Doc. Ing. Jiří Sýkora, CSc.

ČVUT- Fakulta elektrotechnická
katedra telekomunikační techniky
Technická 2
166 27 PRAHA 6

V Praze 22. srpna 2017

Oponentský posudek

doktorské disertační práce pana Ing. Václava Oujezského

Konvergované sítě a tomografie síťového provozu s využitím evolučních algoritmů

Posuzovaná disertační práce pana Ing. Václava Oujezského má rozsah 111 stran textu včetně seznamu použitých zkratek, symbolů, bohatého seznamu literatury, čtyř příloh, publikační činnosti předkladatele, jím vedených a konzultovaných diplomových prací a stručného profesního životopisu. Je rozčleněna do 9 kapitol. Svým zaměřením práce patří do oboru Telekomunikační technika a ze systémového pohledu se zabývá vysoce aktuální problematikou, spadající do oblasti moderních konvergovaných telekomunikačních sítí, především z pohledu detekce bezpečnostních hrozeb. Poněkud překvapivě pro mne působí zakomponování pojmu **tomografie** síťového provozu (i když vím, že je převzatý a v odborné literatuře dnes často používaný – pod tímto označením je myšleno studium interního chování a charakteristiky datového provozu a sítě pomocí externích koncových bodů). Jen chci připomenout, že dosud se pod pojmem **tomografie** rozumí **především** zobrazování v řezech. Zařízení použité pro tomografii se formálně nazývá tomograf. Nemusím snad připomínat její různé aplikace. Konečně, pojem **diagnóza** původně také patřil výhradně do lékařského prostředí. Uvedené není kritikou předkladatele, jen jiný pohled na pojmenovávání různých dějů.

K obsahu práce:

Po stručném úvodu a velmi podrobném přehledu současného stavu studované problematiky (kapitola 1 – pojem tomografie provozu, detekce anomálií provozu, role síťové tomografie) je 2. kapitola věnována teoretickému úvodu evolučních algoritmů (operátory – selekce, křížení, mutace, typům genetických algoritmů a možnostem jejich implementace v programovatelných prvcích). Následující dvě kapitoly jsou věnovány výčtu stěžejních publikací, na které bezprostředně navázal konkretizovaný výzkum, jehož výsledkem jsou splněné cíle disertace. V 5. kapitole - Testování programů pro vývoj a implementaci algoritmu - byl pro výběr vhodného vývojového prostředí proveden rozbor a testování několika vývojových a simulačních programů a jako vhodný pro implementaci vybrán Python verze 3.4 s prostředím pro vývoj PyCharm Professional 2016.2. 6. a 7 kapitola jsou věnovány testování 1. hypotézy analýzy přežití, 2. evolučních algoritmů. V prvém případě je ověřena možnost definovat provoz a jeho životní cyklus v závislosti na podobnosti. Pomocí analýzy

přežití lze verifikovat typ provozu a sestavit referenční mapu provozu. V druhém případě autor charakterizuje tři důležité hodnotící parametry optimalizačních algoritmů.

8. kapitola (návrh algoritmu a modelu) charakterizuje vlastní model, založený na konceptu detekce anomálií provozu na základě statistické metody s využitím stávajících funkcionalit síťových prvků NetFlow. Současně je prezentován funkční model síťové sondy (GDP – Genetic Decision Probe), kde jsou algoritmy implementovány. Konečně v 9. kapitole autor komentuje ze svého pohledu dosažené výsledky a doporučuje oblasti zaměření následného výzkumu.

Moje stanoviska k práci :

Aktuálnost zvoleného tématu

Název i obsah práce jsou problematikou patřící do oblasti konvergovaných technologií a procesů konvergence. Navíc mající dopad do v současnosti mimořádně důležité oblasti – síťové bezpečnosti. Proto je řešené téma nepochybně aktuální.

Splnění cílů disertační práce
Cíle práce jsou uvedeny na str.11 pomocí pěti zcela věcně a srozumitelně formulovaných bodů. Po seznámení se s prací **konstatuji jejich disertabilnost a splnění v celém rozsahu**. Připomínku mám jen k bodu 5 – „publikační činnosti“. Předpokládám, že bylo myšleno opublikování podstatných částí disertace, což je nutná podmínka. Potvrzuji její splnění, jinak nepatří do deklarovaných cílů.

Původní přínosné části disertace
Implicitní odpověď je již uvedena v předcházejícím odstavci – splnění cílů disertace. Konkrétní původní přínosné výsledky: navržen a implementován nový prvek – sonda síťových anomálií GDP, vytvořen nový algoritmus, vycházející ze statistické metody analýzy přežití v kombinaci s genetickým algoritmem. Provedené testy potvrdily funkčnost navrženého řešení.

Celkové zhodnocení práce
Disertační práce má jako celek potřebnou odbornou i grafickou úroveň, je stylisticky srozumitelná a obsahuje původní přínosné části. Konstatuji, že jádro disertace bylo potřebně opublikováno - viz soupis publikací předkladatele. Výsledky, kterých při řešení dané problematiky disertant dosáhl i další, vyplývající ze seznamu vědecké činnosti, svědčí o jeho vědecké erudici.

K práci mám následující dotazy:

1. Jak jste se podílel na projektech pro MV ČR o kterých se zmiňujete v úvodu ?
2. Skutečně jste čerpal ze všech 85 uvedených titulů v seznamu literatury ?
3. Popište bezpečnostní slabinu způsobenou provozem botnetových sítí.

<u>Závěr :</u>
Disertační práce pana Ing. Václava Oujezského přináší zcela nové poznatky, které jsou nepochybně využitelné v praxi. Disertant prokázal schopnosti samostatně vědecky pracovat a

podle mého názoru jednoznačně splňuje obecně uznávané požadavky k udělení akademického titulu.

Proto **doporučuji práci k obhajobě.**