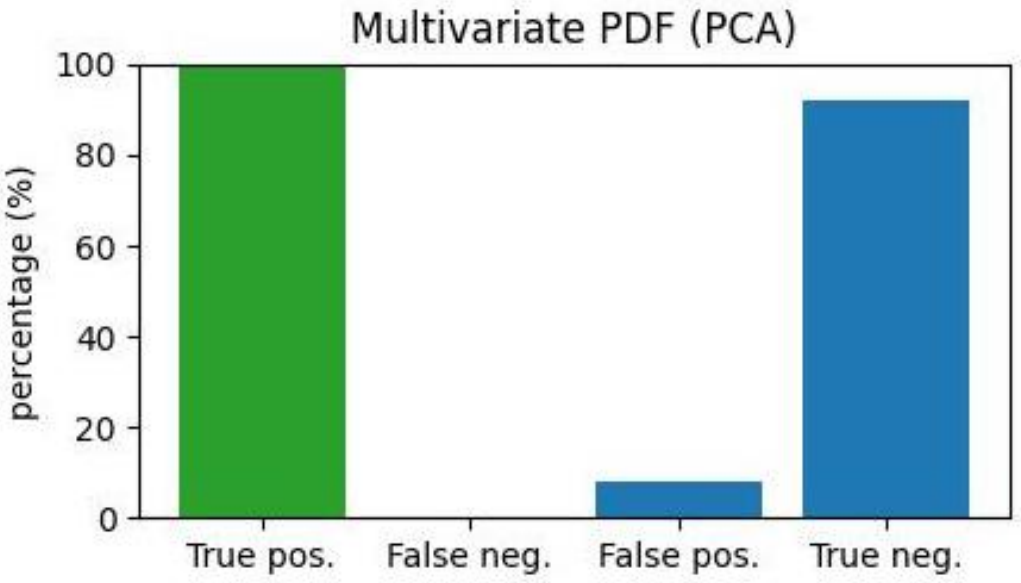






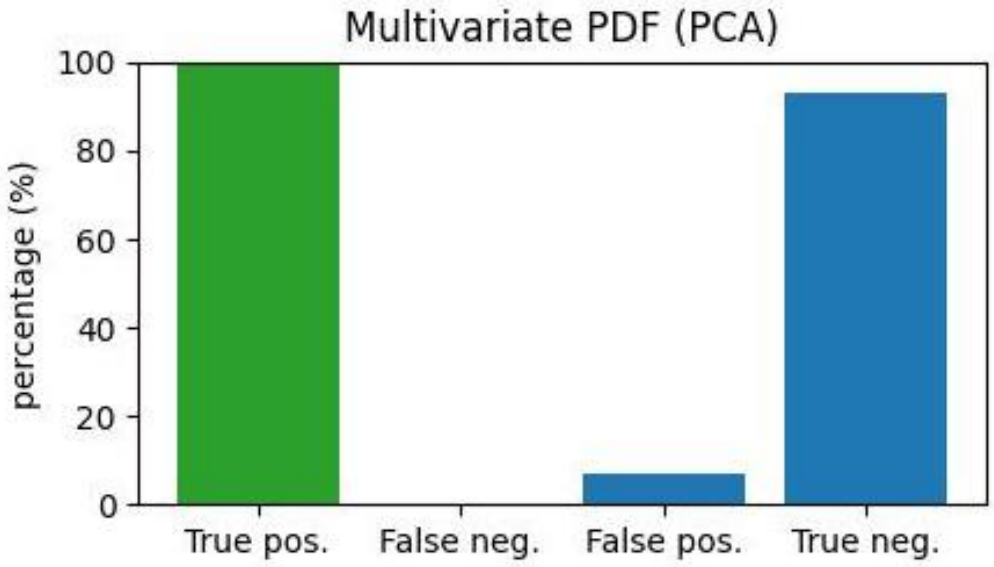
Results >> Window: 20 Slide: 5

PCA 4 components




```
-- Analysis of Multivariate PDF (PCA) --
True Positives: 1206, False Negatives: 1078
True Negatives:   84, False Positives:    0

Accuracy (%):                          54.48
Precision (%):                         100.0
Recall (%):                             52.8
F1-Score:                              69.11
-----------------------------------------
```

PCA 5 components




```
-- Analysis of Multivariate PDF (PCA) --
True Positives: 1206, False Negatives: 1073
True Negatives:   89, False Positives:    0

Accuracy (%):                          54.69
Precision (%):                         100.0
Recall (%):                            52.92
F1-Score:                              69.21
-----------------------------------------
```

Conclusions

- **Limitation:** the **website** service running in the server as only **static** contents that are loaded at once

- There **weren't detected** significant **changes** when the **number** of **PCA components varied**
- **Statistics methods** results were **better** than the **machine learning** ones
- From our perspective this happens due to the **determinism of DoS attacks**
- OneClass **SVM RBF** [PCA] was most **consistent** method in the **detection** of **anomalies** correctly (failed in legit traffic classification)
- The use of statistics approaches, namely, the **Multivariate PDF** with **PCA** revealed to be the **best choice**

DEMO

https://github.com/Torrakanor611/QUIC_Anomaly_Detection

QUESTIONS?

Thank you for your attention!