Toward Designing a Quantum Key Distribution Network Simulation Model

Miralem MEHIC[1], *Peppino FAZIO*[2], *Miroslav VOZNAK*[1], *Erik CHROMY*[3]

[1]Department of Telecommunications, Faculty of Electrical Engineering and Computer Science, VSB–Technical University of Ostrava, 17. listopadu 15, 708 00 Ostrava-Poruba, Czech Republic
[2]Department of Computer Science, Modeling, Electronics and Systems Engineering, University of Calabria, Via Pietro Bucci, 87036 Arcavacata di Rende (CS), Italy
[3]Institute of Telecommunications, Faculty of Electrical Engineering and Information Technology, Slovak University of Technology in Bratislava, Ilkovicova 3, 812 19 Bratislava, Slovak Republic

miralem.mehic.st@vsb.cz, pfazio@dimes.unical.it, miroslav.voznak@vsb.cz, chromy@ut.fei.stuba.sk

DOI: 10.15598/aeee.v14i4.1914

Abstract. *As research in quantum key distribution network technologies grows larger and more complex, the need for highly accurate and scalable simulation technologies becomes important to assess the practical feasibility and foresee difficulties in the practical implementation of theoretical achievements. In this paper, we described the design of simplified simulation environment of the quantum key distribution network with multiple links and nodes. In such simulation environment, we analyzed several routing protocols in terms of the number of sent routing packets, goodput and Packet Delivery Ratio of data traffic flow using NS-3 simulator.*

Keywords

Network simulation, Quantum Key Distribution, routing protocols.

1. Introduction

Quantum Key Distribution (QKD), based on the laws of physics rather than the computational complexity of mathematical problems, provides an Information Theoretically Secure (ITS) way of establishing symmetrical binary keys between two geographically distant users. The keys are secure from eavesdropping during transmission and QKD ensures that any third party's knowledge of the key is reduced to the level of guessing. Due to the specificity of QKD link which requires optical and Internet connection between the network nodes, it is very costly to deploy a complete testbed containing multiple network hosts and links to validate and verify a certain network protocol or a specific network algorithm. The network simulators in these circumstances save a lot of money and time in accomplishing this task.

2. State of the Art

A simulation environment offers the creation of complex network topologies, a high degree of control and repeatable experiments, which in turn allows researchers to conduct exactly the same experiments and confirm their results. Unlike for conventional networks, there are few software applications dealing with QKD. Quantum Cryptography Protocol Simulator [1] developed using C/C++ architecture is able to analyze the Quantum Bit Error Rate (QBER) and eavesdropper influence on the performances of the quantum channel when BB84 or B92 QKD protocol is used. A similar application is reported in [2]. Object-oriented simulation for QKD protocols was reported in [3] while an event-by-event simulation model and polarizer as simulated component for QKD protocols with the presence of eavesdropper and misalignment measurement as scenarios were reported in [4]. A simulation framework for QKD protocols using OptiSystem was reported in [5], and a modeling framework designed to support the development and performance analysis of practically oriented QKD system representations was reported in [6]. Yet all of these applications deal only with optical channel performance or QKD protocols and disregard the public channel and the entirety of the protocol stack above the quantum channel. To the best of our knowledge, applications for simulating QKD networks with multiple nodes and links are not available. There-

fore, in this paper, we describe the design of simplified simulation environment of QKD network with multiple links and nodes. In such simulation environment, we analyze several routing protocols in terms of the number of sent routing packets, goodput and Packet Delivery Ratio of data traffic flow.

The rest of the paper is organized as follows: Section 3. provides the basis of the QKD and describes the hop-by-hop communication approach used in QKD network. The simulation setup is presented in Section 4. , while in Section 5. we provide an evaluation of obtained result and discuss the broader aspects of our approach. Section 6. concludes this study and outlines the future work.

3. Fundamentals of Quantum Key Distribution

QKD networks differ from the traditional communication network in several aspects. One of the main differences is reflected in the implementation of the network link. A QKD link employs two distinct communication channels between the parties: the quantum channel, which is used for transmission of quantum key material encoded in certain photon properties such as polarization or phase, and the public channel, which is used for verification of exchanged key material and transmission of encrypted data (Fig. 1). A quantum channel is always a point-to-point connection between exactly two nodes [7] while public channel can be realized as any conventional connection which may include arbitrary number of intermediate devices [8].

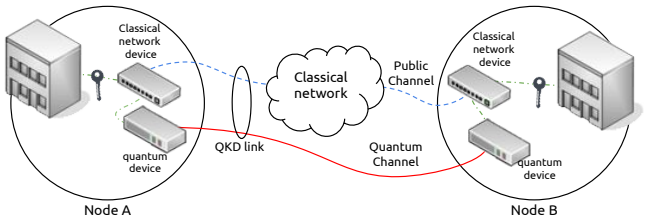

Fig. 1: Overview of a QKD link between two QKD nodes which consist of an optical quantum channel (continuous red line) and a public/classical channel (dashed blue line).

A second important feature of the QKD network is reflected in the limited length of the links and maximal transfer rate. Namely, due to absorption and scattering of polarized photons [9], [10], [11] and [12]], the quantum channel can be realized by a direct optical fiber or free line of sight only for a certain distance. An equally important feature of the link is the amount of key material that can be established in a unit of time and this amount may vary due to humidity, temperature, the stability of devices, global radiation, pressure, dust, sunshine duration or other factors [7] and [13]. However, it mostly depends on the length of the link and it is often referred to as the key generation rate or simply key rate.

The maximum length of the link and the key rate are usually used to evaluate the QKD system. A chronological look at previously deployed QKD networks reveals a rapid improvement in the development of quantum equipment: QKD systems implemented in 2002 in the DARPA BBN QKD network were able to achieve a key rate of approximate 400 bps over 10 km [14]; In 2007 in SECOQC, the maximal key rate was 3.1 kbps over 33 km [15], while the solutions presented in 2009 in Tokyo achieved a key rate of 304 kbps over 45 km [16]. Although key rate results of up to 1 Mbps have been reported [17], [18] and [19], such solutions are limited to very short distances. Therefore, for current systems, the distance at which a QKD link is possible is roughly limited to 100 km in optical fibers, while the stable key rate is currently restricted to a few tens or hundreds of kbps depending on the distance [11] and [13].

Due to the limited key rate, links are organized in the following way: both endpoints of the corresponding link have key storages with limited capacity which are gradually filled with the new key material, which is subsequently used for the encryption/decryption of data flow and QKD devices constantly generate keys at their maximum key rate until the key storages are filled [20]. The type of used encryption algorithm and the amount of network traffic to be encrypted determines the speed of emptying the key storage, often referred as key consumption rate, while the key rate of the link determines the key charging rate [7], [14] and [21]. If there is no enough key material in the storage, encryption of data flow cannot be performed [22] and the link can be characterized as "currently unavailable". To provide Information-Theoretically Secure (ITS) communication, in the public channel the key tends to be applied with a One-Time Pad (OTP) cipher, which requires the length of the key to be the same as the length of the message that is to be encrypted. However, if the ratio between the charging and consumption rates is not appropriate [23] and [24], OTP cannot be used due to the lack of key material, and using less secure algorithms that do not require too much material such as Advanced Encryption Standard (AES) becomes inevitable [25].

QKD networks also differ from the conventional networks in terms of network organization. Although there are theoretical and pioneering results in the field of quantum repeaters and quantum relays [26], [27] and [28], in practice they remain unachievable with current technology [11] and [29]. Therefore, the communication within network usually takes place in a hop-by-hop [30] or in a key relay manner [14] and [31]. Both methods rely on the assumption that all nodes along the path between the sender and receiver must be fully

trusted [22] and [32]. However, this restriction can be overcome when multiple path-based communication or Quantum Network Coding [33] is used.

3.1. Routing in QKD Networks

Due to the specificity of QKD networks, the two requirements for the selection of routing protocol are emphasized:

- Since the communication is usually performed on hop-by-hop basis, it is necessary to minimize the number of links by choosing the shortest path due to key material consumption [7].
- Given that the main objective of QKD is to provide ITS communication, routing packet needs to be either encrypted and authenticated or at least authenticated [7]. This entails that the number of routing packets in the network needs to be minimized.

4. Simulation Setup

To test the performances of various routing protocols in QKD network, we set up a network simulation of 6 fixed nodes forming the topology shown in Fig. 2 which was simulated in Network Simulator 3 (NS-3) of version DCE 1.8 [34]. As noted above, if there is sufficient key material to encrypt the data traffic that flows over the QKD link, the link is seen as "available". Otherwise, the QKD link is noted as "currently unavailable". To simulate such behaviour of QKD link, we used the propagation delay of the point-to-point connection between the nodes. At each point-to-point link, the "virtual buffer" with initial amount of key material is installed. The buffers are referred as "virtual" because they do not perform real encryption of data flow nor they use real key material. Virtual buffers only measure the traffic and reduce its value by the packet payload length. In this way, virtual buffers imitate the OTP cipher from the point of the key material consumption.

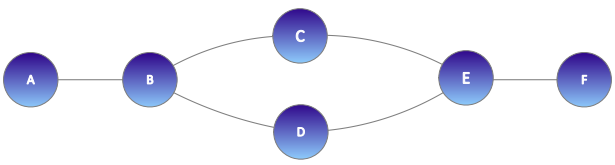

Fig. 2: Topology of simulated network in which data UDP flow of rate 160 kbps between nodes A and F is established. Nodes are connected with point-to-point links.

When the key material is depleted, that is, when the link is marked as "currently unavailable", the propagation delay of the point-to-point link is increased to value of 100 seconds stopping any kind of communication. Otherwise, the propagation delay is set to 2 ms, which is the default value of point-to-point connection in case when the QKD link is seen as "available". The buffers are constantly charged with new key material of constant rate, which means the simulated QKD link can switch from the "available" to "currently unavailable" state and vice versa.

The reason for this simulation setup is a simple imitation of the availability of QKD link. Using of other means, such as the shutdown of network interface will result in informing the routing protocol which would automatically broadcast this information. The described simulation setup provides a simple imitation of QKD network, and allows us to test various routing protocols in a very simple way.

Table 1 presents the nodal model parameters including the key generation rate, charging key rate, packet size, and data traffic parameters. The parameters not given here were the default parameters of the NS-3 simulator.

Tab. 1: Parameter values of the simulation.

Parameter	Value
Total number of nodes	6
Packet Size	512 Bytes
Packet Traffic Type	UDP; CBR
Packet Traffic Rate	160 kbps
Initial amount of key material (link A–B)	6422.528 kBytes
Initial amount of key material (link B–C)	6422.528 kBytes
Initial amount of key material (link B–D)	6422.528 kBytes
Initial amount of key material (link D–E)	1429.648 kBytes
Initial amount of key material (link C–E)	1179.648 kBytes
Initial amount of key material (link E–F)	6422.528 kBytes
Charging key rate for all links	12.8 kBytes
Total Simulation time	300 seconds

5. Simulation Results

The parameters in Tab. 1 indicate the links C–E and D–E have the least amount of initial key material. As tested routing protocols have no information about the status of virtual buffers, they need to choose between one of the two available paths: A–B–D–E–F or A–B–C–E–F. Yet, after a while, the usage of any of these paths results in a disruption of communication since the available key material is quickly consumed. Then, the routing protocol needs to choose an alternative route while the depleted link is charging. Further, when the used link is depleted again, the routing protocol switches to an alternate path and so on.

Routing protocols are broadly classified into proactive and reactive routing protocols. In a reactive routing protocol such as AODV, routing paths are searched only when needed, mainly by flooding the network. The discovery procedure terminates when either a route has been found, or no route is available after all route permutations have been checked. Conversely, the proactive routing protocol, such as DSDV, OLSR or OSPF, continuously evaluate routes to all reachable nodes and attempt to maintain consistent, up-to-date routing information, by exchanging periodically its routing tables (OLSR, DSDV) or exchanging network topology information (OSPF) [35].

AODV is an on-demand variation of distance vector reactive routing protocol which determines a route to a destination only when a route is required. Each node maintains a table with information referring to the first neighbor. This table is updated using periodic Hello messages that are locally broadcast messages utilized to indicate link availability. By default, AODV broadcast Hello messages each second and failure to receive Hello message in "allowed hello loss interval", which is set to 2 seconds by default, indicates a loss of connectivity to that neighbor. When a route for the desired destination is not available or when a routing table entry expires after a predetermined period, a route discovery request is flooded through the network. The obtained route is maintained as long as it is needed by the source.

OSPF is a widely deployed link-state routing protocol which means that each router maintains a link-state database describing the network topology. This database is updated using Link State Announcement (LSA) update information. From the link-state database, each router constructs a tree of shortest paths with itself as the root. By default, OSPF floods LSA each 30 minutes and it exchanges Hello packets to establish and maintain a neighbor relationship on each 10 seconds. If a node does not receive a Hello message from a neighbor within a "dead interval time", OSPF modifies its topology database to indicate that the neighbor is unavailable. This fixed time interval specifies the time that OSPF waits before declaring the neighbor node to be unavailable. By default, it is set to four times the default hello interval, which is 40 seconds in case of point-to-point networks.

OLSR is based on a proactive link-state approach, which makes it very similar to OSPF. It uses Hello and Topology Control (TC) routing messages to discover and disseminate link-state information through the network. OLSR reduces the control traffic overhead by using Multipoint Relays (MPR), which is the key idea behind OLSR. The MPR node is a node's one hop neighbor which has been chosen to forward packets. Instead of pure flooding of the network, packets are forwarded by node's MPRs. This delimits the network overhead, thus being more efficient than pure link state routing protocols. By default, OLSR node sends Hello messages each 2 seconds while TC messages are exchanged each 5 seconds. The holding time is usually three times the Hello message period. Therefore, a link breakage is detected after 6 seconds in the worst case.

DSDV is the most popular proactive routing protocol based on the distributed Bellman-Ford algorithm. In DSDV, each node maintains two tables. One of them is the permanent routing table in which all of the possible destinations within the network, the address of next hop and the total number of hops to reach the destination are listed. Each node is in charge to periodically broadcast its routing table to its neighbor nodes by using periodic update packets based on periodic route update interval which is set to 15 seconds by default. After receiving of the update packet, the neighbor node updates its routing table by incrementing the number of hops by one and forwards the packet further in the network. The process is repeated until all the nodes in the network receive a copy of the update packet with a corresponding value. To avoid the formation of routing loops, entries in the routing table are marked with a sequence number. In addition to regular periodic updates, DSDV uses triggered updates when the network topology suddenly changes. The main purpose of these updates is to advertise the information that has changed since the last periodic update. However, if a periodic and triggered update occurs in a short period of time, the values may be merged and the only periodic update will be performed. To limit the propagation of unstable information, the transmission of triggered updates is delayed using settling time which is recorded in the second DSDV table for each destination node. By default, settling time is set to 5 seconds [35].

Table 2 presents the obtained values based on the number of sent routing data. Packet Delivery Ratio (PDR) which is calculated as the ratio of received and sent application packets, is used to assess the effectiveness of the routing protocol within the specified simulation environment. Table 2 shows that AODV reactive routing protocol sends the largest number of routing packets and has the same PDR as OSPF routing protocol. However, AODV floods route request and hello

Tab. 2: Comparison of the obtained values. The number of routing packets and Packet Delivery Ratio (PDR) which is calculated as the ratio of received and sent application packets is used to assess the effectiveness of the routing protocol.

	Routing data		**Application data**
Routing protocol	Packets	Bytes	PDR (%)
AODV	6714	335728	35.645
OLSR	4441	372102	73.5627
OSPFv2	1268	107392	35.645
DSDV	914	65580	44.2149

Fig. 3: Comparison of traffic generated by routing protocols.

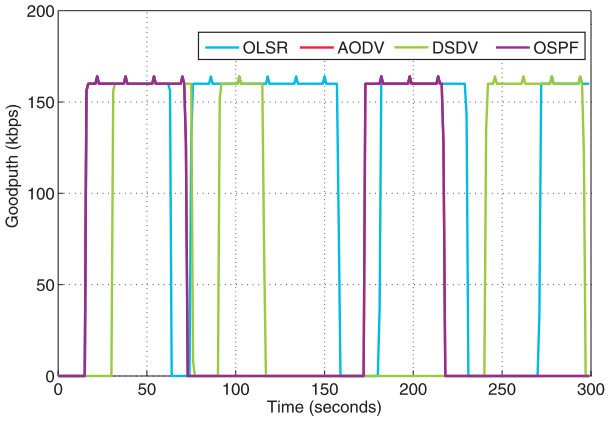

Fig. 4: Goodput of the UDP data flow between nodes A and F.

messages which result in a fast reduction of available key material. This is evident from Fig. 3 where it is shown that in last 60 seconds of the simulation there is no AODV traffic due to lack of available key material.

OSPF sends Hello packets each 10 seconds and on 40^{th} second of the simulation, OSPF exchange the LSA information which is shown as a large peak of OSPF graph on Fig. 3. Due to the large value of "dead interval time", OSPF is not able to react quickly to the changes of the network topology which finally results in a low PDR.

On the other side, the small value of hello and dead interval allows OLSR to react quickly to the changes of a network topology which results in the highest PDR. OLSR floods Hello and TC packets each 2 and 4 seconds, respectively, which results in almost constant propagation of the routing packets. In addition, the flooding based on MPR reduces the consumption of scarce key material when compared to AODV. Although OLSR provides best results in the view of PDR, OLSR is based on constant flooding of the network which is contrary to the requirements specified in Subsection 3.1.

Finally, as shown in Fig. 3, distribution of DSDV packets is almost regular with the period of 15 seconds. DSDV sends the least number of packets and achieves better PDR then well-known OSPF.

The results from Tab. 2 are shown in Fig. 4 from where it can be seen that AODV and OSPF have the same selection of paths which results in the same PDR. OLSR and DSDV alternately choose the available path which provides the better PDR.

6. Conclusion

In this paper, we presented a simple way to mimic QKD network. In such an environment, we tested several routing protocols with reference to the number of routing packets and Packet Delivery Ratio. It is important to stress that none of the simulated routing protocols has built-in mechanisms of congestion detection or QoS mechanisms. Although OSPF routing protocol was used in previously deployed QKD networks [20], [36] and [37], we have shown that DSDV provides better network performances since it provides better PDR with a smaller amount of routing information. On the other hand, AODV and OLSR seem not to be appropriate for QKD network due to the large amount of routing data that are flooded throughout the network.

The main contribution of this paper is the presentation of a simple way to mimic the behavior of QKD network and the performance analysis of the different routing protocols in such simulated environment.

Our future work will focus on developing dedicated simulation module which will allow a more detailed analysis of QKD network.

Acknowledgment

The research received a financial support from the SGS grant No. SP2016/170, VSB–Technical University of Ostrava, Czech Republic.

References

[1] NIEMIEC, M., L. ROMANSKI and M. SWIETY. Quantum Cryptography Protocol Simulator. In: *Communications in Computer and Information Science*. Krakow: Springer, 2011, pp. 286–292. ISBN 978-3642215117. DOI: 10.1007/978-3-642-21512-4_34.

[2] PERESZLENYI, A. Simulation of Quantum Key Distribution with Noisy Channels. In: *Proceedings of the 8th International Conference on Telecommunications (ConTEL)*. Zagreb: IEEE, 2005, pp. 203–210. ISBN 953-184-081-4. DOI: 10.1109/CONTEL.2005.185853.

[3] ZHANG, X. and Q. WEN. Object-Oriented Quantum Cryptography Simulation Model. In: *Third International Conference on Natural Computation*. Haikou: IEEE, 2007, pp. 7–10. ISBN 978-0-7695-2875-5. DOI: 10.1109/ICNC.2007.509.

[4] ZHAO, S. and H. DE RAEDT. Event-by-event Simulation of Quantum Cryptography Protocols. *Journal of Computational and Theoretical Nanoscience*. 2008, vol. 5, no. 4, pp. 490–504. ISSN 1546-1955. DOI: 10.1166/jctn.2008.007.

[5] BUHARI, A. An efficient modeling and simulation of quantum key distribution protocols using OptiSystem^{TM}. In: *IEEE Symposium on Industrial Electronics and Applications (ISIEA)*. Bandung: IEEE, 2012, pp. 84–89. ISBN 978-1-4673-3004-6. DOI: 10.1109/ISIEA.2012.6496677.

[6] MAILLOUX, L. O., J. D. MORRIS, M. R. GRIMAILA , D. D. HODSON, D. R. JACQUES, J. M. COLOMBI, C. V. MCLAUGHLIN and J. A. HOLES. A Modeling Framework for Studying Quantum Key Distribution System Implementation Nonidealities. *IEEE Access*. 2015, vol. 3, iss. 1, pp. 110–130. ISSN 2169-3536. DOI: 10.1109/ACCESS.2015.2399101.

[7] KOLLMITZER, C. and M. PIVK. *Applied quantum cryptography*. New York: Springer, 2010. Lecture notes in physics, 797. ISBN 978-3642048319.

[8] DIANATI, M. and R. ALLEAUME. Architecture of the Secoqc Quantum Key Distribution network. In: *First International Conference on Quantum, Nano, and Micro Technologies*. Gosier: IEEE, 2007, pp. 13–19. ISBN 0-7695-2759-0. DOI: 10.1109/ICQNM.2007.3.

[9] ALLEAUME, R., F. ROUEFF, E. DIAMANTI and N. LUETKENHAUS. Topological Optimization of Quantum Key Distribution Networks. *New Journal of Physics*. 2009, vol. 11, iss. 7, pp. 1–25. ISSN 1367-2630. DOI: 10.1088/1367-2630/11/7/075002.

[10] GISIN, N., G. RIBORDY, W. TITTEL and H. ZBINDEN. Quantum Cryptography. *Reviews of Modern Physics*. 2002, vol. 74, iss. 1, pp. 145–195. ISSN 0034-6861. DOI: 10.1103/RevModPhys.74.145.

[11] SALVAIL, L., M. PEEV, E. DIAMANTI, R. ALLEAUME, N. LUETKENHAUS, NORBERTE and T. LANGER. Security of trusted repeater quantum key distribution networks. *Journal of Computer Security*. 2010, vol. 18, no. 1, pp. 61–87. ISSN 1875-8924. DOI: 10.3233/JCS-2010-0373.

[12] SCARANI, V., H. BECHMANN-PASQUINUCCI, N. J. CERF, M. DUSEK, N. LUETKENHAUS and M. PEEV. The security of practical quantum key distribution. *Reviews of Modern Physics*. 2009, vol. 81, iss. 3, pp. 1301–1350. ISSN 0034-6861. DOI: 10.1103/RevModPhys.81.1301.

[13] DUSEK, M., N. LUETKENHAUS and M. HENDRYCH. Quantum Cryptography. *Progress in Optics*. 2006, vol. 49, iss. 1, pp. 381–454. ISSN 0079-6638. DOI: 10.1016/S0079-6638(06)49005-3.

[14] ELLIOTT, C. and H. YEH. DARPA Quantum Network Testbed. In: *BBN TECHNOLOGIES* [online]. 2007. Available at: `http://www.dtic.mil`.

[15] PEEV, M., C. PACHER, R. ALLEAUME, C. BARREIRO, J. BOUDA, W. BOXLEITNER, T. DEBUISSCHERT, E. DIAMANTI, M. DIANATI, J. F. DYNES, S. FASEL, S. FOSSIER, M. FUERST, J.-D. GAUTIER, O. GAY, N. GISIN, P. GRANGIER, A. HAPPE, Y. HASANI, M. HENTSCHEL, H. HUEBEL, G. HUMER, T. LAUNGER, M. LEGRE, R. LIEGER, J. LODEWYCK, T. LORUENSER, N. LUETKENHAUS, A. MARHOLD, T. MATYUS, O. MAURHART, L. MONAT, S. NAUERTH, J.-B. PAGE, A. POPPE, E. QUERASSER, G. RIBORDY, S. ROBYR, L. SALVAIL, A. W. SHARPE, A. J. SHIELDS, D. STUCKI, M. SUDA, C. TAMAS, T. THEMEL, R. T. THEW, Y. THOMA, A. TREIBER, P. TRINKLER, R. TUALLE-BROURI, F. VANNEL, N. WALENTA, H. WEIER, H. WEINFURTER, I. WIMBERGER, Z. L. YUAN, H. ZBINDEN and A. ZEILINGER. The SECOQC Quantum Key Distribution Network in Vienna. *New Journal of Physics*. 2009, vol. 11, iss. 7, pp. 1–37. ISSN 1367-2630. DOI: 10.1088/1367-2630/11/7/075001.

[16] SASAKI, M., M. FUJIWARA, H. ISHIZUKA, W. KLAUS, K. WAKUI, M. TAKEOKA, S. MIKI, T. YAMASHITA, Z. WANG, A. TANAKA,

K. YOSHINO, Y. NAMBU, S. TAKAHASHI, A. TAJIMA, A. TOMITA, T. DOMEKI, T. HASEGAWA, Y. SAKAI, H. KOBAYASHI, T. ASAI, K. SHIMIZU, T. TOKURA, T. TSURUMARU, M. MATSUI, T. HONJO, K. TAMAKI, H. TAKESUE, Y. TOKURA, J. F. DYNES, A. R. DIXON, A. W. SHARPE, Z. L. YUAN, A. J. SHIELDS, S. UCHIKOGA, M. LEGRE, S. ROBYR, P. TRINKLER, L. MONAT, J.-B. PAGE, G. RIBORDY, A. POPPE, A. ALLACHER, O. MAURHART, T. LAENGER, M. PEEV and A. ZEILINGER. Field test of quantum key distribution in the Tokyo QKD Network. *Optics Express*. 2011, vol. 19, iss. 11, pp. 10387–10409. ISSN 1094-4087. DOI: 10.1364/OE.19.010387.

[17] DIXON, A. R., Z. L. YUAN, J. F. DYNES, A. W. SHARPE and A. J. SHIELDS. Continuous operation of high bit rate quantum key distribution. *Applied Physics Letters*. 2010, vol. 96, iss. 16, pp. 102–110. ISSN 0003-6951. DOI: 10.1063/1.3385293.

[18] KORZH, B., C. C. WEN LIM, R. HOULMANN, N. GISIN, M. J. LI, D. NOLAN, B. SANGUINETTI, R. THEW and H. ZBINDEN. Provably secure and practical quantum key distribution over 307 km of optical fibre. *Nature Photonics*. 2015, vol. 9, iss. 3, pp. 163–168. ISSN 1749-4885. DOI: 10.1038/nphoton.2014.327.

[19] WANG, S., W. CHEN, J.-F. GUO, Z.-Q. YIN, H.-W. LI, Z. ZHOU, G.-C. GUO and Z.-F. HAN. 2 GHz clock quantum key distribution over 260 km of standard telecom fiber. *Optics Letters*. 2012, vol. 37, iss. 6, pp. 1008–1010. ISSN 1539-4794. DOI: 10.1364/OL.37.001008.

[20] DIANATI, M., R. ALLEAUME, M. GAGNAIRE and X. SHEN. Architecture and Protocols of the Future European Quantum Key Distribution Network. *Security and Communication Networks*. 2008, vol. 1, iss. 1, pp. 57–74. ISSN 1939-0114. DOI: 10.1002/sec.13.

[21] MEHIC, M., M. NIEMIEC and M. VOZNAK. Calculation of the Key Length for Quantum Key Distribution. *Elektronika ir Elektrotechnika*. 2015, vol. 21, iss. 6, pp. 81–85. ISSN 2029-5731. DOI: 10.5755/j01.eie.21.6.13768.

[22] ELLIOTT, C. Building the Quantum Network. *New Journal of Physics*. 2002, vol. 4, iss. 1, pp. 1–12. ISSN 1367-2630. DOI: 10.1088/1367-2630/4/1/346.

[23] HAO, W., H. ZHENG-FU, G. GUANG-CAN and H. PEI-LIN. The Queueing Model for Quantum Key Distribution Network. *Chinese Physics B*. 2009, vol. 18, no. 1, pp. 45–50. ISSN 1674-1056. DOI: 10.1088/1674-1056/18/1/008.

[24] KOENIG, S. and S. RASS. On the Transmission Capacity of Quantum Networks. *International Journal of Advanced Computer Science and Applications (IJACSA)*. 2011, vol. 2, iss. 11, pp. 9–16. ISSN 2158-107X. DOI: 10.14569/IJACSA.2011.021102.

[25] RASS, S. and S. KOENIG. Turning Quantum Cryptography against itself: How to avoid indirect eavesdropping in quantum networks by passive and active adversaries. *International Journal on Advances in Systems and Measurements*. 2012, vol. 5, iss. 1, pp. 22–33. ISSN 1942-261x.

[26] COLLINS, D., N. GISIN and H. DE RIEDMATTEN. Quantum Relays for Long-distance Quantum Cryptography. *Journal of Modern Optics*. 2005, vol. 52, iss. 5, pp. 735–753. ISSN 0950-0340. DOI: 10.1080/09500340412331283633.

[27] DUER, W. and H.-J. BRIEGEL. Quantum Repeaters Based on Entanglement Purification. *Physical Review A*. 1999, vol. 59, iss. 1, pp. 169–181. ISSN 1050-2947. DOI: 10.1103/PhysRevA.59.169.

[28] YUAN, Z.-S., Y.-A. CHEN, B. ZHAO, S. CHEN, J. SCHMIEDMAYER and J.-W. PAN. Experimental demonstration of a BDCZ quantum repeater node. *Nature*. 2008, vol. 454, iss. 7208, pp. 1098–1101. ISSN 0028-0836. DOI: 10.1038/nature07241.

[29] ALLEAUME, R., C. BRANCIARD, J. BOUDA, T. DEBUISSCHERT, M. DIANATI, N. GISIN, M. GODFREY, P. GRANGIER, T. LAENGER, N. LUETKENHAUS, C. MONYK, P. PAINCHAULT, M. PEEV, A. POPPE, T. PORNIN, J. RARITY, R. RENNER, G. RIBORDY, M. RIGUIDEL, L. SALVAIL, A. SHIELDS, H. WEINFURTER and A. ZEILINGER. Using Quantum Key Distribution for Cryptographic Purposes: A Survey. *Theoretical Computer Science*. 2014, vol. 560, iss. P1, pp. 62–81. ISSN 0304-3975. DOI: dx.doi.org/10.1016/j.tcs.2014.09.018.

[30] POPPE, A., M. PEEV and O. MAURHART. Outline of the SECOQC Quantum-Key- Distribution Network in Vienna. *International Journal of Quantum Information*. 2008, vol. 6, iss. 209, pp. 1–10. ISSN 0219-7499. DOI: 10.1142/S0219749908003529.

[31] SERGIENKO, A. V. *Quantum communications and cryptography*. Boca Raton, FL: Taylor&Francis, 2006. ISBN 978-0849336843.

[32] MARHOEFER, M., I. WIMBERGER and A. POPPE. Applicability of quantum cryptography for securing mobile communication networks. In: *Long-Term and Dynamical Aspects of Information Security: Emerging Trends in Information and Communication Security*. Freiburg: Nova Science Publishers, 2007, pp. 97–111. ISBN 978-3-540-34640-1.

[33] HAYASHI, M., K. IWAMA, H. NISHIMURA, R. RAYMOND and S. YAMASHITA. Quantum Network Coding. In: *Lecture Notes in Computer Science*. Berlin: Springer, 2007, pp. 610–621. ISBN 978-3-540-70917-6. DOI: 10.1007/978-3-540-70918-3.

[34] RILEY, G. F. and T. R. HENDERSON. The ns-3 Network Simulator. In: *Modeling and Tools for Network Simulation*. Berlin: Springer, 2010, pp. 15–34. ISBN 978-3642123306. DOI: 10.1007/978-3-642-12331-3_2.

[35] MEHIC, M., P. FAZIO, M. VOZNAK, P. PARTILA, D. KOMOSNY, J. TOVAREK and Z. CHMELIKOVA. On using Multiple Routing Metrics with Destination Sequenced Distance Vector Protocol for MultiHop Wireless Ad Hoc Networks. In: *Proceedings of SPIE 9848: Modeling and Simulation for Defense Systems and Applications XI*. Bellingham: SPIE, 2016, pp. 1–6. ISBN 978-151060089-8. DOI: 10.1117/12.2223671.

[36] ELLIOTT, C., A. COLVIN, D. PEARSON, O. PIKALO, J. SCHLAFER and H. YEH. Current status of the DARPA Quantum Network. In: *Proceedings of SPIE 5815: Quantum Information and Computation III*. Bellingham: SPIE, 2005, pp. 138–149. ISBN 0-8194-5800-7. DOI: 10.1117/12.606489.

[37] SUN, Y., X. CHENG and Y. JI. Quality of service realization method applied to quantum key distribution network. *Technology X* [online]. 2012. Available at: `http://www.technology-x.net/H04L/201110360703.html`.

About Authors

Miralem MEHIC is a Ph.D. student at the VSB–Technical University of Ostrava. His research is focused on quantum cryptography networks, network performances and security. He is co-author of fourteen scientific papers indexed in citation database SCOPUS and listed as the main author in four of them. He has extensive programming experience in C/C++, PHP and Java. In September 2015, he received the praise from the Dean of Faculty of Electrical Engineering and Computer Science for the results he achieved during his Ph.D. study.

Peppino FAZIO is an assistant professor at DIMES Department of University of Calabria and since 2011 he is an external collaborator of VSB–Technical University of Ostrava, regarding telecommunications issues. In particular he is an expert in routing issues of mobile/vehicular ad-hoc networks, and his research interests include mobile communication networks, QoS architectures, mobility modeling for WLAN environments, mobility analysis for prediction purposes, vehicular issues in ad-hoc networking, mobile ad-hoc networking and wireless channel modeling. He is peer reviewer and TPC member of different international IEEE conferences, as well as for many IEEE, SPRINGER and ELSEVIER international journals. He published more than 75 papers among International Journals, Conferences and Book Chapters.

Miroslav VOZNAK is an associate professor with Department of Telecommunications, the department chair in Faculty of Electrical Engineering and Computer Science, VSB–Technical University of Ostrava, Czech Republic. He received his Ph.D. degree in telecommunications in 2002 and topics of his research include next generation networks, IP telephony, speech quality and network security. He is a senior member of IEEE Communications Society and many boards of conferences supported by IEEE such as TSP, INBIS or CN.

Erik CHROMY was born in Velky Krtis, Slovakia, in 1981. He received the Master degree in telecommunications in 2005 from Faculty of Electrical Engineering and Information Technology of Slovak University of Technology Bratislava. In 2007 he submitted Ph.D. work. Nowadays he works as assistant professor at the Institute of Telecommunications of Faculty of Electrical Engineering and Information Technology of Slovak University of Technology in Bratislava.