

Μηχανική Μάθηση



Intrusion Detection System with the power of ML

Φοιτητής: Κωνσταντάκος Δημήτρης
Επιβλέπων: Γιαννακόπουλος Θεόδωρος



Πίνακας Περιεχομένων

- Σύνολο Δεδομενων(Dataset)
- Επεξεργασία και προετοιμασία Δεδομένων
- Classifiers
- Αποτελέσματα
- Συμπεράσματα



Λίγα λόγια για το σύνολο δεδομένων

- Επιθέσεις TCP/IP προσομοιωμένες σε ένα στρατιωτικό δίκτυο LAN
- Χωρίζονται σε συνδέσεις
- Κλάση αναγνώρισης περιέχει το είδος σύνδεσης: Normal ή Anomalous
- Κάθε σύνδεση Περιέχει 100 bytes περίπου
- 41 αρχικά features έχουν εξαχθεί απο την κάθε σύνδεση



Στοιχεία για το dataset

Samples: 25192

-Class Normal: 13449

-Class Anomalous: 11743

-Imbalance difference 1706

Types of Data Features:

3 Categorical

15 Float quantitative

23 Int quantitative

Null Values:

None

Duplicates:

None



Data Preprocessing

- Categorical to Quantitive
- Scaling
- Outliers and features with no corrolation deletion
- Max corrolation features deletion
- Changes in Csv
- PCA when Needed
- Shuffling
- Correction of Imbalance



Classifiers

Decision Tree

```
modelDecisionTree=DecisionTreeClassifier(criterion='gini',max_depth=50,random_state=5,splitter='best')
```

SVM

```
modelSVC=SVC(kernel='poly',random_state=None,degree=1, gamma='scale', probability=True, decision_function_shape='ovo')
```

Quadratic

```
modelQuadratic=QuadraticDiscriminantAnalysis(store_covariance=True,reg_param=0.5)
```

Random forest

```
modelRandom=RandomForestClassifier(bootstrap=False,class_weight=None,criterion='entropy',max_depth=30,n_estimators=50,warm_start=True)
```

MLP

```
modelMLP=MLPClassifier(activation='relu', solver='adam',learning_rate='adaptive', max_iter=200,nesterovs_momentum=True)
```

Kneighbors

```
KNeighborsClassifier(n_neighbors=1,weights='uniform',algorithm='auto',n_jobs=1,leaf_size=1)
```

Results

