ŽILINSKÁ UNIVERZITA V ŽILINE
Fakulta riadenia a informatiky

DETEKCIA ANOMÁLNYCH TOKOV V SIETI

Bc. Marián Krnáč
Vedúci práce: Ing. Ondrej Škvarek, PhD.
Konzultant: prof. Ing. Martin Klimo, PhD.

Projekt 3, 7.2.2022

Motivácia

Motiváciou je odhalenie nových, doteraz neznámych útokov v počítačovej sieti pomocou analýzy danej zachytenej sieťovej prevádzky (toku paketov).

Cieľ

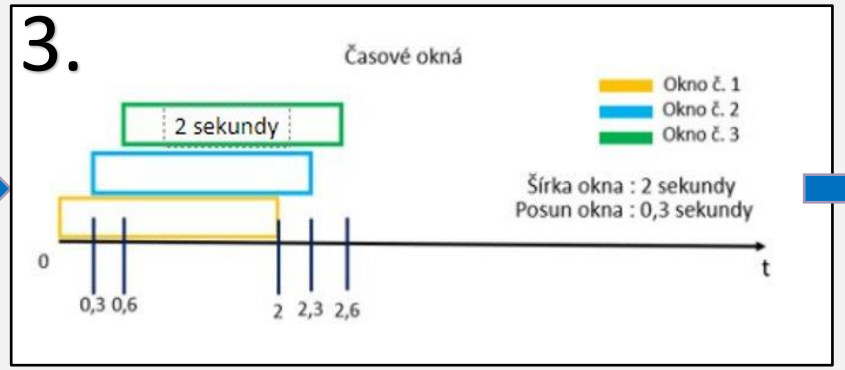
Vytvorenie systému, ktorý bude schopný detegovať anomálie v paketových tokoch v počítačovej sieti a signalizovať dané časové okamihy.

Postup práce

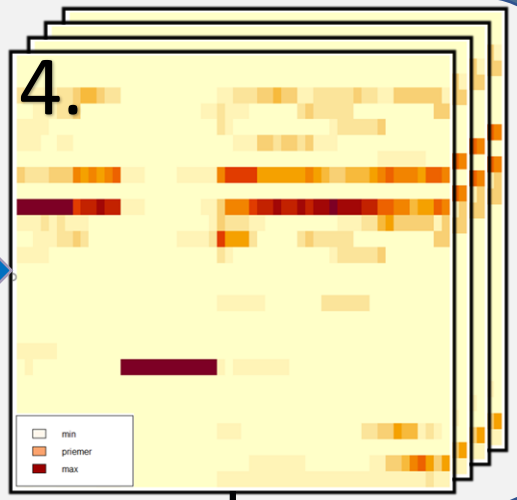
1. Načítanie a filtrácia dát
   Filtrácia dát na základe zadaných podmienok (čas, konkrétne IP adresy, porty atď.)
2. Kategorizácia dát (paketov)
   Jednotlivé pakety je potrebné kategorizovať na základe určených podmienok a na to sme použili niekoľko postupov :
   1. Shannonovo–Fanovo kódovanie (strom)
   2. L2-L3 a L4 atribútov paketov
3. Vytvorenie časových okien
   Kategorizované dáta sú následne utriedené do časových okien. Jedno okno predstavuje početnosti jednotlivých kategórii za daný časový okamih.
4. Vytvorenie teplotných máp
   Mapy slúžia ako vstup do štatistických metód alebo neurónových sieti.
5. PCA - Analýza hlavných komponentov
   Priebeh časových okien v priestore dvoch najdôležitejších PCA komponentov
6. Autoenkóder
   Implementovaný pomocou hlbokých konvolučných neurónových sietí. Priebeh teplotných máp v priestore dvoch najdôležitejších latentných premenných autoenkóderu.

1.

3.

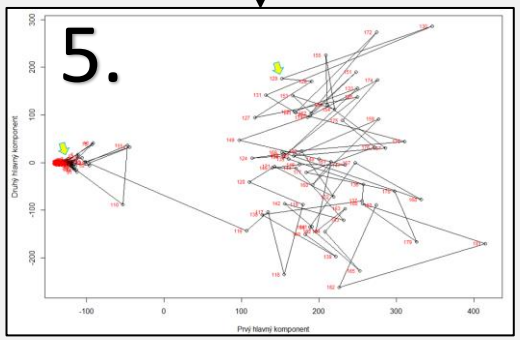


4.

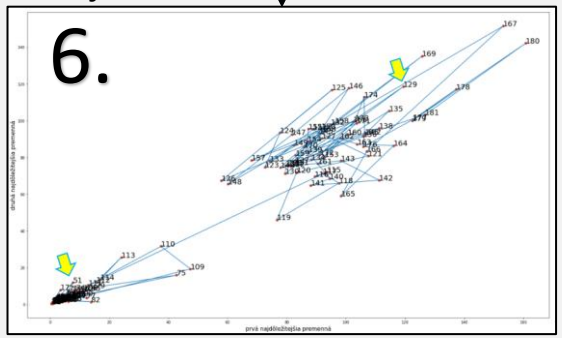


Porovnanie výsledkov

5.



6.



Porovnanie nám slúži na kontrolu výsledkov ktoré nám poskytuje natrénovaná neurónová sieť oproti PCA.

PCA (lineárna transformácia) a autoenkóderu (nelineárna funkcia).

Grafy zobrazujú priebehy jednotlivých máp. Každý bod na grafoch zobrazuje jednu mapu spolu s jej poradovým číslom.