POSUDEK OPONENTA ZÁVĚREČNÉ PRÁCE

I. IDENTIFIKAČNÍ ÚDAJE

Název práce:	Modelovani Různých Obranných Akci v Hrách pro Adverzativní Detekce
Jméno autora:	Martin Řepa
Typ práce:	bakalářská
Fakulta/ústav:	Fakulta elektrotechnická (FEL)
Katedra/ústav:	Katedra Počítačů
Oponent práce:	Jan Mrkos
Pracoviště oponenta práce:	Katedra Počítačů

II. HODNOCENÍ JEDNOTLIVÝCH KRITÉRIÍ

Zadání **náročnější**

Hodnocení náročnosti zadání závěrečné práce.

Zadání bakalářské práce je náročnější.

Splnění zadání **splněno s menšími výhradami**

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.

Odevzdaná práce splňuje zadání s menšími výhradami:

1. Škálovatelnost navrhovaných algoritmů není v práci dostatečně rozvedena. Co víc, podle prezentovaných výsledků (Tabulka 5.2) škálují navrhované algoritmy velmi špatně v počtu příznaků.
2. Modely hry uvedené v kapitole 4 jsou prezentovány jako obecné pro situace kdy zvyšování latence je platná strategie obránce. Ovšem například funkci R (rovnice 4.4c) má konkrétní tvar který dává smysl pro case study z kapitoly 5, ale zřejmě není použitelný pro všechny situace.

Zvolený postup řešení **vynikající**

Posuďte, zda student zvolil správný postup nebo metody řešení.

Student v práci úspěšně použil netriviální kombinaci state-of-the-art technik nalezení řešení zadaného problému.

Odborná úroveň **B - velmi dobře**

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

Odevzdaná práce je na dobré odborné úrovni s několika výhradami:

1. Neobvyklá a těžko formálně popsatelná negativní definice 3.1.4 bez zjevného důvodu této volby
2. Některé koncepty nejsou vhodně uvedeny. Například symbol pro příznakový vektor útočníka „f“ v nejsložitější části popisu modelu není jakkoliv popsán (str. 15, rovnice 4.4).
3. S výjimkou teorie her je popis teorie v kapitole 3 až příliš stručný, především co se píše neuronových sítí (str. 11). Ty jsou popsány stručněji, než by se dalo čekat ve vědeckém článku a nikoliv v rozsahu očekávatelném v bakalářské práci. Ani v apendixu pak není použitá architektura neuronových sítí dostatečně vysvětlena.

Formální a jazyková úroveň, rozsah práce **C - dobře**

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

Práce je vhodně a logicky členěna do kapitol. Práce je psaná čtivou a srozumitelnou angličtinou, přesto obsahuje množství množství drobných gramatických chyb, e.g.:

1. Str.9: „normal *for* game“, str. 20 – „challenges which need to be *encountered*“, str. 22: „purest *as* possible“, str. 23: „*Similarly as latency model…*“ …

Krom gramatických chyb jsou v textu také chyby ve formálním zápisu:

2. V rovnici 4.4b je v druhé části nesprávně použit symbol „f“ místo symboluy „d“. To umocňuje nesrozumitelnost této rovnice způsobenou chybejícím vysvětlením významu symbolů „d“ a „f“.

3. Definice 3.1.4 a 3.1.7 předpokládá dané strategické profily s, správně by bylo „pro dané s_{-i}"
4. Claim 2. předpokládá náhodné konstanty, pravděpodobně mělo být libovolné?
5. Značení tvrzení není jednotné. V práci je nekonzistentně použito *Theorem, Claim* a *Fact*. Theorem a Lemma by bylo vhodnější značení.
6. Jazyk použitý ve větách a definicích je příliš neformální, není jasné, co jsou předpoklady a co je tvrzení. Součástí definic a vět je často text který by v literatuře byl textem který by propojoval věty a definice. Viz například věta 3.1.1 která začíná "It can be proven …" nebo definice 4.2.2 začínající „To sum this up …"
7. Několika grafům chybí označení os (5.1, 5.5, 5.6). Popisy grafů jsou velmi stručné a neumožňují pochopení grafů bez čtení textu.
8. Graf 5.7 v textu zřejmě chybí úplně.

Výběr zdrojů, korektnost citací **B - velmi dobře**

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.

Práce obsahuje vhodné množství zdrojů, ne vždy jsou však vhodně citovány. Například Claim 1. není citován vůbec, Claim 2. je citován na konci znění lematu. Především v textu o neuronových sítích chybí vhodné citace.

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.

Práce je čtivá a řeší zajímavé téma. Velmi zajímavým výsledkem je možnost aplikace bez dostupnosti malicious dat. Přišlo by mi zajímavé vidět citlivost metody na přítomnost malicious dat v benign datasetu a použitelnost metody pro reward funkce v jiném tvaru než 4.4c.
V experimentální části 5.2 není jasné proč jsou zvoleny kroky po 4 000 epochách od 2 000 do 30 000, když podle grafu 5.2 hodnota hry konverguje již po cca 4 000 epochách. Každopádně diskuze overfittingu neuronových sítí je zajímavým důsledkem tohoto experimentu.

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.

Hodnocená bakalářská práce řeší aktuální, zajímavé a náročné téma v oblasti network security kombinací metod teorie her a neuronových sítí. Student v práci dosáhl zajímavých výsledků, které by si však zasloužili ještě hlubší prozkoumání. Práce je psána čtivě, místy však příliš stručně a často až příliš neformálně. Výsledný dojem z práce je však velmi dobrý a práce splňuje zadání.

Otázky k obhajobě:

1. Bylo by možné modifikovat navrhované metody na problém, kde reward funkce R není prakticky spočitatelná jako součin příznaků? Například pro lineární kombinaci příznaků či libovolnou funkci příznaků?
2. Jak moc je navrhovaná metoda citlivá na přitomnost malicous dat v benign datasetu?
3. Bylo by možné navržené metody použít pro počet příznaků >> 3? Jak, nebo jaké změny by to vyžadovalo?

Předloženou závěrečnou práci hodnotím klasifikačním stupněm **B - velmi dobře.**

Datum: 6.6.2019 Podpis: