Comparative Analysis of Machine Learning Models for Network Intrusion Detection

Landrain, A.
Télécom SudParis, France

Konstantinos Karampidis, Giorgos Papadourakis
Hellenic Mediterranean University
Heraklion, Greece

Intrusion Detection

Network intrusion detection is a research domain aiming to identify malicious or unusual activities in computer networks.

Intrusion detection tend to plays a crucial role in the security of computer systems by detecting potential attacks and enabling proactive responses to them.

Conventional methods

- *Signature-based*
- *Anomaly-based*
- *Behavior-based methods.*

Methodology

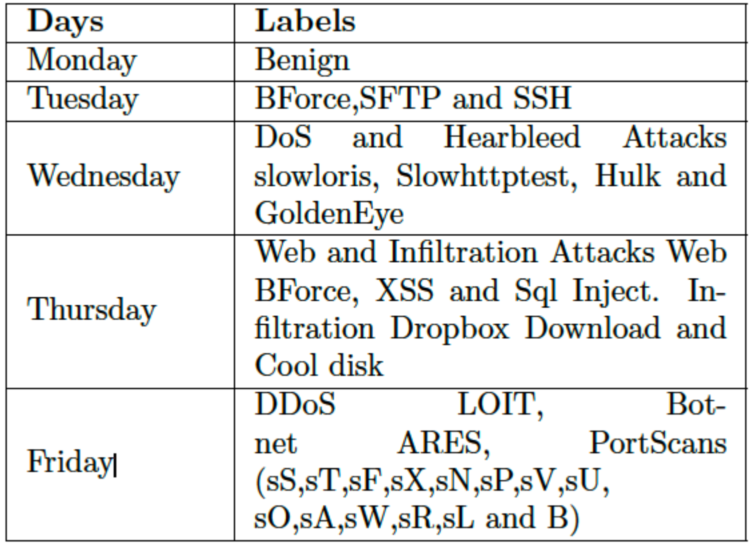
A benchmark dataset was chosen (CICIDS2017) so that the results could be comparable to other similar works.

Three different classifiers were utilized:

- Multi-Layer Perceptron (MLP)
- Support Vector Machine (SVM)
- Random Forest

Methodology – Dataset Description

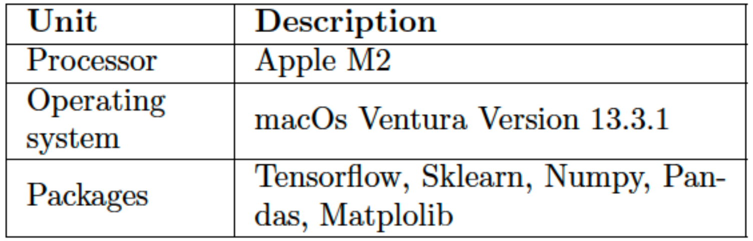
The CICIDS2017 dataset was built by researchers at the University of New Brunswick. It consists of a five-day capture of network activity. Every day a new type of attack is orchestrated as in the next table.



Days	Labels
Monday	Benign
Tuesday	BForce,SFTP and SSH
Wednesday	DoS and Hearbleed Attacks slowloris, Slowhttptest, Hulk and GoldenEye
Thursday	Web and Infiltration Attacks Web BForce, XSS and Sql Inject. Infiltration Dropbox Download and Cool disk
Friday	DDoS LOIT, Botnet ARES, PortScans (sS,sT,sF,sX,sN,sP,sV,sU, sO,sA,sW,sR,sL and B)

- 70% of the dataset was used as a training set and the rest 30% as a test set.

Experimental Setup

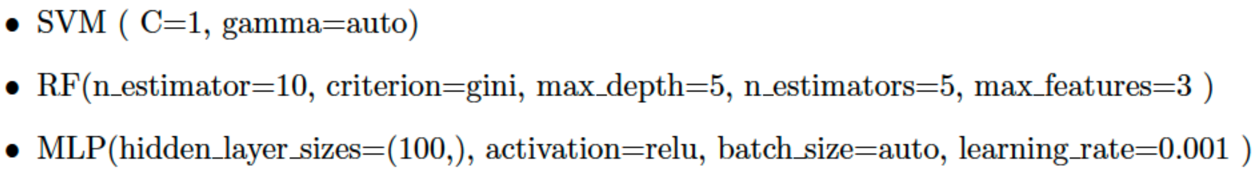


Unit	Description
Processor	Apple M2
Operating system	macOs Ventura Version 13.3.1
Packages	Tensorflow, Sklearn, Numpy, Pandas, Matplolib

Evaluation Metrics:

Accuracy
Precision & Recall
F1 Score

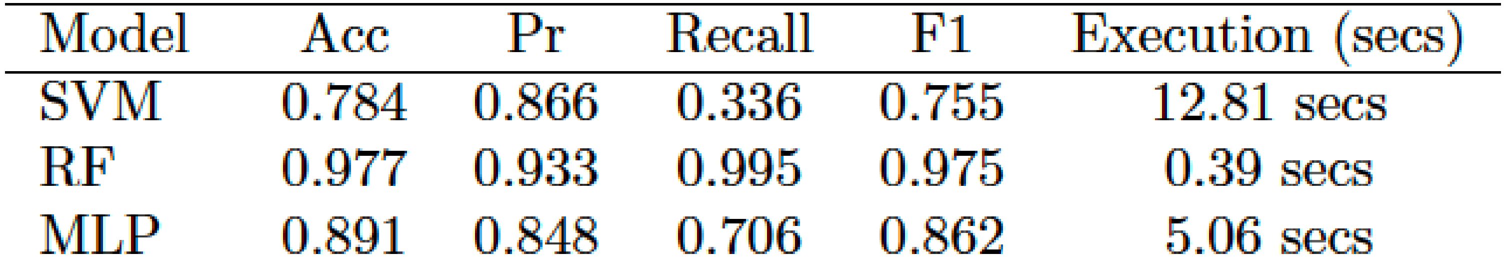
Models Parameters



- SVM (C=1, gamma=auto)
- RF(n_estimator=10, criterion=gini, max_depth=5, n_estimators=5, max_features=3)
- MLP(hidden_layer_sizes=(100,), activation=relu, batch_size=auto, learning_rate=0.001)

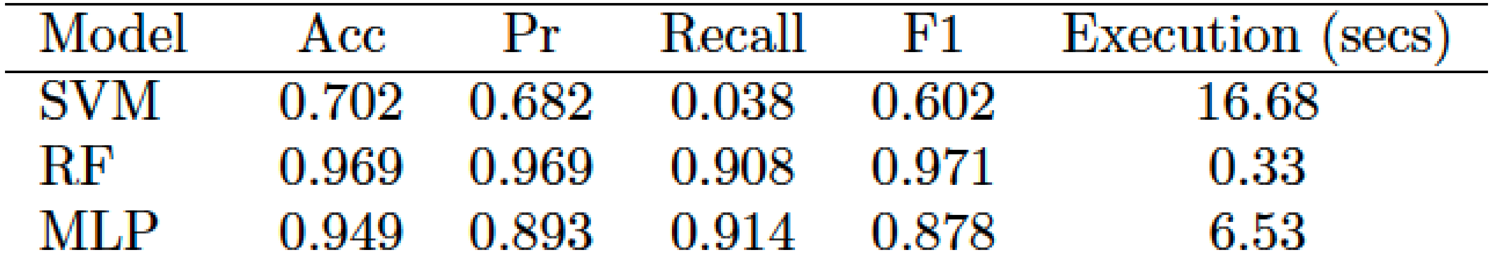
Experimental Results

Performance of Different Models over Botnet intrusion



Model	Acc	Pr	Recall	F1	Execution (secs)
SVM	0.784	0.866	0.336	0.755	12.81 secs
RF	0.977	0.933	0.995	0.975	0.39 secs
MLP	0.891	0.848	0.706	0.862	5.06 secs

Performance of Different Models over web-attacks



Model	Acc	Pr	Recall	F1	Execution (secs)
SVM	0.702	0.682	0.038	0.602	16.68
RF	0.969	0.969	0.908	0.971	0.33
MLP	0.949	0.893	0.914	0.878	6.53

Future work

- Compare our findings against other similar works
- Deploy Deep Learning models

Thank you!