POSUDEK OPONENTA ZÁVĚREČNÉ PRÁCE

I. IDENTIFIKAČNÍ ÚDAJE

Název práce:	**Detekce anomálií v sítích**
Jméno autora:	**Jiří Anděra**
Typ práce:	diplomová
Fakulta/ústav:	Fakulta elektrotechnická (FEL)
Katedra/ústav:	Katedra telekomunikační techniky
Oponent práce:	Ing. Jan Drchal, PhD.
Pracoviště oponenta práce:	Katedra počítačů

II. HODNOCENÍ JEDNOTLIVÝCH KRITÉRIÍ

Zadání **průměrně náročné**

Hodnocení náročnosti zadání závěrečné práce.

V závislosti na použitých datech a metodách hodnotím práci jako průměrně obtížnou. Pokud by byl síťový provoz zpracováván na úrovni net flows, bylo by třeba nastudovat a použít modernější metody a zpracovávat výrazně větší datové sady.

Splnění zadání **splněno**

Posuďte, zda předložená závěrečná práce splňuje zadání. V komentáři případně uveďte body zadání, které nebyly zcela splněny, nebo zda je práce oproti zadání rozšířena. Nebylo-li zadání zcela splněno, pokuste se posoudit závažnost, dopady a případně i příčiny jednotlivých nedostatků.

Zadání bylo splněno bez výhrad.

Zvolený postup řešení **správný**

Posuďte, zda student zvolil správný postup nebo metody řešení.

Celkový postup řešení považuji za správný. Přesto mám za to, že mohlo být otestováno více metod, než jen Isolation Forests (IF) a Local Outlier Factor (LOF) a více datových sad. Předpokládám, že lepších výsledků mohlo být dosaženo i zpracováním na úrovni net flows – student detekuje anomálie pouze na úrovni jednotlivých síťových spojení, ne jejich sekvencí.

Odborná úroveň **C - dobře**

Posuďte úroveň odbornosti závěrečné práce, využití znalostí získaných studiem a z odborné literatury, využití podkladů a dat získaných z praxe.

Z odborného hlediska je práce na dobré úrovni. Výhrady mám k rešeršní části práce, která je bohužel orientována více na typy útoků, než na metody detekce anomálií a charakteristiku dostupných dat. Rešerše je sice rozsáhlá, ale nejde příliš do hloubky. Zejména popis obou použitých metod IF a LOF považuji za nedostatečný. V sekcích popisujících analýzu testovaných datových sad, bych místo tabulek středních hodnot a rozptylu, nestandarně označovaného jako „variabilita“, očekával histogramy. Co se týče předzpracování dat, chybí zásadní detaily transformací IP adres a portů. Naopak oceňuji podrobnou diskusi k výsledkům jednotlivých experimentů. Prezentaci výsledků tabulkami jako 7.6 nebo 7.7 nepovažuji za šťastnou – vhodnější by bylo data vhodně vizualizovat.

Formální a jazyková úroveň, rozsah práce **D - uspokojivě**

Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku.

Text je psán češtinou s minimem překlepů, bohužel je však mnohdy těžce srozumitelný a působí spíše jako nekvalitní překlad z angličtiny. Formální zápis není v práci téměř použit a například metriky (kapitola 5) jsou z neznámého důvodu sázeny jako obrázky, a ne jako vzorce. Z typografického hlediska je práce jinak v pořádku.

Výběr zdrojů, korektnost citací **D - uspokojivě**

Vyjádřete se k aktivitě studenta při získávání a využívání studijních materiálů k řešení závěrečné práce. Charakterizujte výběr pramenů. Posuďte, zda student využil všechny relevantní zdroje. 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.
Rozsah citované literatury je sice značný, ale s výjimkou online zdrojů, se v drtivé většině jedná o články starší 10 a více let. Vzhledem k bouřlivému rozvoji, ke kterému došlo v odvětví strojového učení a jeho aplikací ke zpracovaní síťového provozu v posledních letech, stěží můžeme považovat řešeršní část práce za přehled state-of-the-art.

Další komentáře a hodnocení *Vyjádřete se k úrovni dosažených hlavních výsledků závěrečné práce, např. k úrovni teoretických výsledků, nebo k úrovni a funkčnosti technického nebo programového vytvořeného řešení, publikačním výstupům, experimentální zručnosti apod.*

III. CELKOVÉ HODNOCENÍ, OTÁZKY K OBHAJOBĚ, NÁVRH KLASIFIKACE

Shrňte aspekty závěrečné práce, které nejvíce ovlivnily Vaše celkové hodnocení. Uveďte případné otázky, které by měl student zodpovědět při obhajobě závěrečné práce před komisí.

Vzhledem k rozsahu odvedené práce, i přes výtky zmíňované výše, předloženou závěrečnou práci hodnotím klasifikačním stupněm **C - dobře.**

Datum: 25.8.2020 Podpis: