Review report on the Ph.D. dissertation thesis
„Using Quantum Key Distribution for Securing Real-Time Applications“

submitted by Ing. Miralem Mehić
under supervision of Assoc. Prof. Miroslav Vozňák, Ph.D.

a) Evaluation of fulfilment of stated goals of the dissertation thesis
Goals of dissertation are clearly presented in Chapter 4 of the thesis that is placed after detailed and thorough state of the art proving that topic of this thesis represents up to date and very interesting research area that currently attracts many research groups worldwide. The first aim of the thesis is a new proposal for a Quality of Services-aware (QoS-aware) computational model in Quantum Key Distribution (QKD) networks, with an emphasis on real-time traffic transmitted within the network. This aim is mainly represented by design and development of QKD network simulator covering the most relevant components of this network. Note that this type of simulator was not available yet. The second aim is a verification of the proposed model in QKD network.

Chapter 5 (A Novel Proposal of Quantum Key Distribution Network Simulation Tool), Chapter 6 (Analysis of the Public Channel of Quantum Key Distribution Link) and Chapter 7 (A Novel Proposal of Quality of Service in Quantum Key Distribution Network) form the core of the thesis.

Chapter 5 clarifies that a student started his works by preparing a novel network simulation tool suitable for Network Simulator 3 (ns-3) environment, representing actually an extension of ns-3. Design of this new tool is described on component level, i.e. the main parts of this tool together with their linking is presented. A novel tool referred to as QKDNetSim is already publicly available. The author presents also a section providing an example of usage of implemented simulator with parameters summarized in Table 5.1. Therefore, aim 2 of the dissertation thesis is successfully fulfilled.

Chapter 6 and Chapter 7, especially, are aimed to fulfil the first goal of the thesis. These intentions are finished by adjustment of Greedy Perimeter Stateless Routing Protocol (GPSRQ) for QKD network that is introduced in Chapter 7.4. Simulation results of designed GPSRQ under several scenarios and in comparison with other two already introduced routing protocols are presented in Chapter 7.4.5. These results were obtained with help
of QKDNetSim and prove workability and benefits of the concept. Therefore, also aim 1 of the dissertation thesis is successfully fulfilled.

b) Comments on the procedure for solving the problem and the results of the dissertation, indicating the particular contribution of the student

Procedure of solving the problems addressed by this thesis is not difficult to follow and it is divided into understandable steps within the chapters. However, explaining text is lengthy in some parts, and the whole sentences are sometimes repeated. Nevertheless, a large amount of work that the student had to carry out during particular research stages can also be seen in between lines. These time-consuming works could actually be more emphasized in the text. For instance, I believe that not only one simulation scenario (described by values presented in Table 5.1) was prepared in order to verify behaviour of implemented QKDNetSim simulator, before preparing design of own QoS-aware packet processing solution for QKD networks. It is clear that QKDNetSim represents major contribution to the research community because no such simulator for QKD networks was available before.

Chapter 6 clarifies the impact of the performance of the public channel on performance of the quantum channel and vice versa, therefore, also on the overall performance of the QKD link. These measurement results are understood as another prerequisite for the further steps.

Chapter 7 starts with explanation of each of design decisions of new QoS-aware packet processing model (A Flexible Quality of Service Model for QKD Network - FQKD), among other things consisting of Greedy Perimeter Stateless Routing Protocol (GPSRQ) that was adjusted to fit the purposes of QKD networks. Again, only one simulation scenario is defined (attributes are included in Table 7.4) and although the results are analysed in detail and from several points of view, the author should try to compare the obtained results also in other simulation scenarios. Moreover, from a certain point of view, randomness of network topology that occurs within presented simulations makes a comparison of the presented simulation results and their mutual correlation actually a difficult task. Presented design reflects key requirement of current QKD networks especially, i.e. saving as much as possible of scarce key material used for ciphering. Benefits and also drawbacks of designed routing solution are clarified sufficiently. Most importantly, the obtained simulation results prove that introduced approach to the packet processing in the QKD networks leads to better performance when compared to previously introduced solutions.

Therefore, I consider the chosen procedure for solving the problem as adequate. The results of the dissertation that are appropriately summarized in Conclusions, are truly indicating significant contribution of the student and are already partly published.
c) An expression of relevance to the practice and development of the scientific discipline
Described state of the art presents also tests in real networks and applications of QKD networks and together with listed up-to-date references they are actually representing proof of the relevance of the thesis for current practice and there are no doubts about its contribution to the respective scientific discipline and research community, especially.

d) Comments on the formal aspects of the dissertation and language level
From the formal point of view, the reviewed thesis has very good level. The typing error rate is very low, language is understandable and text has appropriate level of complexity of used expressions. There are only infrequent minor errors, such as incorrect units of particular quantities in figures (e.g. Fig. 5.5).

e) Comments on the student’s publications
Candidate’s research relevant to the topic of the thesis is cited directly in the thesis. It consists of 5 papers published in 2015 and 2016. In Appendix A there is also a list of 12 other papers that student authored or co-authored. He has 15 and 17 scientific records according to Web of Science and Scopus, respectively. His h-index is 2, according to Web of Science and Scopus. Note that there are also several papers of Ph.D. candidate to be published soon in prestigious papers that are not mentioned in the thesis.

Therefore, the student has sufficient number of scientific records in literature.

f) The opponent’s unambiguous statement as to whether or not he recommends a dissertation for defence
Based on the submitted thesis, available data about research work until now, research papers of the Ph.D. candidate and my comments summarized into this review, I highly recommend Ing. Miralem Mehić to defend his Ph.D. thesis successfully.

Questions
1. What are the most important limitations of your simulator of QKD networks, if any?

2. Page 83-84: Description of Fig. 7.4c in text seems to be not in agreement with the content of the figure. Could you explain this issue?

3. Page 101: In my opinion, the comparison you present should take into account that timers of routing protocols (e.g. OSPF) can be adjusted. How will it change the obtained results?

4. How did you determine values that are summarized in Table 5.1 as a description of the simulation scenario?
5. What is the main cause of significant differences in obtained throughput of QKD transmission system in laboratory environment and real network (Fig. 6.1 vs. Fig. 6.6)?

6. Why did you select the routing solution calculating metric from geographical distance (starting from page 88)? Are there any other possibilities that could be useful for these QKD networks?

7. Could you explain how simulation scenario discussed in Chapter 7.4.5 reflects Quality of Service management you designed in the previous chapters? Also please explain where is placed the source and the destination node of CBR application that is used as traffic generator for this simulation.

8. Could you explain the results presented in Fig. 7.13? Why is packet delivery ratio (PDR) almost 100% for each of the protocols in case of 20 or 40 nodes, however, it is very low for 30 nodes, for instance.

This review was written in Brno, Czech Republic,

on 16th May 2017 by

Jan Jeřábek
Assoc. Prof. Jan Jerabek, Ph.D.
Department of Telecommunications
Faculty of Electrical Engineering and Communication
BRNO UNIVERSITY OF TECHNOLOGY
Technicka 12, Brno, 616 00, Czech Republic
T: +420 541 146 982
jerabekj@feec.vutbr.cz
www.vutbr.cz