OPONENTNÍ POSUDEK DISERTAČNÍ PRÁCE

Název disertační práce:	**Konvergované sítě a tomografie síťového provozu s využitím evolučních algoritmů**
Autor disertační práce:	**Ing. Václav Oujezský**
Akademický rok:	2016/17
Oponentní posudek vypracován:	21. 7. 2017
Autor oponentního posudku:	**Ing. Michal Polívka, Ph.D.**

SLOVNÍ HODNOCENÍ

Ing. Václav Oujezský vypracoval disertační práci na téma „Konvergované sítě a tomografie síťového provozu s využitím evolučních algoritmů“. Ing. Oujezský se zaměřil především na využití technik síťové tomografie a evolučních algoritmů v kybernetické bezpečnosti.

První kapitola textové části disertační práce je převážně rešeršní, shrnuje dosavadní stav řešené problematiky, hojně odkazuje na autory, na něž Ing. Oujezský ve svém výzkumu navazuje.

Druhá kapitola je, podobně jako kapitola první, teoretického charakteru. Ing. Oujezský v ní vysvětluje klíčové pojmy a technologie, o něž se ve své práci opírá. Kapitola přehledně shrnuje problematiku síťové tomografie, evolučních a genetických algoritmů, metod křížení, selekce apod.

Kapitola 3 v rámci jedné stránky shrnuje nejzajímavější zdroje, ze kterých autor čerpal. Rozbor stanoveného tématu je pak v úvodu kap. 4, která také popisuje v obecné rovině způsoby řízení botnetů.

Kapitola 5 pojednává o nástrojích, vývojových prostředí, jazycích a dalších technologiích, které byly otestovány a také využity při výzkumu, resp. v rámci implementační a ověřovací fáze. Bylo otestováno několik technologií, z nichž zajímavé je srovnání OMNeT++ a Python. Autor dal kvůli transparentnosti kódu a vyšší efektivitě vývoje přednost implementaci v Pythonu, byť modely tvořené v simulátoru OMNeT++ byly výkonnější. V daném kontextu se jeví být toto rozhodnutí správné.

Původní činnost autora s přímým vztahem k řešené problematice je popisována od kap. 6, ve které autor pojednává o provedeném testování hypotézy přežití. Kladně hodnotím přehlednost grafů. Ing. Oujezskému se podařilo ověřit, resp. prokázat, že je možné určit jednotlivé protokoly, z celkového síťového provozu po transformaci jeho zobrazení na křivky přežití, které jsou pro různé typy provozů různé. V případě obr. 6.5 – protokol UDP – by ale mohlo být zvoleno vhodnější měřítko.

V 7. kapitole jsou popsány testy evolučních algoritmů a vývojových prostředí, které byly Ing. Oujezským provedeny na známých příkladech vícekriteriálních optimalizačních problémů, jako je problém batohu nebo ZDT. V rámci popsané činnosti byly nalezeny optimální frekvence křížení a frekvence mutace.

Poslední obsahová kapitola, kapitola 8, pojednává o implementaci navrženého algoritmu a testování této implementace.

Po stránce typografické text neobsahuje žádné zásadní systematické chyby. Obecně je výskyt typografických i pravopisných chyb úměrný délce textu. Z textu je patrné, že vznikal v delším časovém období, což je zřejmě příčinou určité nejednotnosti – v části textu je např. použita desetinná čárka (mj. na str. 63), v části textu pak desetinná tečka, např. na str. 61, v různých částech textu je použit různý zápis slova chromozom (chromozóm vs. chromozom), byť jsou oba zápisy korektní. Většina původního přínosu autora je zapsána v programovém kódu, jenž je elektronickou přílohou disertační práce. Textová část pak zahrnuje spíše popis algoritmů a části řešení v teoretické rovině.

Aktuálnost tématu

Jedná se o aktuální téma, u něhož lze předpokládat růst významu v čase. V současné době je oblast kybernetické bezpečnosti, detekce hrozeb, šíření maligního softwaru, identifikace útočníků, analýza slabých míst v bezpečnosti atd. intenzivně zkoumána. Autor se ve své disertační práci rozhodl zaměřit na detekci anomálií síťového provozu, které mohou být indikátorem nežádoucí činnosti uživatele, útočníka nebo maligního kódu. Konkrétně je pak práce zaměřena na botnetové sítě, resp. protokoly, kterými jsou kontrolovány. V komerční praxi se touto problematikou intenzivně zabývají např. společnosti GREYCORTEX, Cisco, IBM a např. Darktrace. Jedná se o zcela aktuální problematiku, jejíž zvládnutí je nezbytné pro eliminaci soudobých hrozeb v oblasti kybernetické bezpečnosti.

Splnění cílů

Cíle, které autor v rámci disertační práce definoval, byly zcela naplněny.

Původnost a přínos

Originálním přínosem autora současné vědě je vytvořený detekční algoritmus, jehož potenciál, bude-li se dále rozvíjet, může zásadním způsobem ovlivnit současné metody detekce chování maligního softwaru v sítích.

Publikační činnost

Autor provedený výzkum publikoval v rámci četných konferencí, mj. např. TSP 2016, časopise International Journals of Advanced Research in Computer Science and Software Engineering a dalších. Ing. Václav Oujezský má vědeckou erudici.

Souhrnné hodnocení

Ing. Václav Oujezský se ve své disertační práci zabývá aktuální problematikou, po celou dobu výzkumu pravidelně na předložené téma publikoval. Disertační práce je po obsahové stránce kvalitní, původní a nevykazuje zásadní nedostatky. Předložená disertační práce zcela odpovídá uznávaným požadavkům k udělení akademicko-vědeckého titulu doktora v oboru Teleinformatika. Práci doporučuji k obhajobě.

OTÁZKY K OBHAJOBĚ

- Proč byly jako vstupy pro analýzu zvoleny protokoly NetFlow v 1 a 5 a ne NetFlow v9, resp. IPFIX?
- Bylo NetFlow nějak vzorkováno? Pokud ano, jednalo se o vzorkování na úrovni datového toku nebo na úrovni NetFlow?
- Byla srovnávána výkonnost a přesnost realizovaného řešení, oproti řešení obvyklým v komerční praxi, resp. např. s testovaným řešením Check Point GAiA?