

Posudek oponenta bakalářské práce

Student: Lička Zbyněk
Téma: Detekce anomálií ve Wi-Fi komunikaci (id 25135)
Oponent: Homoliak Ivan, Ing., Ph.D., UITS FIT VUT

- 1. Náročnost zadání** průměrně obtížné zadání
- 2. Splnění požadavků zadání** zadání splněno pouze částečně

Prvý bod zadania bol splnený len čiastočne keďže sa študent venoval len metódam detekcie anomálií založených na strojvome učení a neuvažoval iné metódy. Tiež mám pochybnosti o zameraní riešenia práce na štandard IEEE 802.11 keďže prepojenie na tento štandard vidím len v použití niektorých testovacích dátach. Očakával by som hlbšie zameranie na tento štandard a teda držanie sa zadania.
- 3. Rozsah technické zprávy** splňuje pouze minimální požadavky

Práca obsahuje 46 strán vysádzaného textu (vrátane príloh) a samotný text bez obrázkov predstavuje 45 normostrán. Obrázky tvoria 4.5 normostrán.
- 4. Prezentácia úroveň predloženej práce** 65 b. (D)

Prezentácia úroveň práce je dobrá, kapitoly sú pre čitateľa zrozumiteľné a logicky na seba nadväzujú. Hlavný výhradu mám k popisu výsledkov experimentov v kapitole 6.

Mám aj ďalšie výhrady. Interpretácia a popis obrázkov 6.2 a 6.3 nie sú jasné a zreteľné. Názvy kapitol 4 a 5 sú zbytočne dlhé. Obrázok 5.6 zobrazuje accuracy, čo je nie je vhodná metrika ohodnotenia kvality modelu pretože zvýhodňuje početnejšiu triedu.
- 5. Formálna úprava technickej zprávy** 75 b. (C)

Po formálnej a typografickej stránke má práca priemernú úroveň. Jazykovú stránku práce som nehodnotil.
- 6. Práca s literatúrou** 75 b. (C)

Práca obsahuje 24 zdrojů. Študent čerpal predovšetkým z odborných konferenčných a časopisových článkov. Výběr literatury považuji za přijatelný.
- 7. Realizační výstup** 65 b. (D)

Študent vytvoril realizačný výstup, ktorý z môjho hľadiska splňuje len minimálne požiadavky zadania. Experimenty s reálnymi dátami a ich výsledky sú diskutabilné, keďže študent testoval len dva typy útokov a to v len v dvoch inštanciách. Legitímne dáta boli zozbierané z 2.5 hodiny sieťovej prevádzky.
- 8. Využitelnost výsledků**

Práca stavala na už známých a publikovaných výsledkoch strojového učenia a preto išlo len o reprodukciu experimentov s vlastnými dátami.

Pozn.: Na druhej strane bakalársky program (podľa mojich vedomostí) neobsahuje povinné predmety zameriavajúce sa na (rekurentné) neurónové siete.
- 9. Otázky k obhajobě**

1): Aké metódy detekcie anomálií v prostredí počítačových sietí poznáte a čím sa odlišujú?

2): Aký je rozdiel medzi anomálnymi a signatúrnymi systémami detekcie prienikov (IDS)? Kam by ste zaradili binárne klasifikačné metódy, ktoré popisujete v sekcii 2.2?

3): Ako konkrétne sa dajú využiť evolučné techniky na detekciu anomálií v sieťovej prevádzke?
- 10. Souhrnné hodnocení** 68 b. uspokojivě (D)

Študent vytvoril minimálny realizačný výstup a spracoval priemernú technickú správu preto hodnotím prácu stupňom D (68). V prípade uspokojivého zodpovedania mojich a ďalších otázok nechávam na zvážení komisie zlepšenie známky o jeden stupeň.

V Brně dne: 11. srpna 2022

Homoliak Ivan, Ing., Ph.D.
oponent