ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

POSUDEK OPONENTA ZÁVĚREČNÉ PRÁCE

I. IDENTIFIKAČNÍ ÚDAJE

Název práce:	Adversarialní strojové učení pro detekci škodlivého chování v síťové bezpečnosti
Jméno autora:	Michal Najman
Typ práce:	diplomová
Fakulta/ústav:	Fakulta elektrotechnická (FEL)
Katedra/ústav:	Katedra počítačů
Oponent práce:	Jan Bím
Pracoviště oponenta práce:	FEL ČVUT

II. HODNOCENÍ JEDNOTLIVÝCH KRITÉRIÍ

Zadání — **náročnější**

Hodnocení náročnosti zadání závěrečné práce.

The requirements of this thesis seem to be above average.

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.

In my eyes, the thesis fulfills all the requirements.

Zvolený postup řešení — **vynikající**

Posuďte, zda student zvolil správný postup nebo metody řešení.

The chosen method matches the problem very well and it is also well implemented.

Odborná úroveň — **A - výborně**

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

The scientific level of the thesis is outstanding. It required the student to apply a lot of knowledge from the literature and I would compare the quality to a regular scientific paper.

Formální a jazyková úroveň, rozsah práce — **B - velmi dobře**

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

The thesis is well structured, and the student demonstrated high level of proficiency in use of the language in general. However, the thesis contains few minor issues. First, I would recommend the student to review use of "a posteriori" and "posterior" as he uses very often just "posteriori" which I believe isn't customary. Second, he should also review how to form a noun from the verb "obfuscate". Next, few articles seemed incorrect. Finally, there were a few typos that could have been discovered by a spellchecker and the last term in the Proposition 3.4 should be conditioned on B, not M (though it is correct in the following equations).

Výběr zdrojů, korektnost citací — **A - výborně**

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.

The literature used to create this thesis is exhaustive and well selected. His own work is identifiably distinguished from prior art and his use of citations is adequate.

Další komentáře a hodnocení

ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

POSUDEK OPONENTA ZÁVĚREČNÉ PRÁCE

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. Vložte komentář (nepovinné hodnocení).

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.

In my opinion, the student demonstrated that he is able to compile knowledge from the literature, use it to create a novel approach to the problem and carry out an analysis that assesses performance of the new method. I appreciate the high scientific standard with which the work has been done and that the practical part has a very sound theoretical background.

Questions:

1) Would it be possible and if so, how would you change the kNN classifier to be also stochastic as it seems to be the important benefit of the adversarial one?
2) You mentioned in the introduction that the game-theoretical approach is only one of the possibilities. Do you know how does it compare to the reinforcement learning one?
3) What do you see as the potential future extensions of this work?

Předloženou závěrečnou práci hodnotím klasifikačním stupněm **A - výborně.**

Datum: 19.6.2019

Podpis: