Posudek oponenta bakalářské práce

Student: Odehnal Tomáš
Téma: Mitigace DoS útoků s využitím neuronových sítí (id 21654)
Oponent: Wrona Jan, Ing., UPSY FIT VUT

1. Náročnost zadání **průměrně obtížné zadání**

Cílem bylo implementovat a porovnat dvě metody pro potlačení DoS útoků v počítačových sítích: 1) konvenční ACK Spoofing a 2) heuristickou metodu založenou na strojovém učení.

2. Splnění požadavků zadání **zadání splněno**

Zadání je splněno. U bodu 5. zadání bych ale čekal více vlastní invence, řešitel pouze následoval článek DeepDefense (stejný model i datová sada).

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

Technická zpráva patří mezi kratší, některé části by mohly být informačně bohatější.

4. Prezentační úroveň předložené práce **60 b. (D)**

Struktura teoretického rozboru je dobrá, ale informace by mohly být řazeny lépe. Práce např. několikrát zmiňuje zařízení DDoS Protector ještě před jeho představením. Také pro něj využívá alternativní názvy jako čistička provozu nebo DDP (zkratka ale není nikde vysvětlena). Mitigaci DDoS je možné provádet na samotných koncových zařízeních nebo pomocí nějakého síťového prvku. Práce se zabývá výhradně druhou variantou, ale čtenáře na tento fakt nijak neupozorňuje. Např. u metody SYN Cookies je to poměrně matoucí. Popis neuronových sítí, jejich praktického využití pro mitigaci DDoS a vyhodnocení výsledků nesvědčí o úplném pochopení této problematiky.

Prezentace výsledků je slabá. U metody ACK Spoofing je pouze obšírně popsáno že funguje, ale chybí např. měření propustnosti. Pro experimenty s neuronovou sítí řešitel exkluzivně používá metriku F1, která ale dává stejnou váhu metrikám precision i recall. Chybí diskuze, zda je pro cílovou doménu důležitější nižší míra falešně pozitivních nebo falešně negativních klasifikací. Obrázek 5.2 vysvětluje princip matice záměn, prakticky ale matice nikde zobrazená není. Experimenty s LSTM a GRU ve čtyřech dimenzích jsou důkladné, ale problém vidím především v prezentaci výsledků pouze pomocí spousty čísel a tabulek. Chybí vizualizace a smysluplná diskuse.

5. Formální úprava technické zprávy **65 b. (D)**

Práce obsahuje nevelký počet gramatických chyb. Poměrně časté jsou chyby vzniklé dodatečnou úpravou jako chybějící nebo opakující se slova ve větě. Typografických chyb je více, čitelnosti rozhodně nepomáhá používání prostředí description i v místech, kde patří obyčejné odstavce (např. strana 8 kde není výčet ani nijak nadepsaný, nebo strana 14 až 16). V textu se také vyskytují špatné symboly uvozovek a špatně použité řadové číslovky. Obrázky nejsou vždy jednotné (2.4 vs 2.5 a 2.6, 2.9 vs zbytek neuronových sítí) ani kvalitní (3.3, ten navíc obsahuje anglické popisky). U tabulek je potřeba vizuálně oddělit záhlaví od zbytku obsahu.

6. Práce s literaturou **75 b. (C)**

Práce cituje relevantní zdroje. Zdroj č. 14 uvádí pouze iniciály jmen autorů.

7. Realizační výstup **90 b. (A)**

Realizační výstup je silnější stránkou této práce. Implementace metody mitigace ACK Spoofing se stala součástí DDoS Protectoru a je reálně využívána. Zdrojový kód v jazyku C je přehledný a dostatečně komentovaný. Implementace metody využívající neuronovou síť je o poznání méně povedená, ale stále v pořádku (s přihlédnutím k tomu že je to spíše experimentální část práce).

8. Využitelnost výsledků

Přínos vidím především v modulu implementujícím ACK Spoofing, který nabízí možnost využití výsledků práce v praxi.

9. Otázky k obhajobě

- Tabulka 5.7 zobrazuje, že už při velikosti okna 1 dosahuje metrika F1 hodnoty 99 %. Znamená to, že pro téměř bezchybnou klasifikaci není kontext ostatních paketů vůbec potřeba?
- Je pro tuto doménu důležitější nižší míra falešně pozitivních nebo falešně negativních klasifikací?

10. Souhrnné hodnocení **70 b. dobře (C)**

Technická zpráva má mnohé nedostatky. Praktická část práce zabývající se konvenční metodou ACK Spoofing je kvalitní a přináší prakticky použitelný výstup. Bohužel druhá část opírající se o strojové učení mě na základě

prezentovaných výsledků o svých kvalitách příliš nepřesvědčila. Navrhuji hodnocení stupněm C.

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

V Brně dne: 30. května 2019

Wrona Jan, Ing.
oponent