Posudek oponenta závěrečné práce

České vysoké učení technické v Praze **Fakulta informačních technologií**

Student: Martin Petráček
Oponent práce: Ing. Tomáš Čejka
Název práce: Detekce anomálií založená na strojovém učení v reálném síťovém provozu
Obor: Teoretická informatika (bakalářský)

Datum vytvoření: 7. 6. 2015

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 5:*
1. Náročnost a další komentář k zadání	*1=mimořádně náročné zadání,* ***2=náročnější zadání,*** *3=průměrně náročné zadání,* *4=lehčí, ale ještě dostatečně náročné zadání,* *5=nedostatečně náročné zadání*

Popis kritéria:
Podrobněji charakterizujte diplomovou (bakalářskou) práci a její případné návaznosti na předchozí nebo běžící projekty. Dále posuďte, čím je zadání této ZP náročné. (U obtížnější ZP lze dále tolerovat některé nedostatky, které by u ZP standardní obtížnosti tolerovány nebyly; a naopak u jednoduché ZP mohou být zjištěné nedostatky hodnoceny přísněji.)

Komentář:
Tato práce se zabývá náročnou a velice důležitou problematikou v oblasti síťové bezpečnosti, konkrétně detekcí anomálií v síťovém provozu.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 4:*
2. Splnění zadání	***1=zadání splněno,*** *2=zadání splněno s menšími výhradami,* *3=zadání splněno s většími výhradami,* *4=zadání nesplněno*

Popis kritéria:
Posuďte, zda předložená ZP splňuje zadání. V komentáři uveďte body zadání, které nebyly zcela splněny, případně rozšíření ZP oproti původnímu zadání. Nebylo-li zadání zcela splněno, pokuste se posoudit závažnost, dopady a případně i příčiny jednotlivých nedostatků.

Komentář:
Zadání bylo kompletně splněno.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 4:*
3. Rozsah písemné zprávy	***1=splňuje požadavky,*** *2=splňuje požadavky s menšími výhradami,* *3=splňuje požadavky s většími výhradami,* *4=nesplňuje požadavky*

Popis kritéria:
Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části.

Komentář:
Text práce obsahuje všechny důležité části, neobsahuje žádné zbytečné části. Rozsah práce splňuje požadavky.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Věcná a logická úroveň práce	*80 (B)*

Popis kritéria:
Posuďte, zda předložená ZP je po věcné stránce v pořádku, případně vyskytují-li se v práci věcné chyby nebo nepřesnosti. Zhodnoťte dále logickou strukturu ZP, návaznosti jednotlivých kapitol a pochopitelnost textu pro čtenáře.

Komentář:
Text obsahuje nepřesnosti jako například dělení nulou (str. 21) a zvláštní terminologii (např. "nejanomálnější" str. 29).

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
5. Formální úroveň práce	*75 (C)*

Popis kritéria:
Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 12/2014, článek 3.

Komentář:
Text práce obsahuje překlepy (např. str. 7 nebo str. 12). Po typografické stránce obsahuje práce různé nedokonalosti jako chybné mezery (např. str. 4), vzorce na str. 21 by bylo vhodné vysázet lépe (podíl).

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Práce se zdroji	*75 (C)*

Popis kritéria:
Vyjádřete se k aktivitě studenta při získávání a využívání studijních materiálů k řešení ZP. Charakterizujte výběr studijních pramenů. Posuďte, zda student využil všechny relevantní zdroje nebo zda se pokoušel řešit již vyřešené problémy. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků a úvah, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami.

Komentář:
Společnost INVEA-TECH a.s. je v textu zmiňována nepřesně. Některé citace mají zvláštně uvedené jméno autora (např. [3], [9], [10]).
Ostatní citace se zdají být uvedeny v pořádku.
Práce obsahuje výroky, které by mohly a podle mého názoru měly být podložené citací: např. str. 12 "Síťový sken není přímo metodou útoku, ale útoku téměř vždy předchází", použít by se dalo např. Václav Bartoš, Martin Žádník: An Analysis of Correlations of Intrusion Alerts in an NREN. In: 2014 IEEE 19th International Workshop on Computer-Aided Modeling Analysis and Design of Communication Links and Networks (CAMAD). IEEE, 2014.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
7. Hodnocení výsledků, publikační výstupy a ocenění	*90 (A)*

Popis kritéria:
Vyjádřete se k úrovni dosažených hlavních výsledků ZP, např. k úrovni teoretických výsledků, nebo k úrovni a funkčnosti technického nebo programového vytvořeného řešení, apod. Případně také zhodnoťte, zda software nebo zdrojové texty, které nevytvořil sám student, byly v ZP použity v souladu s licenčními podmínkami a autorským právem. Popište případnou publikační činnost a získaná ocenění související s řešením této ZP.

Komentář:
Výsledky práce jsou na dobré úrovni a odpovídají rozsahu bakalářské práce. Zdrojové kódy jsou přehledné, ale bylo by dobré doplnit komentáře.

Hodnotící kritérium:	*Způsob hodnocení - nehodnotí se*
8. Komentář o využitelnosti výsledků	

Popis kritéria:
Uveďte, zda hlavní výsledky ZP rozšiřují již publikované známé výsledky a/nebo přinášející zcela nové poznatky. Uveďte možnosti využití výsledků ZP v praxi.

Komentář:
Výsledky práce jsou využitelné v praxi pro analýzu síťového provozu menších počítačových sítí.

Hodnotící kritérium:	*Způsob hodnocení - nehodnotí se*
9. Otázky k obhajobě	

Popis kritéria:
Uveďte případné dotazy, které by měl student zodpovědět při obhajobě ZP před komisí (body oddělte odrážkami).

Otázky:
Obrázek 4.2 zobrazuje závislost doby běhu algoritmu na počtu bodů. Podle str. 25 byla použita technologie OpenMP pro paralelizaci některých částí programu.
Byla naměřena závislost doby běhu algoritmu na počtu vláken?
Jakým způsobem by bylo možné zvýšit výkon výsledné aplikace? (množství zpracovaných záznamů o tocích za sekundu)

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
10. Celkové hodnocení	*95 (A)*

Popis kritéria:
Shrňte stránky ZP studenta, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení **nemusí** být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích 1 až 9.

Text hodnocení:
Výsledkem práce je implementace algoritmu pro detekci anomálií. Zadání bylo splněno a výsledný kód byl otestován.
Vzhledem k náročnosti zadání hodnotím známkou A.

Podpis oponenta práce: