

I. IDENTIFICATION DATA

Thesis name:	Modeling Various Defense Actions in Adversarial Anomaly Detection Games
Author's name:	Martin Řepa
Type of thesis :	bachelor
Faculty/Institute:	Faculty of Electrical Engineering (FEE)
Department:	Computer Science
Thesis supervisor:	Ing. Karel Durkota Ph.D.
Supervisor's department:	Computer Science

II. EVALUATION OF INDIVIDUAL CRITERIA

Assignment	challenging
<i>Evaluation of thesis difficulty of assignment.</i>	
The thesis was challenging as it required learning new disciplines (e.g. game theory, machine learning) their corresponding algorithms. Moreover, student had to study the problems in the network security domains.	

Satisfaction of assignment	fulfilled
<i>Assess that handed thesis meets assignment. Present points of assignment that fell short or were extended. Try to assess importance, impact or cause of each shortcoming.</i>	
Student has fulfilled the assignment by modeling the attacker and defender interaction as a game and proposed algorithms to compute player strategies. Student considered various defense actions and generalized the model to include various special cases. Student proposed algorithms to compute strategies and experimentally evaluated their performance.	

Activity and independence when creating final thesis	A - excellent.
<i>Assess that student had positive approach, time limits were met, conception was regularly consulted and was well prepared for consultations. Assess student's ability to work independently.</i>	
Martin is very goal-oriented and was proactive during the bachelor thesis. He was able to spot the new challenges and immediately propose solutions to them. We had regular meetings, where Martin was always in time. It was a pleasure to be his advisor.	

Technical level	A - excellent.
<i>Assess level of thesis specialty, use of knowledge gained by study and by expert literature, use of sources and data gained by experience.</i>	
The thesis focuses on a way of mixing machine learning, which is currently widely used, with game theory, that is appropriate for problems with multiple rational decision-makers. The interconnection of the two disciplines allows developing robust machine learning classifier for security domains, which is currently not performed by network security companies. I believe, that Martin acquired perspective to machine learning problems and will apply the gained knowledge in his future activities.	

Formal and language level, scope of thesis	B - very good.
<i>Assess correctness of usage of formal notation. Assess typographical and language arrangement of thesis.</i>	
Student formalized the problem setting and problem solution mathematically. Algorithms and claims with proofs seem to be sound. Although, there are some technical caveats, such as: <ul style="list-style-type: none"> - Student defines best-response against strategy profile (instead of a strategy of the opponent). - Players are defined as $N=\{a,d\}$, but strategies are referred as S_1 (instead of S_a or S_d). - In English "an utility" should be "a utility" 	

Selection of sources, citation correctness	A - excellent.
<i>Present your opinion to student's activity when obtaining and using study materials for thesis creation. Characterize selection</i>	

of sources. Assess that student used all relevant sources. Verify that all used elements are correctly distinguished from own results and thoughts. Assess that citation ethics has not been breached and that all bibliographic citations are complete and in accordance with citation convention and standards.

Citations seem to be appropriate to the work content.

Additional commentary and evaluation

Present your opinion to achieved primary goals of thesis, e.g. level of theoretical results, level and functionality of technical or software conception, publication performance, experimental dexterity etc.

Please insert your commentary (voluntary evaluation).

III. OVERALL EVALUATION, QUESTIONS FOR DEFENSE, CLASSIFICATION SUGGESTION

Summarize thesis aspects that swayed your final evaluation.

I have two questions for Martin:

- 1) Do you have any plans for evaluating the strategies in the real deployment?
- 2) What happens, if $\alpha_m < \alpha_b$ (meaning, that defender has higher costs for false-positives than having the network attacked). Would this setting results in classifier, that does not block nor increases any latency in the network?

I evaluate handed thesis with classification grade **A - excellent**.

Date: **30.5.2019**

Signature: