Posudek oponenta bakalářské práce

Student: Rádsetoulal Vlastimil
Téma: Detekce anomálií HTTP aplikací (id 23896)
Oponent: Homoliak Ivan, Ing., Ph.D., UITS FIT VUT

1. Náročnost zadání **obtížnější zadání**

Zadanie bolo mierne obtiažnejšie vzhľadom na bakalársky študijný program, keďže pracuje so state-of-the-art metódami umelej inteligencie.

2. Splnění požadavků zadání **zadání téměř splněno**

Zadanie bolo dostatočne splnené vo včšine bodov. U posledného bodu by som očakával rozšírnejšiu diskusiu problémoch navrhnutého riešenia a spôsoboch akým sa dá vylepšiť alebo efektívne využiť.

3. Rozsah technické zprávy **splňuje pouze minimální požadavky**

Práca obsahuje 35 strán latex-om sádzaného textu, čo na mňa pôsobí ako splnenie dolnej hranice.

4. Prezentační úroveň předložené práce **75 b. (C)**

Práca je pre čitateľa pochopiteľná, jednotlivé kapitoly na seba logicky nadväzujú. Rozsahy a prehľadnosť väčšiny kapitol sú prípustné. Výnimkou je sekcia 5.5, zaoberajúca sa výsledkami, ktorá je veľmi stručná a dosiahnuté výsledky hlbšie neanalyzuje. Táto sekcia prináša len jeden typ experimentu, ktorý je vyhodnotený dvoma spôsobmi.
Kapitola 2.4 menuje možné útoky na HTTP, pričom detailne popisuje len 3 útoky, bez akéhokoľvek predchádzajúceho zdôvodnenia. Autor uvádza na strane 16, že útoky, ktoré nevyzerajú ako anomálie, nie sú vhodné pre detekciu anomálnymi systémami. Táto veta je veľmi subjektívna a nesprávna keďže úlohou útočníka je svoj útok zamaskovať; a to hlavne v prípadoch keď vie aký detekčný systém je v cieľovom prostredí nasadený. Táto oblasť sa tiež označuje ako adversariálna klasifikácia a zaslúžila by si zmienku v práci. Na strane 20 nie je uvedená matematická notácia aktivačnej funkcie konkrétnej neurónovej siete.

5. Formální úprava technické zprávy **75 b. (C)**

Práca disponuje zvýšenou frekvenciou výskytu gramatických chýb a preklepov. Po typografickej stránke sa v práci nachádzajú tiež chyby. Jedná sa hlavne o chýbajúce bodky za citáciami a to najmä v názvoch obrázkov. Slovo chapter a section sa v angličtine píše s veľkým počiatočným písmenom. Tvrdá medzera pred citáciami všade chýba, niekedy chýba vôbec nejaká medzera. Slovo therefore je použité s chybou v celej práci. Poznámky pod čiarou sú v celej práci použité typograficky nesprávne.

6. Práce s literaturou **75 b. (C)**

Práca s literatúrou je na vyhovujúcej úrovni. Zvolené študijné prameňe sú relevantné a sú aj odlíšené od vlastných výsledkov. Rozsah práce s literatúrou je adekvátny bakalárskemu dielu. Poznamenal by som, že auto-enkódery sa používáju už niekoľko rokov na rôzne klasifikačné úlohy a to aj v oblasti sieťovej bezpečnosti. Preto je škoda, že práve takéto metódy nie sú vo väčšej miere citované a popísané.

7. Realizační výstup **80 b. (B)**

Práca má určitý realizačný výstup. No na dotiahnutie by bolo potrebné viac experimentov aj s prípadnými modifikáciami. Trénovanie auto-enkóderu by mohlo systematicky využiť napr. len výlučne normálne dáta a to z rozličných typov útokov, pričom by sa jednotlivé analýzy mohli robiť separátne a plynulo ich nadviazať na súčasnú (čisto unsupervised) metódu, ktorá zahrnula aj určité útoky do trénovania klasifikátorov normálnej prevádzky.

8. Využitelnost výsledků

Výsledky práce môžu byť využité v naväzujúcej diplomovej práci alebo tiež v ďalších bakalárskych projektoch zaoberajúcich sa auto-enkódermi.

9. Otázky k obhajobě

Uveďte aspoň dva ďalšie príklady využitia auto-enkóderov, ktoré v práci neboli spomenuté.

10. Souhrnné hodnocení **78 b. dobře (C)**

Práca je štandardne obtiažneho zadania. Zadanie bolo splnené takmer vo všetkých bodoch. Študent volil vhodnú literatúru, no niektoré relevantné zdroje chýbajú. Práca poskytuje prvotné výsledky, no chýba jej systematický prístup k experimentom. Celkovo prácu hodnotím stupňom **C (78 bodov)**. V prípade úspešne zvládnutej prezentácie z pozitívnou odozvou komisie je možné zvážiť aj zlepšenie známky.

Prohlášení: Uděluji VUT v Brně souhlas ke zveřejnění tohoto posudku v listinné i elektronické formě.

V Brně dne: 4. června 2021

Homoliak Ivan, Ing., Ph.D.
oponent