VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

Detekcia anomálií v sieťovej prevádzke za použitia algoritmov strojového učenia

Přenos dat, počítačové sítě a protokoly

Bc. Ján Jakub Kubík

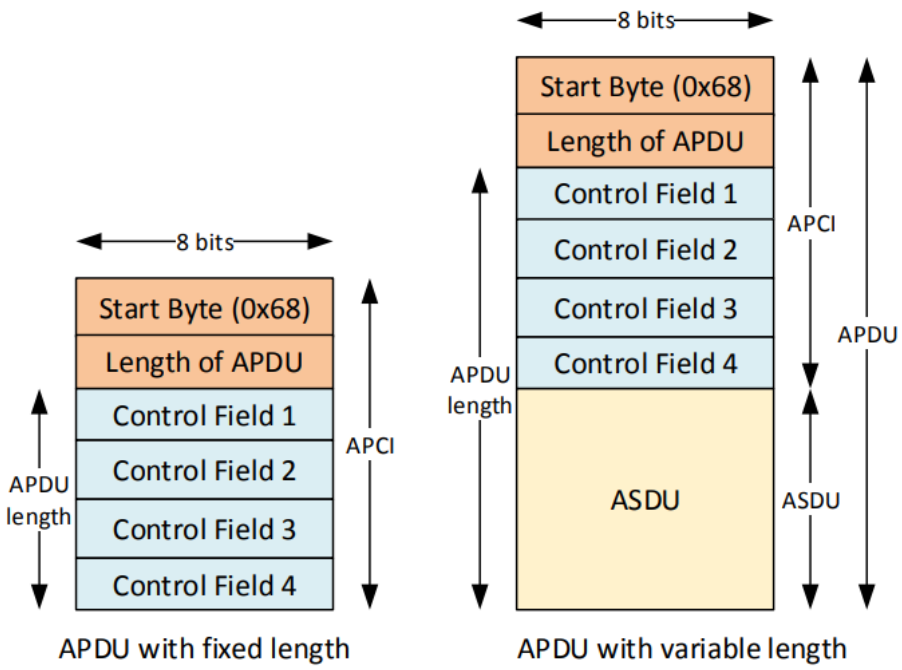
15. apríla 2022

Obsah

1 Úvod

Táto správa k projektu z predmetu *Přenos dat, počítačové sítě a protokoly* sa zaoberá detekciou anomálií v sieťovej prevádzke za použitia algoritmov strojového učenia. Protokol v ktorom sú detekované anomálie sa nazýva IEC 60870-5-104 (IEC 104).

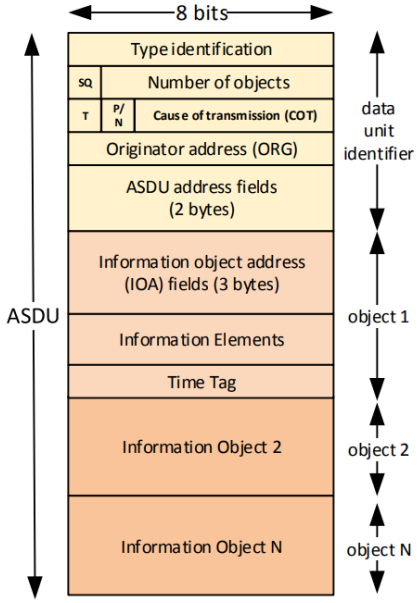
IEC 104 je nástupcom IEC 60870-5-101 (IEC 101), ktorý bol určený na monitorovanie, riadenie a pridruženú komunikáciu v rôznych priemyselných systémoch. IEC 104 zabezpečuje prenos IEC 101 cez TCP/IP. IEC 104 funguje na princípe master slave, kde kontrolná stanica (master) odosiela kontrolovanej stanici (slave) príkazy, dotazy a zbiera odpovede od nej. TCP payload IEC 104 obsahuje 1 alebo viac Application Protocol Data Units (APDUs). APDU je na obrázku 1.1. APDU sa skladá z Application Protocol Control Information (APCI) a môže obsahovať tiež Application Service Data Unit (ASDU). APCI sa dá považovať za hlavičku správy. Obsahuje štartovací byte s hodnotou 0x68, dĺžku celého APDU a 4 byty kontrolných polí.



Obr. 1.1: APDU formát
zdroj: https://www.fit.vut.cz/research/publication-file/11570/TR-IEC104.pdf

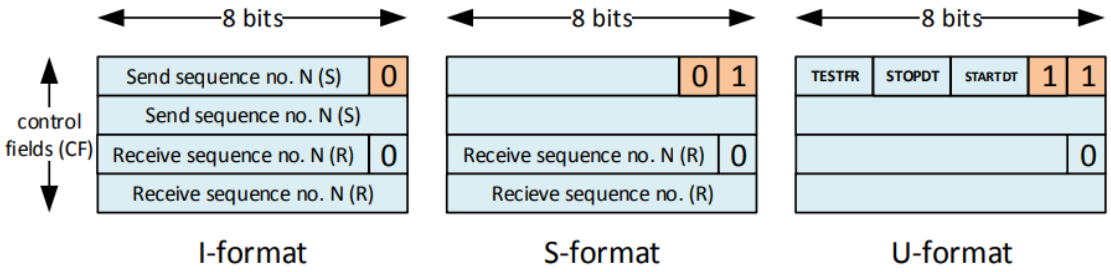
Na obrázku 1.2 je ASDU [3]. ASDU slúži na prenos dát zo senzorov a príkazy medzi kon-

trolovanou a kontrolnou stanicou.



Obr. 1.2: ASDU formát
zdroj: https://www.fit.vut.cz/research/publication-file/11570/TR-IEC104.pdf

Existujú 3 formáty APDU [2]. Sú určené pomocou bitov v kontrolných poliach APCI (obrázok 1.3):



Obr. 1.3: Formáty APDU
zdroj: https://www.fit.vut.cz/research/publication-file/11570/TR-IEC104.pdf

- **I-Format** sa používa na prenos dát zo senzorov, kontrolných dát a príkazov. Skladajú sa z Data Unit Identifier (DUI) a z Information Objects (IO). Každe IO reprezentuje špecifické zariadenie, ktoré má unikátnu adresu nazývanú Information Object Adress (IOA). Prvý ASDU oktet je Type Identification (TypeID), ktoré definuje presný formát dát alebo typ príkazu, ktorý následuje. ASDU ďalej obsahuje Cause Of Transmission (COT). ASDU typeID špecifikuje 'čo/aký' typ dát/príkazu je posielaný a COT určuje 'dôvod' odosielania.

- **S-Format** APDUs slúžia na potvrdzovanie doručených I-format APDUs.
- **U-Format** APDUs poskytujú 3 kontrolné funkcie komunikácie: zahájenie prenosu I-Format APDUs správou STARTDT, zastavenie prenosu I-format APDUs správou STOPDT a udržanie spojenia I-Format APDUs správou TESTRF.

Úlohami projektu je:

1. analýza komunikácie IEC 104,
2. výber a extrakcia atribútov, ktoré dostatočne popisujú celú komunikáciu,
3. tvorba modelu strojového učenia za použitia extrahovaných atribútov,
4. experimenty s normálnymi dátami a s dátami obsahujúcimi anomálie a ich vyhodnotenie.

Kapitola 2 obsahuje spracovanie, podrobný popis, výber a extrakciu jednotlivých atribútov pre model strojového učenia. Kapitola 3 vysvetľuje výber a použitie metódy strojového učenia pre detekciu anomálii v sieťovej prevádzke. Kapitola 4 popisuje experimenty a diskutuje ich výsledky.

2 Spracovanie a príprava dát

V tejto kapitole sú popísané použité dátové sady a výber, extrakcia atribútov z dátových sád, ktoré ich dostatočne popisujú. Ďalej je popísaná agregácii a úprava extrahovaných atribútov pre použitie v strojovom učení.

2.1 Dátové sady

Súhrnné informácie o použitých dátových sadách sú v tabuľke 2.1. Počty paketov v dátových sadách sú počty len pre protokol IEC 104. Pretože v dátových sadách sú zahrnuté aj iné protokoly.

Tabuľka 2.1: Základné informácie o použitých dátových sadách

Dátová sada	Počet paketov	Trvanie	# masters	# slaves
mega104-17-12-18.pcapng (dataset 1)	58929	67h 55min	1	1
10122018-104Mega.pcapng (dataset 2)	76865	4h 53min	1	3

2.2 Výber a extrakcia vlastností z dátových sád

2.2.1 Výber vlastností

Normálna IEC 104 komunikácia má pravidelný charakter, čiže je vhodná na detekovanie anomálii.

Sú dve možnosti ako pracovať s dátami, buď po jednotlivých paketoch alebo po väčších celkoch. Ja som sa rozhodol pracovať s väčšími celkami pretože tam môžem zahrnúť väčšie množstvo jednotlivých atribútov a teda presnejšie opísať ICE 104 komunikáciu. Komunikáciu som rozdelil na 2 toky a to od master stanice ku všetkým slave staniciam a od všetkých slave staníc k master stanici.

V jednotlivých komunikačných tokoch som agregoval extrahované atribúty do väčších celkov po 5 minútových intervaloch. Vybrané atribúty dostatočne popisujúce dátové sady pre daný časový interval sú:

- priemerný inter-arrival time paketov - rozdiel času medzi 2 paketami
- priemerná veľkosť prenesených paketov

- celkový počet prenesených paketov

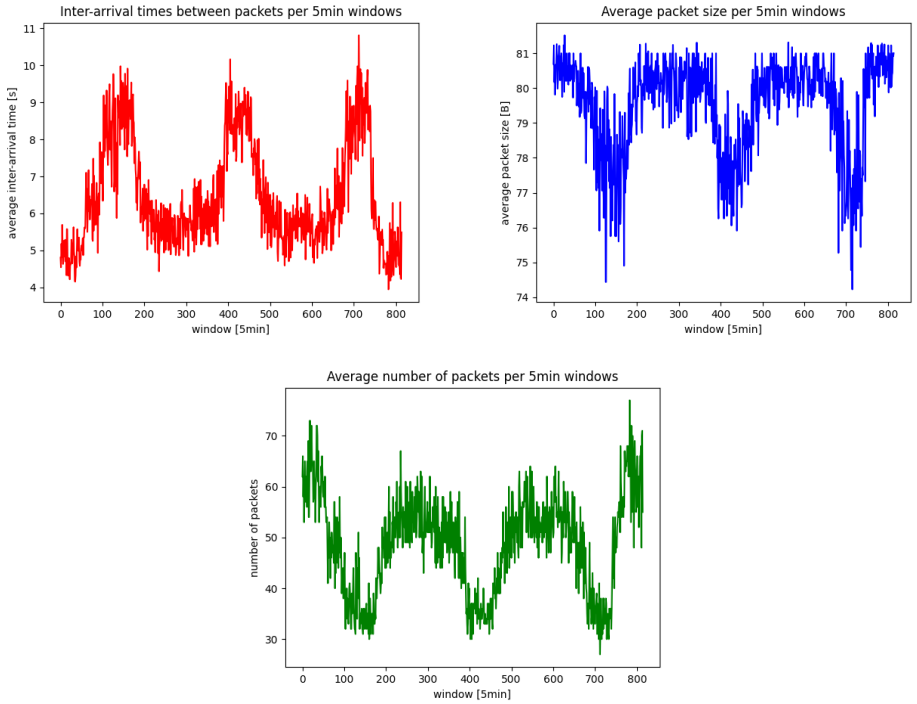
2.2.2 Postup

Najskôr som si musel pomocou tsharku [1] vytiahnúť požadované atribúty z pcapng súborov. Pre jednotlivé pakety som vytiahol nasledujúce vlastnosti: zdrojovú IP adresu a port, cieľovú IP adresu a port, **čas paketu**, jeho **veľkosť** a vyfiltroval som len IEC komunikáciu. Použitý tshark príkaz:

```
$ tshark -r <dataset>.pcapng  -T fields -E separator=";" \
-e ip.src -e tcp.srcport -e ip.dst -e tcp.dstport  -e \
_ws.col.Time -e frame.len  -R "iec60870_104" -2 > <filename>.csv
```

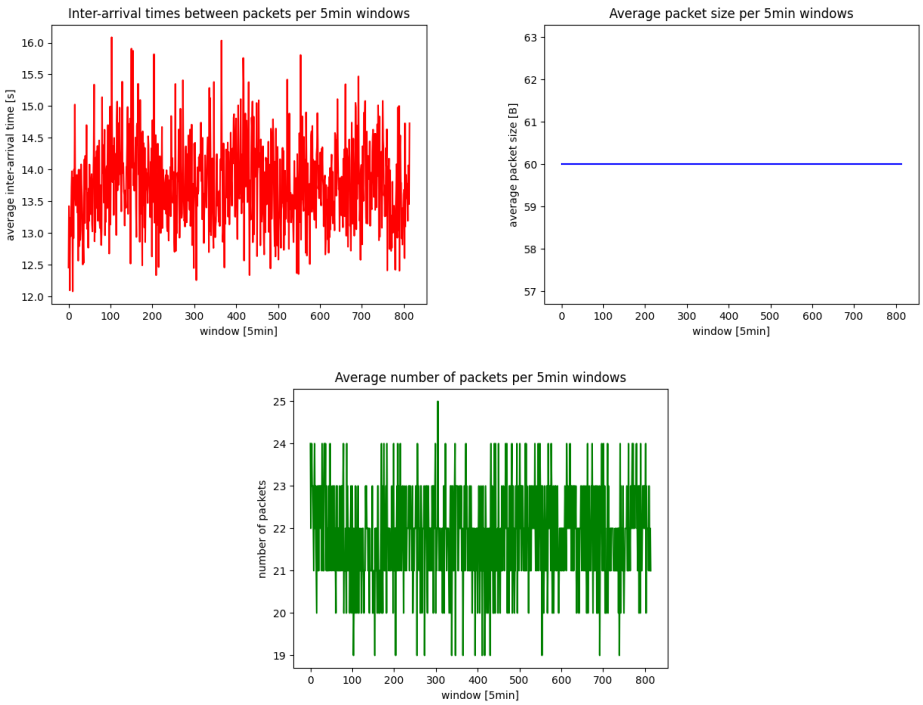
Vytiahnuté dáta som si musel ešte upraviť pomocou python skriptu *datasets.py* (dodatok A) do 2 nezávyslých tokov od mastra ku všetkým slaves a naopak. Toto som spravil pomocou zistenia ktorá stanica je master z dátovej sady a rozdelil som to pomocou IP adresy a portu master stanice. Ďalej som to musel ešte upraviť do **5 minútových okien**, ktoré agregujú **celkový počet prenesených paketov**, **priemernú veľkosť prenesených paketov** a **priemerný inter-arrival time paketov** v danom časovom okne.

Extrahované, upravené dáta som zobrazil a vizuálne som skontroloval, či IEC 104 komunikácia je pravidelná a nie sú tam žiadne drastické zmeny (obrázok 2.1, 2.2 a 2.3).

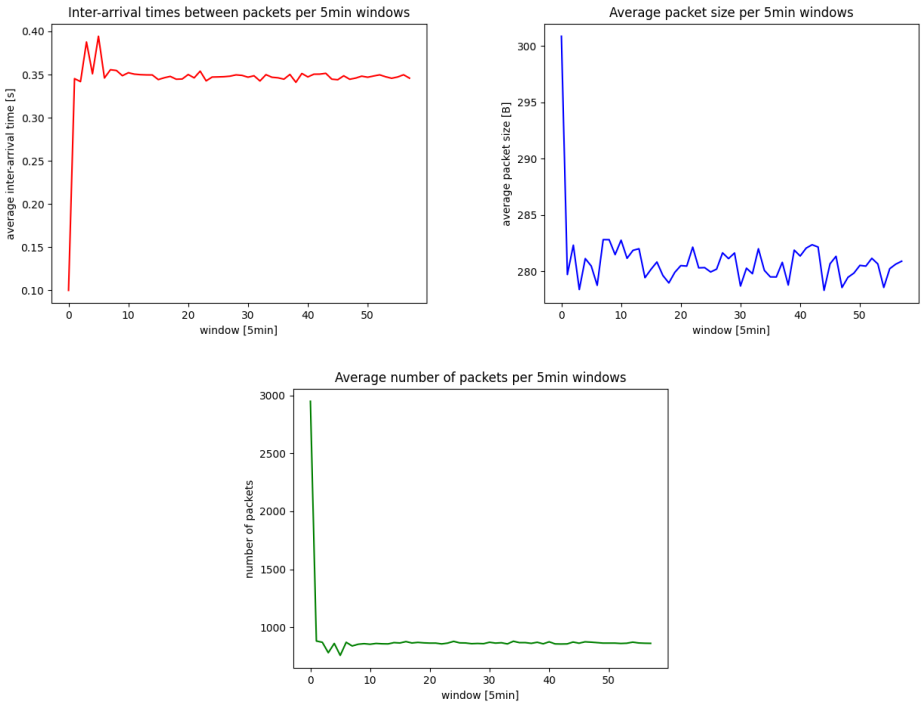


Obr. 2.1: dátová sada 1 z master do všetých slaves

[1] https://www.wireshark.org/docs/man-pages/tshark.html



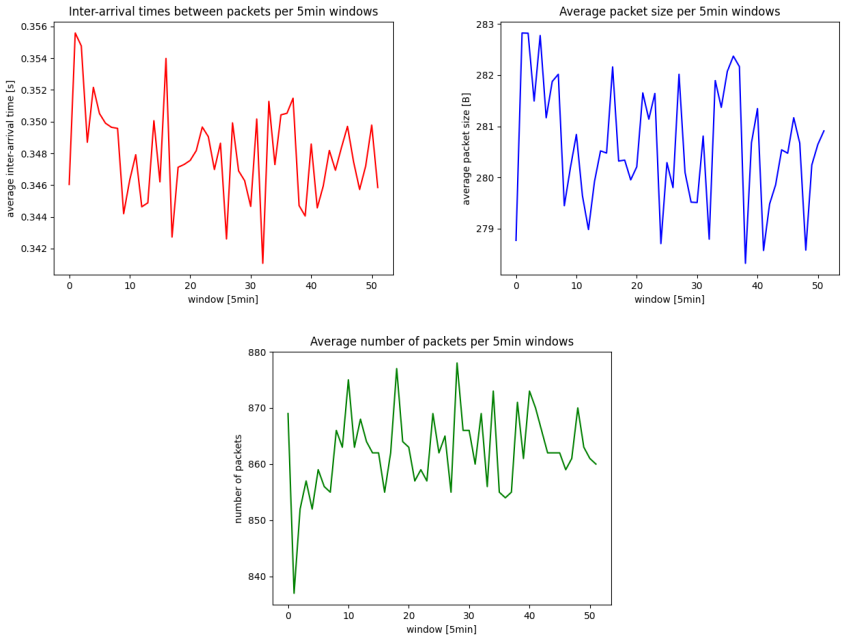
Obr. 2.2: dátová sada 1 zo všetkých slaves do mastra



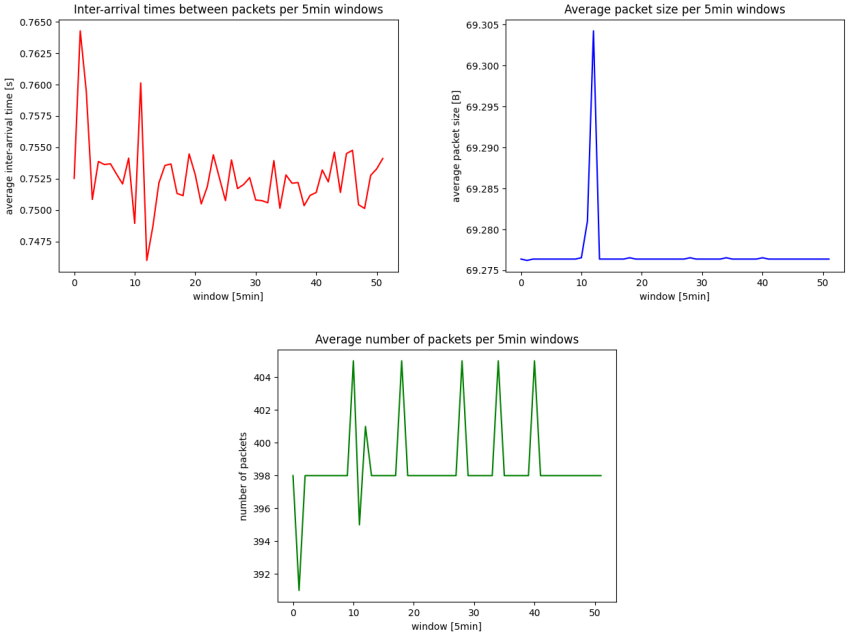
Obr. 2.3: dátová sada 2 z master do všetých slaves

V dátovej sade 2 obrázok 2.3, sú viditeľné dosť veľké zmeny vo všetkých grafor. Rovnako to

je pre dátovú sadu aj s komunikáciou od všetkých slaves do mastra. Z tohoto dôvodu som sa rozhodol problematické atribúty z nej odstrániť. Konkrétne počiatočných 6 5 minútových okien. Po odstránení grafy vyzerali následovne (obrázok 2.4 a 2.5).



Obr. 2.4: dátová sada 2 z mastra do všetých slaves



Obr. 2.5: dátová sada 2 zo všetých slaves do mastra

3 Model strojového učenia

V tejto kapitole je vysvetlená použitá metóda strojového učenia. Konkrétne SVM klasifikácia do 1 triedy. Ďalej je vysvetlený postup tvorby modelu strojového učenia za použitia SVM klasifikátora do 1 triedy.

3.1 SVM klasifikácia do 1 triedy

Cieľom projektu je detekcia anomálii v IEC-104 komunikácii výberom vhodných atribútov dostatočne popisujúcich IEC komunikáciu a ich použitím v strojovom učení. Detekcia anomálii alebo aj inak povedané detekcia odľahlých hodnôt je určovanie hodnôt, ktoré sú nejakým spôsobom iné ako normálne hodnoty. Detekcia anomálii v tomto protokole slúži na odchytenie útokov alebo výpadkov 1 alebo viacerých zariadení.

Ak nie sú v dátovej sade rovnomerne zastúpené normálne a odľahlé hodnoty alebo sú v dátovej sade buď len normálne alebo len odľahlé hodnoty, tak je klasifikácia do 1 triedy vhodným kandidátom z algoritmov strojového učenia na riešenie tohoto problému. Vo väčšine prípadov je odľahlých hodnôt v dátových sadách podstatne menej ako normálnych hodnôt.

Princíp modelov založených na klasifikácii do 1 triedy je že sú natrénované len na dátach ktoré majú normálnu/odľahlú hodnotu. Po natrénovaní sú tieto modely schopné predpovedať či nové dáta patria do skupiny normálnych/odľahlých hodnôt alebo nie, čiže sú to odľahlé/normálné hodnoty [1].

3.2 Postup

Pre normalizáciu dátových sád a tvorbu modelu bol použitý skript *model.py* (dodatok A). Normalizácia bola potrebná aby 1 atribút nemal väčší vplyv na trénovanie ako ostané atribúty. Na normalizovanie bola použitá funkcia **log** z knižnice numpy [1]. Funkcia log počíta prirodzený logaritmus zo zadaných hodnôt. Na ňu bola aplikovaná funkcia **abs** zo štandardnej knižnice Pythonu[2]. Funkcia abs počíta absolútnu hodnotu zo zadaných čísiel.

Podľa zadania bolo potrebné ešte obe normalizované dátové sady rozdeliť na 2 časti. 1. časť 2/3 dátovej sady bola použitá na trénovanie modelu a 2. časť 1/3 bola použitá na validovanie modelu. Obe dátové sady boli rozdelné na komunikáciu od mastra ku všetkým

[1] https://numpy.org/doc/stable/reference/generated/numpy.log.html
[2] https://docs.python.org/3/library/functions.html#abs

slaves a naopak. Pre tieto 2 toky komunikácie pre obe dátové sady boli vytvorené modely. Celkovo teda vznikli 4 modely.

Pre vytvorenie modelu z normalizovaných dát bol použitý OneClassSVM klasifikátor z knižnice scikit-learn [3]. Kód:

```
model = OneClassSVM(nu=0.001, kernel="poly", gamma="auto").fit(train_data)
```

Nu parameter musí byť v rozsahu (0, 1>. Zjednodušene hovorí o očakávanom zastúpení odľahlých hodnôt v trénovacej dátovej sade. Nemôže byť 0. Preto som zvolil dostatočne malú nenulovú hodnotu. **Gamma** určuje stupeň zakryvenia rozhodovacej hranice. **Kernel** slúži na transformácie dát v ktorých sa potom lepšie určujú hranice rôznych tried. Po vyskúšaní kernelových funkcií linear, poly, rbf a sigmoid na všetkých 4 dátových sadách som dospel k záveru, že použitie kernelovej funkcie poly je najvhodnejšie.

V tabuľke 3.1 je vyhodnotenie úspešnoti klasifikovania do triedy normálnej prevádzky na trénovacích a validačných častiach dátových sád.

Tabuľka 3.1: Vyhodnotenie úspešnosti na trénovacích a validačných častiach dátových sád

Dátová sada	**Trénovacia časť**	**Validačná časť**
ds 1: master –> slave	100.00%	98.92%
ds 1: slaves –> master	99.81%	99.64%
ds 2: master –> slaves	97.37%	90.00%
ds 2: slaves –> master	97.36 %	100.00%

[3] https://scikit-learn.org/stable/auto_examples/svm/plot_oneclass.html

4 Testovanie a experimenty

V tejto kapitole je popísané testovanie. Otestoval som detekciu DDOS útoku.

4.1 Testy

Testovanie prebiehalo tak, že druhú polovicu vyextrahovaných, upravených dát agregovaných do 5 minútových okien som upravil aby simulovali DDOS útok.

Otestované boli všetky 4 modely. Na experimenty som použil skript *tests.py* (dodatok A).

4.1.1 DDOS útok

Pre simulovanie DDOS útoku som v druhej polovici všetkých dátových sád pre jednolivé časové okná zvýšil počet paketov na 200%, znížil som inter arrival time na 50% a zmenil som priemernú veľkosť paketov postupne na 130%, 80% a 30% pôvodnej veľkosti.

Tabuľka 4.1 je vyhodnotenie DDOS útoku so 130% priemernou velkosťou paketov pre jednotlivé 5 minútové časové okná. Obsahuje konfúznu maticu, ktorá popisuje úspešnosti jednotlivých modelov.

Tabuľka 4.1: Konfúzna matica pre DDOS útok pre pakety o veľkosti 130%

Dátová sada	Celkovo hodnôt	T pozit	F pozit	T negat	F negat
ds 1: master –> slave	poz:407, neg:408	407 [100%]	0 [0%]	0 [0%]	407 [100%]
ds 1: slaves –> master	poz:407, neg:408	406 [99.75%]	1 [0.25%]	0 [0%]	408 [100%]
ds 2: master –> slaves	poz:26, neg:26	26 [100%]	0 [0%]	0 [0%]	26 [100%]
ds 2: slaves –> master	poz:26, neg:26	26 [100%]	0 [0%]	0 [0%]	26 [100%]

Tabuľka 4.2 je vyhodnotenie DDOS útoku s 80% priemernou veľkosťou paketov pre jednotlivé 5 minútové časové okná. Obsahuje konfúznu maticu, ktorá popisuje úspešnosti jednotlivých modelov.

Tabuľka 4.2: Konfúzna matica pre DDOS útok pre pakety o veľkosti 80%

Dátová sada	Celkovo hodnôt	T pozit	F pozit	T negat	F negat
ds 1: master –> slave	poz:407, neg:408	407 [100%]	0 [0%]	23 [5.7%]	385 [94.3%]
ds 1: slaves –> master	poz:407, neg:408	406 [99.75%]	1 [0.25%]	294 [72%]	114 [28%]
ds 2: master –> slaves	poz:26, neg:26	25 [96%]	1 [4%]	0 [0%]	26 [100%]
ds 2: slaves –> master	poz:26, neg:26	26 [100%]	0 [0%]	0 [0%]	26 [100%]

Tabuľka 4.3 je vyhodnotenie DDOS útoku s 30% priemernou veľkosťou paketov pre jednotlivé 5 minútové časové okná. Obsahuje konfúznu maticu, ktorá popisuje úspešnosti jednotlivých modelov.

Tabuľka 4.3: Konfúzna matica pre DDOS útok pre pakety o veľkosti 30%

Dátová sada	Celkovo hodnôt	T pozit	F pozit	T negat	F negat
ds 1: master –> slave	poz:407, neg:408	406 [99.75%]	1 [0.25%]	407 [99.8%]	1 [0.2%]
ds 1: slaves –> master	poz:407, neg:408	406 [99.75%]	1 [0.25%]	408 [100%]	0 [0%]
ds 2: master –> slaves	poz:26, neg:26	25 [96%]	1 [4%]	26 [100%]	0 [0%]
ds 2: slaves –> master	poz:26, neg:26	26 [100%]	0 [0%]	26 [100%]	0 [0%]

Z testov vyplýva, že použité modely sú schopné zachytiť DDOS útoky s menšiou veľkosťou paketov ako je pôvodná veľkosť paketov. S útokmi obsahujúcimi pakety pôvodnej alebo väčšej veľkosti majú všetky 4 modely veľký problém.

5 Záver

Modely pre detekciu anomálii v sieťovej prevádzke IEC104 vedia pomerne presne detekovať normálnu prevádzku, ale majú veľký problém s neobvyklou prevádzkou aká je napríklad pri DDOS útokoch za použitia veľkých paketov. No pre malé pakety vedia modely DDOS útok pomerne spoľahlivo detekovať.

Pre spresnenie modelov by bolo vhodné vyskúšať rozdeliť dátové toky na toky medzi jednotlivými zariadeniami. To znamená od mastra ku knkrétnemu slave a naopak. Mne na toto už nezostal čas.

Projekt bol vypracovaný na základe prezentácie a materiálov poskytnutých vedúcim projektu Ing. Petrom Matouškom, Ph.D., M.A..

Literatúra

[1] Brownlee, J. *One-Class Classification Algorithms for Imbalanced Datasets*. Dostupné z: https://machinelearningmastery.com/one-class-classification-algorithms/.

[2] Mai, K., Qin, X., Ortiz, N., Molina, J. a Cardenas, A. A. Uncharted Networks: A First Measurement Study of the Bulk Power System. In: *Proceedings of the ACM Internet Measurement Conference*. New York, NY, USA: Association for Computing Machinery, 2020, s. 201–213. IMC '20. Dostupné z: https://doi.org/10.1145/3419394.3423630. ISBN 9781450381383.

[3] Matoušek, P. *Description and analysis of IEC 104 Protocol*. 2017. 38 s. Dostupné z: https://www.fit.vut.cz/research/publication/11570.

A Súbory k Projektu

Dodatok obsahujem zoznam súborov k projektu dostupných na Google Drive[1].

- datasets/ – adresár s dátovými sadami a vyextrahovanými atribútmi pre trénovanie modelov
  - 104_mega/
    - mega104-17-12-18.pcapng
    - 104_mega.csv
    - 104_mega_master_slaves.csv
    - 104_mega_slaves_master.csv
  - 10122018/
    - 10122018-104Mega.pcapng
    - 104_mega.csv
    - 10122018_master_slaves.csv
    - 10122018_slaves_master.csv
- imgs/ – vytvorené grafy
- datasets.py – skript na prípravu dátových sád
- models.py – skript na tvorbu a vyhodnotenie modelov
- tests.py – skript na testovanie
- requirements.txt – požadované balíčky pre spustenie skriptov
- README.txt

[1] https://drive.google.com/drive/folders/1LO9q8kO62SkNfMT9Kiv5tOMTlL2bitB-?usp=sharing