REVIEWER‘S OPINION OF FINAL THESIS

I. IDENTIFICATION DATA

Thesis name:	**Trust Models on Adversarial Distributed Security Agents**
Author's name:	Dita Hollmannová
Type of thesis :	master
Faculty/Institute:	Faculty of Electrical Engineering (FEE)
Department:	Dept. of Computer Science
Thesis reviewer:	Martin Rehak, Ph.D.
Reviewer's department:	Dept. of Computer Science

II. EVALUATION OF INDIVIDUAL CRITERIA

Assignment **challenging**

Evaluation of thesis difficulty of assignment.

The scope and complexity of the assignment topic would be sufficient for a Ph.D. thesis.

Satisfaction of assignment **fulfilled**

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.

The results are clearly sufficient for a master thesis.

Method of conception **correct**

Assess that student has chosen correct approach or solution methods.

The methodology is correct and the approach follows the guidelines and the literature recommended by the supervisor. On the other hand, the thesis could have benefited from a broader literature review and incorporation of a broader set of trust and reputation modeling techniques beyond the P2P security field.

More specifically:

Page 12, Eq. 3.1 - How is the local confidence determined?
Page 12, Sec. 3.3 - How is the set P determined exactly. Is there a time cutoff to eliminate old/outdated reports (This may be highly relevant for DHCP-assigned IPv4 addresses that may be unstable?)
Page 13, Section 3.3.1 - The confidence formula (Eq. 3.1) may potentially exhibit security weakness, where the mere fact of untrusted peers submitting their IDS score (regardless of that score value) lowers the confidence of the system. This may be used to effectively mount the DoS-like attack to render the whole mechanism ineffective by lowering the confidence. The better strategy might be the elimination of untrusted peers from the set P.
Page 13, Section 3.3.2 - Why do you normalize the trust value into the reduced interval, and not the full [0,1] interval. This might give some minimal weight also to completely untrusted peers? This may not be the optimal allocation of weights in the environment where the creation of a new peer is cheap and a plausible method of attack. On the other hand, the bias is in the same direction as the confidence bias in the Eq. 3.1. The attacker may flood the system with a high number of low-trust peers and introduce bias, but the confidence of such result would be low. Hence my DDoS-like designation from the previous comment, which will be developed further. Also, the confidence reported by the remote peer might have been considered in weighting?
Page 15, Section 3.5 - I like the IP-PeerID mapping mechanism. Let me just notice that this might be a potential security risk should the traffic origin in specific IP not be properly authenticated? (It almost never is for UDP and it gets tricky for the first TCP packet as well.)
Sections **3.6** and **3.7** address many of the attacks against the reputation systems known in the P2P context and their inclusion is highly appreciated. The structure of the chapters also drives the design of the experiments that assess the robustness of the system.
As for the **experiments**, I'd only suggest working with a larger set of peers (100 times or so). It is at that scale where many of the interesting phenomena emerge and when the problems of visibility, shared knowledge and "conflicts of interest" (such as attackers performing only a selective attack against a small subset of other peers) start to emerge.

Technical level	**A - excellent.**
Assess level of thesis specialty, use of knowledge gained by study and by expert literature, use of sources and data gained by experience.	
Commendable security methodology, good architecture, solid implementation and well-designed experiments.	

Formal and language level, scope of thesis	**A - excellent.**
Assess correctness of usage of formal notation. Assess typographical and language arrangement of thesis.	
Please insert your commentary.	

Selection of sources, citation correctness	**B - very good.**
Present your opinion to student's activity when obtaining and using study materials for thesis creation. Characterize selection 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.	
More extensive and detailed discussion of related work would have been appropriate, especially with regard to well-established field of trust modeling. (Jordi Sabater-Mir and his colleagues have authored several good reviews of the field.) This would have allowed the author to rely on existing trust models and benefit from the body of work in trust and reputation system field.	

III. OVERALL EVALUATION, QUESTIONS FOR DEFENSE, CLASSIFICATION SUGGESTION

Summarize thesis aspects that swayed your final evaluation. Please present apt questions which student should answer during defense.

The thesis clearly demonstrates the qualities of the candidate as an engineer. It shows that the candidate is capable to deliver well-designed solutions to correctly defined security problems, reason about the trade-offs involved in building secure distributed systems and concentrate on the essential elements of the design. The work as presented is not without gaps, but these are primarily driven by a healthy ambition to learn, deliver and improve. Dita is a highly talented engineer and I wish her good luck in her future successful career.

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

Date: **3.9.2020**

Signature: