FeatureImportance_Slowloris

June 28, 2021

[11]:
```
##############################################################################
# Random Forest Classification Model (TensorFlow)                            #
# For Slowloris Dataset                                                      #
# Based on the Implementation of:                                            #
# https://www.tensorflow.org/decision_forests/tutorials/beginner_colab       #
##############################################################################
```

[12]:
```
# Installieren aller benötigten Pakete
!pip install pandas
!pip install tensorflow_decision_forests
!pip install wurlitzer
!pip install matplotlib
!pip install ipython
```

```
Requirement already satisfied: pandas in /home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (1.2.5)
Requirement already satisfied: pytz>=2017.3 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from pandas)
(2021.1)
Requirement already satisfied: python-dateutil>=2.7.3 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from pandas)
(2.8.1)
Requirement already satisfied: numpy>=1.16.5 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from pandas)
(1.19.2)
Requirement already satisfied: six>=1.5 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from python-
dateutil>=2.7.3->pandas) (1.15.0)
Requirement already satisfied: tensorflow_decision_forests in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (0.1.7)
Requirement already satisfied: numpy in /home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorflow_decision_forests) (1.19.2)
```

```
Requirement already satisfied: absl-py in /home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorflow_decision_forests) (0.13.0)
Requirement already satisfied: wheel in /home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorflow_decision_forests) (0.35.0)
Requirement already satisfied: tensorflow~=2.5 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorflow_decision_forests) (2.5.0)
Requirement already satisfied: six in /home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorflow_decision_forests) (1.15.0)
Requirement already satisfied: pandas in /home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorflow_decision_forests) (1.2.5)
Requirement already satisfied: packaging>=20.2 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
wheel->tensorflow_decision_forests) (20.9)
Requirement already satisfied: typing-extensions~=3.7.4 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorflow~=2.5->tensorflow_decision_forests) (3.7.4.3)
Requirement already satisfied: astunparse~=1.6.3 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorflow~=2.5->tensorflow_decision_forests) (1.6.3)
Requirement already satisfied: protobuf>=3.9.2 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorflow~=2.5->tensorflow_decision_forests) (3.17.3)
Requirement already satisfied: flatbuffers~=1.12.0 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorflow~=2.5->tensorflow_decision_forests) (1.12)
Requirement already satisfied: grpcio~=1.34.0 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorflow~=2.5->tensorflow_decision_forests) (1.34.1)
Requirement already satisfied: keras-nightly~=2.5.0.dev in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorflow~=2.5->tensorflow_decision_forests) (2.5.0.dev2021032900)
Requirement already satisfied: tensorflow-estimator<2.6.0,>=2.5.0rc0 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorflow~=2.5->tensorflow_decision_forests) (2.5.0)
```

```
Requirement already satisfied: opt-einsum~=3.3.0 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorflow~=2.5->tensorflow_decision_forests) (3.3.0)
Requirement already satisfied: google-pasta~=0.2 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorflow~=2.5->tensorflow_decision_forests) (0.2.0)
Requirement already satisfied: keras-preprocessing~=1.1.2 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorflow~=2.5->tensorflow_decision_forests) (1.1.2)
Requirement already satisfied: wrapt~=1.12.1 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorflow~=2.5->tensorflow_decision_forests) (1.12.1)
Requirement already satisfied: gast==0.4.0 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorflow~=2.5->tensorflow_decision_forests) (0.4.0)
Requirement already satisfied: tensorboard~=2.5 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorflow~=2.5->tensorflow_decision_forests) (2.5.0)
Requirement already satisfied: termcolor~=1.1.0 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorflow~=2.5->tensorflow_decision_forests) (1.1.0)
Requirement already satisfied: h5py~=3.1.0 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorflow~=2.5->tensorflow_decision_forests) (3.1.0)
Requirement already satisfied: python-dateutil>=2.7.3 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
pandas->tensorflow_decision_forests) (2.8.1)
Requirement already satisfied: pytz>=2017.3 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
pandas->tensorflow_decision_forests) (2021.1)
Requirement already satisfied: pyparsing>=2.0.2 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
packaging>=20.2->wheel->tensorflow_decision_forests) (2.4.7)
Requirement already satisfied: google-auth-oauthlib<0.5,>=0.4.1 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorboard~=2.5->tensorflow~=2.5->tensorflow_decision_forests) (0.4.4)
```

```
Requirement already satisfied: tensorboard-data-server<0.7.0,>=0.6.0 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorboard~=2.5->tensorflow~=2.5->tensorflow_decision_forests) (0.6.1)
Requirement already satisfied: markdown>=2.6.8 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorboard~=2.5->tensorflow~=2.5->tensorflow_decision_forests) (3.3.4)
Requirement already satisfied: werkzeug>=0.11.15 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorboard~=2.5->tensorflow~=2.5->tensorflow_decision_forests) (2.0.1)
Requirement already satisfied: google-auth<2,>=1.6.3 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorboard~=2.5->tensorflow~=2.5->tensorflow_decision_forests) (1.32.0)
Requirement already satisfied: requests<3,>=2.21.0 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorboard~=2.5->tensorflow~=2.5->tensorflow_decision_forests) (2.25.1)
Requirement already satisfied: setuptools>=41.0.0 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorboard~=2.5->tensorflow~=2.5->tensorflow_decision_forests) (44.0.0)
Requirement already satisfied: tensorboard-plugin-wit>=1.6.0 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
tensorboard~=2.5->tensorflow~=2.5->tensorflow_decision_forests) (1.8.0)
Requirement already satisfied: requests-oauthlib>=0.7.0 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from google-auth-
oauthlib<0.5,>=0.4.1->tensorboard~=2.5->tensorflow~=2.5->tensorflow_decision_for
ests) (1.3.0)
Requirement already satisfied: rsa<5,>=3.1.4; python_version >= "3.6" in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from google-
auth<2,>=1.6.3->tensorboard~=2.5->tensorflow~=2.5->tensorflow_decision_forests)
(4.7.2)
Requirement already satisfied: cachetools<5.0,>=2.0.0 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from google-
auth<2,>=1.6.3->tensorboard~=2.5->tensorflow~=2.5->tensorflow_decision_forests)
(4.2.2)
Requirement already satisfied: pyasn1-modules>=0.2.1 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from google-
auth<2,>=1.6.3->tensorboard~=2.5->tensorflow~=2.5->tensorflow_decision_forests)
(0.2.8)
```

```
Requirement already satisfied: idna<3,>=2.5 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from requests<3,>
=2.21.0->tensorboard~=2.5->tensorflow~=2.5->tensorflow_decision_forests) (2.10)
Requirement already satisfied: certifi>=2017.4.17 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from requests<3,>
=2.21.0->tensorboard~=2.5->tensorflow~=2.5->tensorflow_decision_forests)
(2021.5.30)
Requirement already satisfied: chardet<5,>=3.0.2 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from requests<3,>
=2.21.0->tensorboard~=2.5->tensorflow~=2.5->tensorflow_decision_forests) (4.0.0)
Requirement already satisfied: urllib3<1.27,>=1.21.1 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from requests<3,>
=2.21.0->tensorboard~=2.5->tensorflow~=2.5->tensorflow_decision_forests)
(1.26.6)
Requirement already satisfied: oauthlib>=3.0.0 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from requests-
oauthlib>=0.7.0->google-auth-oauthlib<0.5,>=0.4.1->tensorboard~=2.5->tensorflow~
=2.5->tensorflow_decision_forests) (3.1.1)
Requirement already satisfied: pyasn1>=0.1.3 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
rsa<5,>=3.1.4; python_version >= "3.6"->google-
auth<2,>=1.6.3->tensorboard~=2.5->tensorflow~=2.5->tensorflow_decision_forests)
(0.4.8)
Requirement already satisfied: wurlitzer in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (2.1.0)
Requirement already satisfied: matplotlib in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (3.4.2)
Requirement already satisfied: pillow>=6.2.0 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from matplotlib)
(8.2.0)
Requirement already satisfied: numpy>=1.16 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from matplotlib)
(1.19.2)
Requirement already satisfied: python-dateutil>=2.7 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from matplotlib)
(2.8.1)
Requirement already satisfied: kiwisolver>=1.0.1 in
```

```
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from matplotlib)
(1.3.1)
Requirement already satisfied: pyparsing>=2.2.1 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from matplotlib)
(2.4.7)
Requirement already satisfied: cycler>=0.10 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from matplotlib)
(0.10.0)
Requirement already satisfied: six>=1.5 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from python-
dateutil>=2.7->matplotlib) (1.15.0)
Requirement already satisfied: ipython in /home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (7.25.0)
Requirement already satisfied: setuptools>=18.5 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from ipython)
(44.0.0)
Requirement already satisfied: traitlets>=4.2 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from ipython)
(5.0.5)
Requirement already satisfied: pexpect>4.3; sys_platform != "win32" in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from ipython)
(4.8.0)
Requirement already satisfied: pygments in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from ipython)
(2.9.0)
Requirement already satisfied: decorator in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from ipython)
(5.0.9)
Requirement already satisfied: pickleshare in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from ipython)
(0.7.5)
Requirement already satisfied: backcall in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from ipython)
(0.2.0)
Requirement already satisfied: jedi>=0.16 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from ipython)
```

```
(0.18.0)
Requirement already satisfied: prompt-toolkit!=3.0.0,!=3.0.1,<3.1.0,>=2.0.0 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from ipython)
(3.0.19)
Requirement already satisfied: matplotlib-inline in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from ipython)
(0.1.2)
Requirement already satisfied: ipython-genutils in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
traitlets>=4.2->ipython) (0.2.0)
Requirement already satisfied: ptyprocess>=0.5 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from pexpect>4.3;
sys_platform != "win32"->ipython) (0.7.0)
Requirement already satisfied: parso<0.9.0,>=0.8.0 in
/home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from
jedi>=0.16->ipython) (0.8.2)
Requirement already satisfied: wcwidth in /home/julianbuecher/Projects/Bachelor-
Thesis/ML.Proxy.FeatureImportance/lib/python3.8/site-packages (from prompt-
toolkit!=3.0.0,!=3.0.1,<3.1.0,>=2.0.0->ipython) (0.2.5)
```

[13]:
```python
# Laden der benötigten Python Pakete
import pandas as pd
import numpy as np
import tensorflow_decision_forests as tfdf
from wurlitzer import sys_pipes
import matplotlib.pyplot as plt
```

[14]:
```python
# Prüfung der installierten TensorFlow Decision Forests Version
print(f"Found TensorFlow Decision Forests v{tfdf.__version__}")
```

```
Found TensorFlow Decision Forests v0.1.7
```

[15]:
```python
# Laden der Netzwerk Traffic Daten für den GoldenEye Angriff
data_Slowloris = pd.read_csv('../Data/Optimized/
 ↪Thursday-15-02-2018_Slowloris-Attack.csv')
```

[16]:
```python
# Suchen und Ersetzen von NaN Werten im Dataset
nan_count = data_Slowloris.isna().sum().sum()
print(f"Initial Count of NaN in Dataset: {nan_count}")

data_Slowloris = data_Slowloris.replace([np.inf, -np.inf], np.nan)
data_Slowloris = data_Slowloris.interpolate()
```

```
nan_count = data_Slowloris.isna().sum().sum()
print(f"Count of NaN in Dataset after Cleanse: {nan_count}")
```

```
Initial Count of NaN in Dataset: 4921
Count of NaN in Dataset after Cleanse: 0
```

[17]:
```
# Festlegen des Wertes der bestimmten Variable
label = 'label'
```

[18]:
```
# Aufteilen des Datasets in Training- und Test-Daten
def split_dataset(dataset,  test_ratio=0.30):
    """Splits a panda dataframe in two dataframes."""
    test_indices = np.random.rand(len(dataset)) < test_ratio
    return dataset[~test_indices], dataset[test_indices]

training_data_Slowloris, testing_data_Slowloris = split_dataset(data_Slowloris)

print("{} examples in training, {} examples for testing.".format(
    len(training_data_Slowloris), len(testing_data_Slowloris)))
```

```
704941 examples in training, 302126 examples for testing.
```

[19]:
```
# Konvertieren des Panda Dataframes in ein TensorFlow Dataset
print("Converting Panda Dataframe into TensorFlow Dataset...")
training_dataset_Slowloris = tfdf.keras.
 ↪pd_dataframe_to_tf_dataset(training_data_Slowloris, label=label)
testing_dataset_Slowloris = tfdf.keras.
 ↪pd_dataframe_to_tf_dataset(testing_data_Slowloris, label=label)
```

```
Converting Panda Dataframe into TensorFlow Dataset…
```

[20]:
```
# Erstellen des Random Forest Modells
model = tfdf.keras.RandomForestModel()
model.compile(metrics=["accuracy"])
```

[21]:
```
# Trainieren des Modells
print("Training the Model: ")
with sys_pipes():
    model.fit(x=training_dataset_Slowloris)
```

```
Training the Model:
11015/11015 [==============================] - 63s 6ms/step
[INFO kernel.cc:746] Start Yggdrasil model training
[INFO kernel.cc:747] Collect training examples
[INFO kernel.cc:392] Number of batches: 11015
[INFO kernel.cc:393] Number of examples: 704941
[INFO data_spec_inference.cc:289] 31737 item(s) have been pruned (i.e. they are
```

```
considered out of dictionary) for the column timestamp (2000 item(s) left)
because min_value_count=5 and max_number_of_unique_values=2000
[INFO kernel.cc:769] Dataset:
Number of records: 704941
Number of columns: 80

Number of columns by type:
        NUMERICAL: 78 (97.5%)
        CATEGORICAL: 2 (2.5%)

Columns:

NUMERICAL: 78 (97.5%)
        0: "ack_flag_cnt" NUMERICAL mean:0.283114 min:0 max:1 sd:0.450512
        1: "active_max" NUMERICAL mean:182167 min:0 max:1.11992e+08
sd:1.20938e+06
        2: "active_mean" NUMERICAL mean:111171 min:0 max:1.11992e+08 sd:950296
        3: "active_min" NUMERICAL mean:81805.5 min:0 max:1.11992e+08 sd:871158
        4: "active_std" NUMERICAL mean:49027.7 min:0 max:6.01771e+07 sd:379077
        5: "bwd_blk_rate_avg" NUMERICAL mean:0 min:0 max:0 sd:0
        6: "bwd_byts/b_avg" NUMERICAL mean:0 min:0 max:0 sd:0
        7: "bwd_header_len" NUMERICAL mean:135.282 min:0 max:379492 sd:1931.16
        8: "bwd_iat_max" NUMERICAL mean:3.68954e+06 min:0 max:1.19714e+08
sd:1.30593e+07
        9: "bwd_iat_mean" NUMERICAL mean:1.41581e+06 min:0 max:1.19714e+08
sd:7.47293e+06
        10: "bwd_iat_min" NUMERICAL mean:679332 min:0 max:1.19714e+08
sd:6.60057e+06
        11: "bwd_iat_std" NUMERICAL mean:1.15221e+06 min:0 max:8.45025e+07
sd:4.20646e+06
        12: "bwd_iat_tot" NUMERICAL mean:1.02694e+07 min:0 max:1.2e+08
sd:2.99989e+07
        13: "bwd_pkt_len_max" NUMERICAL mean:320.72 min:0 max:2708 sd:493.76
        14: "bwd_pkt_len_mean" NUMERICAL mean:118.86 min:0 max:1457.94
sd:186.594
        15: "bwd_pkt_len_min" NUMERICAL mean:35.029 min:0 max:1176 sd:56.3532
        16: "bwd_pkt_len_std" NUMERICAL mean:113.145 min:0 max:931.26 sd:202.496
        17: "bwd_pkts/b_avg" NUMERICAL mean:0 min:0 max:0 sd:0
        18: "bwd_pkts/s" NUMERICAL mean:3789.02 min:0 max:2e+06 sd:44967.2
        19: "bwd_psh_flags" NUMERICAL mean:0 min:0 max:0 sd:0
        20: "bwd_seg_size_avg" NUMERICAL mean:118.86 min:0 max:1457.94
sd:186.594
        21: "bwd_urg_flags" NUMERICAL mean:0 min:0 max:0 sd:0
        22: "cwe_flag_count" NUMERICAL mean:0 min:0 max:0 sd:0
        23: "down/up_ratio" NUMERICAL mean:0.583372 min:0 max:126 sd:0.746481
        24: "dst_port" NUMERICAL mean:7704.81 min:0 max:65534 sd:17846.1
        25: "ece_flag_cnt" NUMERICAL mean:0.0635358 min:0 max:1 sd:0.243924
        26: "fin_flag_cnt" NUMERICAL mean:0.00608703 min:0 max:1 sd:0.0777816
```

```
        27: "flow_byts/s" NUMERICAL mean:443755 min:0 max:9.12e+08
sd:5.29728e+06
        28: "flow_duration" NUMERICAL mean:1.44381e+07 min:0 max:1.2e+08
sd:3.38551e+07
        29: "flow_iat_max" NUMERICAL mean:6.66201e+06 min:0 max:1.19992e+08
sd:1.73406e+07
        30: "flow_iat_mean" NUMERICAL mean:2.93892e+06 min:0 max:1.19992e+08
sd:1.12358e+07
        31: "flow_iat_min" NUMERICAL mean:2.29248e+06 min:0 max:1.19992e+08
sd:1.10278e+07
        32: "flow_iat_std" NUMERICAL mean:1.41179e+06 min:0 max:8.43107e+07
sd:5.13121e+06
        33: "flow_pkts/s" NUMERICAL mean:44763.7 min:0.0166678 max:4e+06
sd:269344
        34: "fwd_act_data_pkts" NUMERICAL mean:1.92331 min:0 max:1468 sd:5.7925
        35: "fwd_blk_rate_avg" NUMERICAL mean:0 min:0 max:0 sd:0
        36: "fwd_byts/b_avg" NUMERICAL mean:0 min:0 max:0 sd:0
        37: "fwd_header_len" NUMERICAL mean:105.033 min:0 max:204920 sd:823.22
        38: "fwd_iat_max" NUMERICAL mean:6.36229e+06 min:0 max:1.19992e+08
sd:1.71809e+07
        39: "fwd_iat_mean" NUMERICAL mean:3.48917e+06 min:0 max:1.19992e+08
sd:1.24199e+07
        40: "fwd_iat_min" NUMERICAL mean:2.65785e+06 min:0 max:1.19992e+08
sd:1.2318e+07
        41: "fwd_iat_std" NUMERICAL mean:1.3764e+06 min:0 max:8.43894e+07
sd:4.72503e+06
        42: "fwd_iat_tot" NUMERICAL mean:1.40196e+07 min:0 max:1.2e+08
sd:3.37546e+07
        43: "fwd_pkt_len_max" NUMERICAL mean:146.036 min:0 max:64440 sd:270.909
        44: "fwd_pkt_len_mean" NUMERICAL mean:43.5759 min:0 max:16529.3
sd:57.7645
        45: "fwd_pkt_len_min" NUMERICAL mean:14.5419 min:0 max:1460 sd:23.8856
        46: "fwd_pkt_len_std" NUMERICAL mean:47.2455 min:0 max:18401.6
sd:87.9603
        47: "fwd_pkts/b_avg" NUMERICAL mean:0 min:0 max:0 sd:0
        48: "fwd_pkts/s" NUMERICAL mean:38382.8 min:0 max:4e+06 sd:255230
        49: "fwd_psh_flags" NUMERICAL mean:0.0536272 min:0 max:1 sd:0.225281
        50: "fwd_seg_size_avg" NUMERICAL mean:43.5759 min:0 max:16529.3
sd:57.7645
        51: "fwd_seg_size_min" NUMERICAL mean:15.9548 min:0 max:56 sd:6.92459
        52: "fwd_urg_flags" NUMERICAL mean:0 min:0 max:0 sd:0
        53: "idle_max" NUMERICAL mean:4.47742e+06 min:0 max:1.19992e+08
sd:1.47679e+07
        54: "idle_mean" NUMERICAL mean:4.2012e+06 min:0 max:1.19992e+08
sd:1.40996e+07
        55: "idle_min" NUMERICAL mean:3.95608e+06 min:0 max:1.19992e+08
sd:1.38471e+07
        56: "idle_std" NUMERICAL mean:273348 min:0 max:6.81937e+07
```

```
sd:2.38528e+06
        57: "init_bwd_win_byts" NUMERICAL mean:5821.24 min:-1 max:65535
sd:17432.4
        58: "init_fwd_win_byts" NUMERICAL mean:4712.16 min:-1 max:65535
sd:10111.8
        59: "pkt_len_max" NUMERICAL mean:330.349 min:0 max:64440 sd:509.607
        60: "pkt_len_mean" NUMERICAL mean:79.1216 min:0 max:3326.99 sd:119.921
        61: "pkt_len_min" NUMERICAL mean:14.3694 min:0 max:1460 sd:22.6913
        62: "pkt_len_std" NUMERICAL mean:105.728 min:0 max:10579.8 sd:162.827
        63: "pkt_len_var" NUMERICAL mean:37690.8 min:0 max:1.11932e+08 sd:169145
        64: "pkt_size_avg" NUMERICAL mean:92.3922 min:0 max:3328.3 sd:123.421
        65: "protocol" NUMERICAL mean:9.66535 min:0 max:17 sd:5.3622
        66: "psh_flag_cnt" NUMERICAL mean:0.351532 min:0 max:1 sd:0.477449
        67: "rst_flag_cnt" NUMERICAL mean:0.0635387 min:0 max:1 sd:0.243929
        68: "subflow_bwd_byts" NUMERICAL mean:5002.94 min:0 max:2.7425e+07
sd:137460
        69: "subflow_bwd_pkts" NUMERICAL mean:6.51502 min:0 max:18974 sd:96.2729
        70: "subflow_fwd_byts" NUMERICAL mean:431.849 min:0 max:8.73731e+06
sd:28518
        71: "subflow_fwd_pkts" NUMERICAL mean:5.20759 min:1 max:8832 sd:34.989
        72: "syn_flag_cnt" NUMERICAL mean:0.0536272 min:0 max:1 sd:0.225281
        74: "tot_bwd_pkts" NUMERICAL mean:6.51502 min:0 max:18974 sd:96.2729
        75: "tot_fwd_pkts" NUMERICAL mean:5.20759 min:1 max:8832 sd:34.989
        76: "totlen_bwd_pkts" NUMERICAL mean:5002.94 min:0 max:2.7425e+07
sd:137460
        77: "totlen_fwd_pkts" NUMERICAL mean:431.849 min:0 max:8.73731e+06
sd:28518
        78: "urg_flag_cnt" NUMERICAL mean:0.0496155 min:0 max:1 sd:0.217149

CATEGORICAL: 2 (2.5%)
        73: "timestamp" CATEGORICAL has-dict vocab-size:2001 num-oods:31737
(4.50208%) most-frequent:"<OOD>" 31737 (4.50208%)
        79: "__LABEL" CATEGORICAL integerized vocab-size:3 no-ood-item

Terminology:
        nas: Number of non-available (i.e. missing) values.
        ood: Out of dictionary.
        manually-defined: Attribute which type is manually defined by the user
i.e. the type was not automatically inferred.
        tokenized: The attribute value is obtained through tokenization.
        has-dict: The attribute is attached to a string dictionary e.g. a
categorical attribute stored as a string.
        vocab-size: Number of unique values.

[INFO kernel.cc:772] Configure learner
[INFO kernel.cc:797] Training config:
learner: "RANDOM_FOREST"
features: "ack_flag_cnt"
```

```
features: "active_max"
features: "active_mean"
features: "active_min"
features: "active_std"
features: "bwd_blk_rate_avg"
features: "bwd_byts/b_avg"
features: "bwd_header_len"
features: "bwd_iat_max"
features: "bwd_iat_mean"
features: "bwd_iat_min"
features: "bwd_iat_std"
features: "bwd_iat_tot"
features: "bwd_pkt_len_max"
features: "bwd_pkt_len_mean"
features: "bwd_pkt_len_min"
features: "bwd_pkt_len_std"
features: "bwd_pkts/b_avg"
features: "bwd_pkts/s"
features: "bwd_psh_flags"
features: "bwd_seg_size_avg"
features: "bwd_urg_flags"
features: "cwe_flag_count"
features: "down/up_ratio"
features: "dst_port"
features: "ece_flag_cnt"
features: "fin_flag_cnt"
features: "flow_byts/s"
features: "flow_duration"
features: "flow_iat_max"
features: "flow_iat_mean"
features: "flow_iat_min"
features: "flow_iat_std"
features: "flow_pkts/s"
features: "fwd_act_data_pkts"
features: "fwd_blk_rate_avg"
features: "fwd_byts/b_avg"
features: "fwd_header_len"
features: "fwd_iat_max"
features: "fwd_iat_mean"
features: "fwd_iat_min"
features: "fwd_iat_std"
features: "fwd_iat_tot"
features: "fwd_pkt_len_max"
features: "fwd_pkt_len_mean"
features: "fwd_pkt_len_min"
features: "fwd_pkt_len_std"
features: "fwd_pkts/b_avg"
features: "fwd_pkts/s"
```

```
features: "fwd_psh_flags"
features: "fwd_seg_size_avg"
features: "fwd_seg_size_min"
features: "fwd_urg_flags"
features: "idle_max"
features: "idle_mean"
features: "idle_min"
features: "idle_std"
features: "init_bwd_win_byts"
features: "init_fwd_win_byts"
features: "pkt_len_max"
features: "pkt_len_mean"
features: "pkt_len_min"
features: "pkt_len_std"
features: "pkt_len_var"
features: "pkt_size_avg"
features: "protocol"
features: "psh_flag_cnt"
features: "rst_flag_cnt"
features: "subflow_bwd_byts"
features: "subflow_bwd_pkts"
features: "subflow_fwd_byts"
features: "subflow_fwd_pkts"
features: "syn_flag_cnt"
features: "timestamp"
features: "tot_bwd_pkts"
features: "tot_fwd_pkts"
features: "totlen_bwd_pkts"
features: "totlen_fwd_pkts"
features: "urg_flag_cnt"
label: "__LABEL"
task: CLASSIFICATION
[yggdrasil_decision_forests.model.random_forest.proto.random_forest_config] {
  num_trees: 300
  decision_tree {
    max_depth: 16
    min_examples: 5
    in_split_min_examples_check: true
    missing_value_policy: GLOBAL_IMPUTATION
    allow_na_conditions: false
    categorical_set_greedy_forward {
      sampling: 0.1
      max_num_items: -1
      min_item_frequency: 1
    }
    growing_strategy_local {
    }
    categorical {
```

```
      cart {
      }
    }
    num_candidate_attributes_ratio: -1
    axis_aligned_split {
    }
    internal {
      sorting_strategy: PRESORTED
    }
  }
  winner_take_all_inference: true
  compute_oob_performances: true
  compute_oob_variable_importances: false
  adapt_bootstrap_size_ratio_for_maximum_training_duration: false
}

[INFO kernel.cc:800] Deployment config:

[INFO kernel.cc:837] Train model
[INFO random_forest.cc:303] Training random forest on 704941 example(s) and 79
feature(s).
[INFO random_forest.cc:578] Training of tree  1/300 (tree index:4) done
accuracy:0.999958 logloss:0.00152823
[INFO random_forest.cc:578] Training of tree  11/300 (tree index:8) done
accuracy:0.999974 logloss:0.000371098
[INFO random_forest.cc:578] Training of tree  21/300 (tree index:21) done
accuracy:0.999984 logloss:0.000116897
[INFO random_forest.cc:578] Training of tree  31/300 (tree index:29) done
accuracy:0.999984 logloss:6.43326e-05
[INFO random_forest.cc:578] Training of tree  41/300 (tree index:40) done
accuracy:0.999986 logloss:6.26781e-05
[INFO random_forest.cc:578] Training of tree  51/300 (tree index:49) done
accuracy:0.999987 logloss:6.16098e-05
[INFO random_forest.cc:578] Training of tree  61/300 (tree index:59) done
accuracy:0.999987 logloss:5.90725e-05
[INFO random_forest.cc:578] Training of tree  71/300 (tree index:73) done
accuracy:0.999989 logloss:5.90699e-05
[INFO random_forest.cc:578] Training of tree  81/300 (tree index:79) done
accuracy:0.999987 logloss:5.93677e-05
[INFO random_forest.cc:578] Training of tree  91/300 (tree index:90) done
accuracy:0.999989 logloss:5.82467e-05
[INFO random_forest.cc:578] Training of tree  101/300 (tree index:99) done
accuracy:0.999989 logloss:5.72201e-05
[INFO random_forest.cc:578] Training of tree  111/300 (tree index:110) done
accuracy:0.999991 logloss:5.76986e-05
[INFO random_forest.cc:578] Training of tree  121/300 (tree index:122) done
accuracy:0.99999 logloss:5.72194e-05
[INFO random_forest.cc:578] Training of tree  131/300 (tree index:129) done
```

```
accuracy:0.99999 logloss:5.82669e-05
[INFO random_forest.cc:578] Training of tree  141/300 (tree index:140) done
accuracy:0.999989 logloss:5.85682e-05
[INFO random_forest.cc:578] Training of tree  151/300 (tree index:150) done
accuracy:0.99999 logloss:5.92311e-05
[INFO random_forest.cc:578] Training of tree  161/300 (tree index:160) done
accuracy:0.99999 logloss:5.92355e-05
[INFO random_forest.cc:578] Training of tree  171/300 (tree index:168) done
accuracy:0.999989 logloss:6.00446e-05
[INFO random_forest.cc:578] Training of tree  181/300 (tree index:180) done
accuracy:0.999991 logloss:6.05264e-05
[INFO random_forest.cc:578] Training of tree  191/300 (tree index:190) done
accuracy:0.999986 logloss:6.01335e-05
[INFO random_forest.cc:578] Training of tree  201/300 (tree index:200) done
accuracy:0.999984 logloss:6.08181e-05
[INFO random_forest.cc:578] Training of tree  211/300 (tree index:209) done
accuracy:0.999987 logloss:6.05704e-05
[INFO random_forest.cc:578] Training of tree  221/300 (tree index:218) done
accuracy:0.999987 logloss:6.02536e-05
[INFO random_forest.cc:578] Training of tree  231/300 (tree index:231) done
accuracy:0.999989 logloss:5.98425e-05
[INFO random_forest.cc:578] Training of tree  241/300 (tree index:240) done
accuracy:0.999987 logloss:5.97918e-05
[INFO random_forest.cc:578] Training of tree  251/300 (tree index:251) done
accuracy:0.99999 logloss:5.97172e-05
[INFO random_forest.cc:578] Training of tree  261/300 (tree index:258) done
accuracy:0.99999 logloss:5.98936e-05
[INFO random_forest.cc:578] Training of tree  271/300 (tree index:270) done
accuracy:0.999989 logloss:6.01438e-05
[INFO random_forest.cc:578] Training of tree  281/300 (tree index:279) done
accuracy:0.999989 logloss:6.02035e-05
[INFO random_forest.cc:578] Training of tree  291/300 (tree index:288) done
accuracy:0.999989 logloss:6.03442e-05
[INFO random_forest.cc:578] Training of tree  300/300 (tree index:299) done
accuracy:0.999989 logloss:5.98876e-05
[INFO random_forest.cc:645] Final OOB metrics: accuracy:0.999989
logloss:5.98876e-05
[INFO kernel.cc:856] Export model in log directory: /tmp/tmpz7mqurqp
[INFO kernel.cc:864] Save model in resources
[INFO kernel.cc:960] Loading model from path
[INFO decision_forest.cc:590] Model loaded with 300 root(s), 27116 node(s), and
67 input feature(s).
[INFO abstract_model.cc:973] Engine "RandomForestGeneric" built
[INFO kernel.cc:820] Use fast generic engine
```

[22]:
```python
# Evaluation des trainierten Modells mit den Testdaten
print("Evaluating the Model...")
```

```
evaluation = model.evaluate(testing_dataset_Slowloris, return_dict=True)

print()

for name, value in evaluation.items():
    print(f"{name}: {value:.4f}")
```

```
Evaluating the Model…
4721/4721 [==============================] - 30s 6ms/step - loss: 0.0000e+00 -
accuracy: 1.0000

loss: 0.0000
accuracy: 1.0000
```

[23]:
```
# Erstellen einer Bilanz für das trainierte Modell
model.summary()
```

```
4.          "protocol"  7.225300 ###############
   15. "fwd_act_data_pkts"  7.219609 ###############
   16.      "urg_flag_cnt"  7.210363 ###############
   17.   "bwd_pkt_len_min"  7.197026 ###############
   18.     "down/up_ratio"  7.194212 ###############
   19.       "pkt_len_min"  7.191280 ###############
   20.      "psh_flag_cnt"  7.180366 ###############
   21.      "tot_bwd_pkts"  7.172341 ###############
   22.  "subflow_fwd_pkts"  7.170572 ###############
   23.   "fwd_pkt_len_std"  7.167852 ###############
   24.   "bwd_pkt_len_std"  7.161721 ###############
   25.  "subflow_bwd_pkts"  7.156462 ###############
   26.      "tot_fwd_pkts"  7.152198 ###############
   27.         "timestamp"  7.150396 ###############
   28.       "bwd_iat_tot"  7.139798 ###############
   29.          "idle_max"  7.101867 ###############
   30.          "idle_min"  7.085014 ##############
   31.      "syn_flag_cnt"  7.080036 ##############
   32.    "bwd_header_len"  7.066946 ##############
   33.     "fwd_psh_flags"  7.064813 ##############
   34.        "active_std"  7.062241 ##############
   35.       "pkt_len_max"  7.036115 ##############
   36.      "pkt_len_mean"  7.016146 ##############
   37.  "bwd_seg_size_avg"  6.997092 ##############
   38. "init_bwd_win_byts"  6.995345 ##############
   39.      "ack_flag_cnt"  6.992150 ##############
   40.       "pkt_len_std"  6.985186 ##############
   41.       "pkt_len_var"  6.970307 ##############
   42.  "subflow_fwd_byts"  6.966463 ##############
   43.         "idle_mean"  6.962201 ##############
   44.   "totlen_bwd_pkts"  6.956871 ##############
```

```
45.   "bwd_pkt_len_max"  6.945252 #############
46.  "subflow_bwd_byts"  6.927178 #############
47.      "pkt_size_avg"  6.922550 #############
48.        "active_min"  6.918933 #############
49.   "fwd_pkt_len_min"  6.914335 #############
50.  "bwd_pkt_len_mean"  6.902844 #############
51.       "fwd_iat_std"  6.873784 #############
52.          "idle_std"  6.872637 #############
53.   "totlen_fwd_pkts"  6.863553 #############
54.      "fin_flag_cnt"  6.848130 #############
55.   "fwd_pkt_len_max"  6.819533 #############
56.       "active_mean"  6.818260 #############
57.        "active_max"  6.813350 #############
58.  "fwd_pkt_len_mean"  6.807699 #############
59.  "fwd_seg_size_avg"  6.741335 ############
60.       "flow_byts/s"  6.707868 ############
61.        "bwd_pkts/s"  6.687029 ############
62.       "fwd_iat_tot"  6.643890 ###########
63.    "fwd_header_len"  6.640266 ###########
64.     "flow_duration"  6.511651 ##########
65.       "bwd_iat_std"  6.511062 ##########
66.     "flow_iat_mean"  6.435049 ##########
67.      "flow_iat_min"  6.384849 ##########
68.       "fwd_iat_max"  6.369104 #########
69.      "flow_iat_max"  6.352430 #########
70.      "fwd_iat_mean"  6.345549 #########
71.       "fwd_iat_min"  6.204718 ########
72.          "dst_port"  6.178456 ########
73.        "fwd_pkts/s"  6.172157 ########
74.       "flow_pkts/s"  6.170163 ########
75.       "bwd_iat_min"  6.159928 ########
76.      "flow_iat_std"  6.107963 ########
77.      "bwd_iat_mean"  5.994053 #######
78.       "bwd_iat_max"  5.797237 ######
79. "init_fwd_win_byts"  5.058868
80.  "fwd_seg_size_min"  4.933844


Winner take all: true
Out-of-bag evaluation: accuracy:0.999989 logloss:5.98876e-05
Number of trees: 300
Total number of nodes: 27116

Number of nodes by tree:
Count: 300 Average: 90.3867 StdDev: 20.2115
Min: 45 Max: 153 Ignored: 0
----------------------------------------------
```

```
[  45,  50)  4   1.33%   1.33% #
[  50,  55)  4   1.33%   2.67% #
[  55,  61) 12   4.00%   6.67% ###
[  61,  66) 15   5.00%  11.67% ####
[  66,  72) 21   7.00%  18.67% ######
[  72,  77) 19   6.33%  25.00% #####
[  77,  83) 35  11.67%  36.67% ##########
[  83,  88) 32  10.67%  47.33% #########
[  88,  94) 31  10.33%  57.67% #########
[  94,  99) 17   5.67%  63.33% #####
[  99, 104) 35  11.67%  75.00% ##########
[ 104, 110) 23   7.67%  82.67% #######
[ 110, 115) 14   4.67%  87.33% ####
[ 115, 121) 20   6.67%  94.00% ######
[ 121, 126)  4   1.33%  95.33% #
[ 126, 132)  2   0.67%  96.00% #
[ 132, 137)  4   1.33%  97.33% #
[ 137, 143)  6   2.00%  99.33% ##
[ 143, 148)  0   0.00%  99.33%
[ 148, 153]  2   0.67% 100.00% #

Depth by leafs:
Count: 13708 Average: 7.36475 StdDev: 2.5504
Min: 2 Max: 15 Ignored: 0
-----------------------------------------------
[  2,  3)  189   1.38%   1.38% #
[  3,  4)  717   5.23%   6.61% ###
[  4,  5)  954   6.96%  13.57% ####
[  5,  6) 1384  10.10%  23.67% ######
[  6,  7) 1975  14.41%  38.07% #########
[  7,  8) 2152  15.70%  53.77% ##########
[  8,  9) 1995  14.55%  68.33% #########
[  9, 10) 1614  11.77%  80.10% ########
[ 10, 11) 1149   8.38%  88.48% #####
[ 11, 12)  761   5.55%  94.03% ####
[ 12, 13)  415   3.03%  97.06% ##
[ 13, 14)  242   1.77%  98.83% #
[ 14, 15)  111   0.81%  99.64% #
[ 15, 15]   50   0.36% 100.00%

Number of training obs by leaf:
Count: 13708 Average: 15427.7 StdDev: 68342.5
Min: 5 Max: 682791 Ignored: 0
-----------------------------------------------
[      5,  34144) 12681  92.51%  92.51% ##########
[  34144,  68283)   374   2.73%  95.24%
[  68283, 102423)   159   1.16%  96.40%
[ 102423, 136562)    83   0.61%  97.00%
```

```
[ 136562, 170701)    72   0.53%  97.53%
[ 170701, 204841)    19   0.14%  97.67%
[ 204841, 238980)    15   0.11%  97.78%
[ 238980, 273119)    19   0.14%  97.91%
[ 273119, 307259)    22   0.16%  98.07%
[ 307259, 341398)    14   0.10%  98.18%
[ 341398, 375537)    23   0.17%  98.34%
[ 375537, 409677)    32   0.23%  98.58%
[ 409677, 443816)    31   0.23%  98.80%
[ 443816, 477955)    68   0.50%  99.30%
[ 477955, 512095)    36   0.26%  99.56%
[ 512095, 546234)    24   0.18%  99.74%
[ 546234, 580373)    21   0.15%  99.89%
[ 580373, 614513)     5   0.04%  99.93%
[ 614513, 648652)     0   0.00%  99.93%
[ 648652, 682791]    10   0.07% 100.00%

Attribute in nodes:
        1688 : dst_port [NUMERICAL]
        945 : init_fwd_win_byts [NUMERICAL]
        567 : fwd_seg_size_min [NUMERICAL]
        545 : flow_iat_min [NUMERICAL]
        487 : flow_iat_max [NUMERICAL]
        486 : fwd_pkts/s [NUMERICAL]
        466 : fwd_iat_min [NUMERICAL]
        445 : fwd_iat_max [NUMERICAL]
        445 : flow_pkts/s [NUMERICAL]
        397 : flow_duration [NUMERICAL]
        390 : fwd_iat_mean [NUMERICAL]
        367 : fwd_iat_tot [NUMERICAL]
        365 : flow_iat_mean [NUMERICAL]
        310 : fin_flag_cnt [NUMERICAL]
        258 : fwd_header_len [NUMERICAL]
        246 : flow_iat_std [NUMERICAL]
        235 : bwd_pkts/s [NUMERICAL]
        203 : flow_byts/s [NUMERICAL]
        195 : fwd_seg_size_avg [NUMERICAL]
        189 : fwd_pkt_len_max [NUMERICAL]
        183 : fwd_pkt_len_mean [NUMERICAL]
        178 : ack_flag_cnt [NUMERICAL]
        163 : pkt_len_std [NUMERICAL]
        163 : init_bwd_win_byts [NUMERICAL]
        160 : bwd_iat_mean [NUMERICAL]
        157 : fwd_iat_std [NUMERICAL]
        154 : pkt_len_var [NUMERICAL]
        154 : bwd_iat_max [NUMERICAL]
        150 : bwd_header_len [NUMERICAL]
        145 : totlen_fwd_pkts [NUMERICAL]
```

```
        142 : pkt_len_max [NUMERICAL]
        137 : pkt_size_avg [NUMERICAL]
        135 : subflow_fwd_byts [NUMERICAL]
        126 : pkt_len_mean [NUMERICAL]
        120 : fwd_pkt_len_std [NUMERICAL]
        111 : timestamp [CATEGORICAL]
        109 : totlen_bwd_pkts [NUMERICAL]
        108 : subflow_bwd_byts [NUMERICAL]
        107 : bwd_iat_min [NUMERICAL]
        106 : bwd_pkt_len_mean [NUMERICAL]
        103 : fwd_pkt_len_min [NUMERICAL]
        94 : bwd_seg_size_avg [NUMERICAL]
        79 : bwd_pkt_len_max [NUMERICAL]
        79 : bwd_iat_std [NUMERICAL]
        78 : bwd_iat_tot [NUMERICAL]
        76 : bwd_pkt_len_std [NUMERICAL]
        75 : subflow_bwd_pkts [NUMERICAL]
        72 : fwd_psh_flags [NUMERICAL]
        70 : tot_fwd_pkts [NUMERICAL]
        65 : tot_bwd_pkts [NUMERICAL]
        63 : syn_flag_cnt [NUMERICAL]
        60 : subflow_fwd_pkts [NUMERICAL]
        41 : idle_max [NUMERICAL]
        40 : active_mean [NUMERICAL]
        39 : psh_flag_cnt [NUMERICAL]
        38 : idle_mean [NUMERICAL]
        38 : active_min [NUMERICAL]
        36 : urg_flag_cnt [NUMERICAL]
        36 : fwd_act_data_pkts [NUMERICAL]
        35 : active_max [NUMERICAL]
        32 : down/up_ratio [NUMERICAL]
        30 : idle_min [NUMERICAL]
        28 : idle_std [NUMERICAL]
        23 : protocol [NUMERICAL]
        19 : active_std [NUMERICAL]
        13 : bwd_pkt_len_min [NUMERICAL]
        9 : pkt_len_min [NUMERICAL]

Attribute in nodes with depth <= 0:
        44 : bwd_iat_max [NUMERICAL]
        33 : bwd_iat_mean [NUMERICAL]
        32 : bwd_iat_min [NUMERICAL]
        31 : fwd_seg_size_min [NUMERICAL]
        25 : bwd_iat_std [NUMERICAL]
        23 : init_fwd_win_byts [NUMERICAL]
        20 : flow_iat_std [NUMERICAL]
        14 : active_mean [NUMERICAL]
        14 : active_max [NUMERICAL]
```

```
        13 : idle_std [NUMERICAL]
        11 : active_min [NUMERICAL]
        6 : active_std [NUMERICAL]
        5 : fwd_iat_max [NUMERICAL]
        5 : flow_iat_mean [NUMERICAL]
        4 : idle_mean [NUMERICAL]
        4 : fwd_iat_mean [NUMERICAL]
        4 : flow_pkts/s [NUMERICAL]
        3 : subflow_bwd_byts [NUMERICAL]
        2 : idle_max [NUMERICAL]
        1 : totlen_fwd_pkts [NUMERICAL]
        1 : subflow_fwd_byts [NUMERICAL]
        1 : fwd_pkt_len_mean [NUMERICAL]
        1 : fwd_header_len [NUMERICAL]
        1 : flow_iat_max [NUMERICAL]
        1 : flow_duration [NUMERICAL]
        1 : bwd_iat_tot [NUMERICAL]

Attribute in nodes with depth <= 1:
        98 : fwd_seg_size_min [NUMERICAL]
        78 : bwd_iat_max [NUMERICAL]
        62 : init_fwd_win_byts [NUMERICAL]
        60 : bwd_iat_mean [NUMERICAL]
        51 : bwd_iat_min [NUMERICAL]
        39 : flow_iat_std [NUMERICAL]
        33 : bwd_iat_std [NUMERICAL]
        23 : bwd_pkts/s [NUMERICAL]
        22 : fwd_iat_min [NUMERICAL]
        22 : flow_iat_min [NUMERICAL]
        20 : totlen_bwd_pkts [NUMERICAL]
        20 : dst_port [NUMERICAL]
        19 : flow_pkts/s [NUMERICAL]
        17 : subflow_bwd_byts [NUMERICAL]
        17 : fwd_iat_max [NUMERICAL]
        16 : idle_std [NUMERICAL]
        16 : active_mean [NUMERICAL]
        16 : active_max [NUMERICAL]
        15 : fwd_iat_mean [NUMERICAL]
        14 : flow_iat_mean [NUMERICAL]
        14 : active_min [NUMERICAL]
        13 : bwd_seg_size_avg [NUMERICAL]
        13 : bwd_iat_tot [NUMERICAL]
        12 : fwd_iat_tot [NUMERICAL]
        12 : bwd_pkt_len_mean [NUMERICAL]
        12 : bwd_pkt_len_max [NUMERICAL]
        11 : idle_mean [NUMERICAL]
        11 : fwd_pkts/s [NUMERICAL]
        11 : fwd_pkt_len_max [NUMERICAL]
```

```
        11 : flow_iat_max [NUMERICAL]
        11 : flow_duration [NUMERICAL]
        10 : fwd_seg_size_avg [NUMERICAL]
        10 : fwd_iat_std [NUMERICAL]
        9 : fwd_pkt_len_mean [NUMERICAL]
        9 : bwd_header_len [NUMERICAL]
        7 : totlen_fwd_pkts [NUMERICAL]
        7 : subflow_fwd_byts [NUMERICAL]
        7 : idle_min [NUMERICAL]
        6 : pkt_size_avg [NUMERICAL]
        6 : idle_max [NUMERICAL]
        6 : active_std [NUMERICAL]
        5 : flow_byts/s [NUMERICAL]
        4 : fin_flag_cnt [NUMERICAL]
        4 : bwd_pkt_len_std [NUMERICAL]
        3 : pkt_len_max [NUMERICAL]
        3 : bwd_pkt_len_min [NUMERICAL]
        2 : pkt_len_var [NUMERICAL]
        2 : pkt_len_mean [NUMERICAL]
        2 : fwd_psh_flags [NUMERICAL]
        2 : fwd_header_len [NUMERICAL]
        1 : tot_fwd_pkts [NUMERICAL]
        1 : tot_bwd_pkts [NUMERICAL]
        1 : psh_flag_cnt [NUMERICAL]
        1 : pkt_len_std [NUMERICAL]
        1 : init_bwd_win_byts [NUMERICAL]
        1 : fwd_pkt_len_std [NUMERICAL]
        1 : down/up_ratio [NUMERICAL]

Attribute in nodes with depth <= 2:
        196 : fwd_seg_size_min [NUMERICAL]
        128 : init_fwd_win_byts [NUMERICAL]
        93 : bwd_iat_max [NUMERICAL]
        82 : bwd_iat_mean [NUMERICAL]
        61 : bwd_iat_min [NUMERICAL]
        58 : flow_iat_min [NUMERICAL]
        53 : flow_iat_std [NUMERICAL]
        53 : dst_port [NUMERICAL]
        52 : flow_pkts/s [NUMERICAL]
        46 : fwd_iat_min [NUMERICAL]
        44 : bwd_pkts/s [NUMERICAL]
        41 : flow_iat_mean [NUMERICAL]
        40 : fwd_seg_size_avg [NUMERICAL]
        36 : fwd_iat_mean [NUMERICAL]
        36 : bwd_iat_std [NUMERICAL]
        35 : fwd_iat_tot [NUMERICAL]
        35 : flow_iat_max [NUMERICAL]
        35 : flow_byts/s [NUMERICAL]
```

34 : fwd_pkts/s [NUMERICAL]
34 : fwd_iat_max [NUMERICAL]
34 : flow_duration [NUMERICAL]
33 : totlen_bwd_pkts [NUMERICAL]
32 : subflow_bwd_byts [NUMERICAL]
32 : fwd_pkt_len_max [NUMERICAL]
31 : fwd_header_len [NUMERICAL]
29 : bwd_seg_size_avg [NUMERICAL]
28 : bwd_pkt_len_max [NUMERICAL]
28 : bwd_header_len [NUMERICAL]
27 : fwd_pkt_len_mean [NUMERICAL]
25 : totlen_fwd_pkts [NUMERICAL]
25 : bwd_pkt_len_mean [NUMERICAL]
22 : init_bwd_win_byts [NUMERICAL]
21 : pkt_size_avg [NUMERICAL]
21 : fwd_iat_std [NUMERICAL]
21 : bwd_iat_tot [NUMERICAL]
21 : active_mean [NUMERICAL]
19 : fwd_psh_flags [NUMERICAL]
18 : idle_std [NUMERICAL]
18 : active_min [NUMERICAL]
18 : active_max [NUMERICAL]
17 : subflow_fwd_byts [NUMERICAL]
17 : idle_mean [NUMERICAL]
16 : syn_flag_cnt [NUMERICAL]
13 : pkt_len_std [NUMERICAL]
13 : pkt_len_max [NUMERICAL]
12 : pkt_len_var [NUMERICAL]
12 : fin_flag_cnt [NUMERICAL]
12 : bwd_pkt_len_std [NUMERICAL]
11 : pkt_len_mean [NUMERICAL]
10 : tot_fwd_pkts [NUMERICAL]
10 : idle_min [NUMERICAL]
10 : fwd_pkt_len_min [NUMERICAL]
10 : down/up_ratio [NUMERICAL]
9 : active_std [NUMERICAL]
8 : idle_max [NUMERICAL]
7 : fwd_pkt_len_std [NUMERICAL]
6 : bwd_pkt_len_min [NUMERICAL]
5 : subflow_fwd_pkts [NUMERICAL]
4 : subflow_bwd_pkts [NUMERICAL]
4 : ack_flag_cnt [NUMERICAL]
3 : fwd_act_data_pkts [NUMERICAL]
2 : tot_bwd_pkts [NUMERICAL]
2 : psh_flag_cnt [NUMERICAL]
2 : pkt_len_min [NUMERICAL]
1 : protocol [NUMERICAL]

```
Attribute in nodes with depth <= 3:
        285 : fwd_seg_size_min [NUMERICAL]
        198 : init_fwd_win_byts [NUMERICAL]
        135 : dst_port [NUMERICAL]
        102 : bwd_iat_max [NUMERICAL]
        98 : flow_iat_min [NUMERICAL]
        98 : bwd_iat_mean [NUMERICAL]
        91 : fwd_pkts/s [NUMERICAL]
        84 : flow_pkts/s [NUMERICAL]
        79 : bwd_pkts/s [NUMERICAL]
        77 : flow_iat_std [NUMERICAL]
        75 : fwd_header_len [NUMERICAL]
        70 : flow_iat_mean [NUMERICAL]
        70 : flow_iat_max [NUMERICAL]
        68 : fwd_seg_size_avg [NUMERICAL]
        67 : fwd_iat_tot [NUMERICAL]
        65 : fwd_iat_mean [NUMERICAL]
        64 : fwd_iat_min [NUMERICAL]
        64 : fwd_iat_max [NUMERICAL]
        63 : flow_byts/s [NUMERICAL]
        63 : bwd_iat_min [NUMERICAL]
        59 : fwd_pkt_len_mean [NUMERICAL]
        59 : flow_duration [NUMERICAL]
        52 : fwd_pkt_len_max [NUMERICAL]
        51 : totlen_bwd_pkts [NUMERICAL]
        48 : init_bwd_win_byts [NUMERICAL]
        47 : fwd_pkt_len_min [NUMERICAL]
        46 : subflow_bwd_byts [NUMERICAL]
        45 : bwd_header_len [NUMERICAL]
        44 : fwd_iat_std [NUMERICAL]
        43 : bwd_pkt_len_mean [NUMERICAL]
        43 : bwd_iat_std [NUMERICAL]
        39 : pkt_len_var [NUMERICAL]
        39 : pkt_len_std [NUMERICAL]
        38 : totlen_fwd_pkts [NUMERICAL]
        37 : pkt_size_avg [NUMERICAL]
        37 : bwd_seg_size_avg [NUMERICAL]
        37 : bwd_pkt_len_max [NUMERICAL]
        34 : fwd_psh_flags [NUMERICAL]
        32 : pkt_len_max [NUMERICAL]
        30 : subflow_fwd_byts [NUMERICAL]
        28 : pkt_len_mean [NUMERICAL]
        28 : active_mean [NUMERICAL]
        27 : bwd_iat_tot [NUMERICAL]
        25 : fin_flag_cnt [NUMERICAL]
        25 : active_max [NUMERICAL]
        24 : tot_fwd_pkts [NUMERICAL]
        24 : syn_flag_cnt [NUMERICAL]
```

```
        23 : bwd_pkt_len_std [NUMERICAL]
        22 : idle_std [NUMERICAL]
        22 : active_min [NUMERICAL]
        20 : fwd_pkt_len_std [NUMERICAL]
        19 : subflow_fwd_pkts [NUMERICAL]
        19 : idle_mean [NUMERICAL]
        17 : ack_flag_cnt [NUMERICAL]
        16 : subflow_bwd_pkts [NUMERICAL]
        16 : idle_min [NUMERICAL]
        16 : idle_max [NUMERICAL]
        12 : down/up_ratio [NUMERICAL]
        11 : tot_bwd_pkts [NUMERICAL]
        10 : active_std [NUMERICAL]
        8 : psh_flag_cnt [NUMERICAL]
        8 : fwd_act_data_pkts [NUMERICAL]
        8 : bwd_pkt_len_min [NUMERICAL]
        4 : urg_flag_cnt [NUMERICAL]
        4 : pkt_len_min [NUMERICAL]
        3 : timestamp [CATEGORICAL]
        1 : protocol [NUMERICAL]

Attribute in nodes with depth <= 5:
        511 : dst_port [NUMERICAL]
        490 : init_fwd_win_byts [NUMERICAL]
        433 : fwd_seg_size_min [NUMERICAL]
        230 : flow_iat_min [NUMERICAL]
        219 : fwd_pkts/s [NUMERICAL]
        204 : flow_pkts/s [NUMERICAL]
        178 : flow_iat_max [NUMERICAL]
        164 : fwd_iat_mean [NUMERICAL]
        162 : flow_duration [NUMERICAL]
        160 : fwd_iat_tot [NUMERICAL]
        160 : fwd_iat_max [NUMERICAL]
        156 : fwd_iat_min [NUMERICAL]
        149 : bwd_pkts/s [NUMERICAL]
        148 : flow_iat_mean [NUMERICAL]
        144 : flow_byts/s [NUMERICAL]
        143 : fwd_header_len [NUMERICAL]
        137 : fwd_seg_size_avg [NUMERICAL]
        131 : flow_iat_std [NUMERICAL]
        131 : bwd_iat_mean [NUMERICAL]
        126 : fwd_pkt_len_mean [NUMERICAL]
        126 : fwd_pkt_len_max [NUMERICAL]
        121 : bwd_iat_max [NUMERICAL]
        106 : init_bwd_win_byts [NUMERICAL]
        94 : fin_flag_cnt [NUMERICAL]
        93 : pkt_len_std [NUMERICAL]
        91 : fwd_pkt_len_min [NUMERICAL]
```

```
        89 : pkt_size_avg [NUMERICAL]
        89 : bwd_header_len [NUMERICAL]
        88 : pkt_len_var [NUMERICAL]
        86 : totlen_bwd_pkts [NUMERICAL]
        86 : fwd_iat_std [NUMERICAL]
        84 : totlen_fwd_pkts [NUMERICAL]
        83 : subflow_fwd_byts [NUMERICAL]
        81 : pkt_len_mean [NUMERICAL]
        79 : pkt_len_max [NUMERICAL]
        76 : subflow_bwd_byts [NUMERICAL]
        76 : bwd_iat_min [NUMERICAL]
        69 : bwd_pkt_len_mean [NUMERICAL]
        64 : ack_flag_cnt [NUMERICAL]
        62 : fwd_pkt_len_std [NUMERICAL]
        62 : bwd_seg_size_avg [NUMERICAL]
        60 : bwd_iat_std [NUMERICAL]
        57 : bwd_pkt_len_max [NUMERICAL]
        56 : syn_flag_cnt [NUMERICAL]
        54 : fwd_psh_flags [NUMERICAL]
        54 : bwd_pkt_len_std [NUMERICAL]
        45 : bwd_iat_tot [NUMERICAL]
        41 : subflow_bwd_pkts [NUMERICAL]
        40 : subflow_fwd_pkts [NUMERICAL]
        38 : tot_fwd_pkts [NUMERICAL]
        35 : active_mean [NUMERICAL]
        34 : idle_max [NUMERICAL]
        30 : tot_bwd_pkts [NUMERICAL]
        30 : active_min [NUMERICAL]
        29 : active_max [NUMERICAL]
        28 : psh_flag_cnt [NUMERICAL]
        26 : idle_mean [NUMERICAL]
        25 : idle_std [NUMERICAL]
        22 : idle_min [NUMERICAL]
        22 : fwd_act_data_pkts [NUMERICAL]
        22 : down/up_ratio [NUMERICAL]
        19 : urg_flag_cnt [NUMERICAL]
        17 : timestamp [CATEGORICAL]
        14 : active_std [NUMERICAL]
        11 : bwd_pkt_len_min [NUMERICAL]
        8 : pkt_len_min [NUMERICAL]
        2 : protocol [NUMERICAL]

Condition type in nodes:
        13297 : HigherCondition
        99 : ContainsCondition
        12 : ContainsBitmapCondition
Condition type in nodes with depth <= 0:
        300 : HigherCondition
```

```
Condition type in nodes with depth <= 1:
        900 : HigherCondition
Condition type in nodes with depth <= 2:
        1911 : HigherCondition
Condition type in nodes with depth <= 3:
        3213 : HigherCondition
        3 : ContainsBitmapCondition
Condition type in nodes with depth <= 5:
        6783 : HigherCondition
        9 : ContainsCondition
        8 : ContainsBitmapCondition
Node format: NOT_SET

Training OOB:
        trees: 1, Out-of-bag evaluation: accuracy:0.999958 logloss:0.00152823
        trees: 11, Out-of-bag evaluation: accuracy:0.999974 logloss:0.000371098
        trees: 21, Out-of-bag evaluation: accuracy:0.999984 logloss:0.000116897
        trees: 31, Out-of-bag evaluation: accuracy:0.999984 logloss:6.43326e-05
        trees: 41, Out-of-bag evaluation: accuracy:0.999986 logloss:6.26781e-05
        trees: 51, Out-of-bag evaluation: accuracy:0.999987 logloss:6.16098e-05
        trees: 61, Out-of-bag evaluation: accuracy:0.999987 logloss:5.90725e-05
        trees: 71, Out-of-bag evaluation: accuracy:0.999989 logloss:5.90699e-05
        trees: 81, Out-of-bag evaluation: accuracy:0.999987 logloss:5.93677e-05
        trees: 91, Out-of-bag evaluation: accuracy:0.999989 logloss:5.82467e-05
        trees: 101, Out-of-bag evaluation: accuracy:0.999989 logloss:5.72201e-05
        trees: 111, Out-of-bag evaluation: accuracy:0.999991 logloss:5.76986e-05
        trees: 121, Out-of-bag evaluation: accuracy:0.99999 logloss:5.72194e-05
        trees: 131, Out-of-bag evaluation: accuracy:0.99999 logloss:5.82669e-05
        trees: 141, Out-of-bag evaluation: accuracy:0.999989 logloss:5.85682e-05
        trees: 151, Out-of-bag evaluation: accuracy:0.99999 logloss:5.92311e-05
        trees: 161, Out-of-bag evaluation: accuracy:0.99999 logloss:5.92355e-05
        trees: 171, Out-of-bag evaluation: accuracy:0.999989 logloss:6.00446e-05
        trees: 181, Out-of-bag evaluation: accuracy:0.999991 logloss:6.05264e-05
        trees: 191, Out-of-bag evaluation: accuracy:0.999986 logloss:6.01335e-05
        trees: 201, Out-of-bag evaluation: accuracy:0.999984 logloss:6.08181e-05
        trees: 211, Out-of-bag evaluation: accuracy:0.999987 logloss:6.05704e-05
        trees: 221, Out-of-bag evaluation: accuracy:0.999987 logloss:6.02536e-05
        trees: 231, Out-of-bag evaluation: accuracy:0.999989 logloss:5.98425e-05
        trees: 241, Out-of-bag evaluation: accuracy:0.999987 logloss:5.97918e-05
        trees: 251, Out-of-bag evaluation: accuracy:0.99999 logloss:5.97172e-05
        trees: 261, Out-of-bag evaluation: accuracy:0.99999 logloss:5.98936e-05
        trees: 271, Out-of-bag evaluation: accuracy:0.999989 logloss:6.01438e-05
        trees: 281, Out-of-bag evaluation: accuracy:0.999989 logloss:6.02035e-05
        trees: 291, Out-of-bag evaluation: accuracy:0.999989 logloss:6.03442e-05
        trees: 300, Out-of-bag evaluation: accuracy:0.999989 logloss:5.98876e-05
```

[24]:
```
# Erstellen der Feature Importance Kriterien aus Sicht des TensorFlow Modells
model.make_inspector().variable_importances()
```

[24]:
```
{'NUM_AS_ROOT': [("bwd_iat_max" (1; #8), 44.0),
  ("bwd_iat_mean" (1; #9), 33.0),
  ("bwd_iat_min" (1; #10), 32.0),
  ("fwd_seg_size_min" (1; #51), 31.0),
  ("bwd_iat_std" (1; #11), 25.0),
  ("init_fwd_win_byts" (1; #58), 23.0),
  ("flow_iat_std" (1; #32), 20.0),
  ("active_max" (1; #1), 14.0),
  ("active_mean" (1; #2), 14.0),
  ("idle_std" (1; #56), 13.0),
  ("active_min" (1; #3), 11.0),
  ("active_std" (1; #4), 6.0),
  ("flow_iat_mean" (1; #30), 5.0),
  ("fwd_iat_max" (1; #38), 5.0),
  ("idle_mean" (1; #54), 4.0),
  ("flow_pkts/s" (1; #33), 4.0),
  ("fwd_iat_mean" (1; #39), 4.0),
  ("subflow_bwd_byts" (1; #68), 3.0),
  ("idle_max" (1; #53), 2.0),
  ("fwd_header_len" (1; #37), 1.0),
  ("fwd_pkt_len_mean" (1; #44), 1.0),
  ("subflow_fwd_byts" (1; #70), 1.0),
  ("totlen_fwd_pkts" (1; #77), 1.0),
  ("flow_iat_max" (1; #29), 1.0),
  ("bwd_iat_tot" (1; #12), 1.0),
  ("flow_duration" (1; #28), 1.0)]}
```