Posudek oponenta diplomové práce

Identifikační údaje

Název práce: Detekce anomálií na službách v počítačové síti

Jméno autora: Bc. Lukáš Kysilka

Typ práce: Diplomová

Fakulta: Fakulta jaderná a fyzikálně inženýrská (FJFI)

Katedra: Katedra matematiky

Oponent práce: Mgr. Jan Kohout, Ph.D., TruU, Inc.

Hodnocení jednotlivých kritérií

Zadání - průměrně náročné

Zadání vychází z předchozího výzkumného úkolu studenta, rozsahem je dostatečné pro diplomovou práci.

Splnění zadání - splněno

Zadání práce bylo splněno.

Zvolený postup řešení - správný

Postup řešení je v zásadě správný, práci ale chybí lepší návaznost a provázanost jednotlivých kapitol.

Odborná úroveň - B – velmi dobře

V práci jsou patrné rozdíly v odbornosti - zatímco teoretické poznatky z oblasti pravděpodobnosti a statistiky jsou na vyšší úrovni, doménová odbornost je nižší - např. problematika služeb v počítačové síti i detekce anomálií jsou popsány velmi povrchně, místy i nepřesně. V hodnocení odbornosti ale vycházím z toho, že primárním studijním oborem a zájmem autora práce je právě pravděpodobnost a statistika, nikoliv počítačové sítě.

Formální a jazyková úroveň - B – velmi dobře

Ve srovnání s výzkumným úkolem se jazyková úroveň práce zlepšila, nicméně práce nadále trpí místy neobratnými formulacemi. V práci se také objevují zbytečné anglicismy – forget perioda, warmup perioda apod.

Výběr zdrojů, korektnost citací - A - výborně

Zdroje jsou citovány odpovídajícím způsobem, vytkl bych několik odkazů na Wikipedii/WikiSkripta, kde určitě bylo možné nalézt jiný, odborně garantovaný zdroj.

Další komentáře a hodnocení

Za největší nedostatky práce považuji nižší odbornou úroveň v oblasti aplikační domény práce (problematika počítačových sítí a monitorování služeb v nich) a malý rozhled v oblasti detekce anomálií obecně. Tyto nedostatky pak vedou k velmi stručným a povrchním popisům řešené problematiky a horšímu zasazení práce do kontextu jiných prací z dané oblasti. Např. ilustrační příklady (typy anomálií apod.) by bylo vhodné volit právě z cílové domény (detekce anomálií v objemu komunikace na síťové služby) - pomohlo by to lepší provázanosti práce a pochopení, co je přesně cílem práce.

Naopak předností práce je dobrý postup návrhu detektoru, který je dostatečně teoreticky podložen a také experimentální část práce.

Celkové hodnocení, otázky k obhajobě, návrh klasifikace

Otázka:

Nalezení vhodné rodiny distribucí, kterou bude model používat, stále vyžaduje před nasazením detektoru pro novou službu ruční analýzu. Bylo by možné tento krok plně automatizovat tak, aby si detektor zvolil vhodnou distribuci sám v rámci adaptace na nová data? Jak by případně mohl být tento krok implementován?

Předloženou diplomovou práci hodnotím klasifikačním stupněm **B – velmi dobře.**

Datum: 19.5.2023

Podpis: