Securing the control channel of a moving robot with quantum key distribution

N.Yu. Dema[1], K. Artemov[1], A.B. Vasiliev[2], V.V. Chistiakov[2], A.V. Gleim[2], S.A. Kolyubin[1], V.I. Egorov[2,*]

[1]*ITMO University, Faculty of Control Systems and Robotics, 197101 Kronverksky pr. 49, Saint Petersburg, Russia*
[2]*ITMO University, Faculty of Photonics and Optical Information, 199034 Kadetskaya line 3b, Saint Petersburg, Russia*
**viegorov@corp.ifmo.ru*

Transition to «Internet of Things» has become a mayor trend in network development during the last decade. It implies emergence of a new type of network nodes: cyber-physical systems (CPS) such as drones and unmanned vehicles communicating with human operators and unmanned devices. From security point of view managing CPS networks leads to a new type of threat: unlike enterprise networks where eavesdropping generally results in financial loss, hacking into CPS communication channels may lead to disruption of large-scale infrastructural objects and man-made disasters. A possible answer to these challenges is using quantum key distribution (QKD) technology for securing CPS control plane. At the same time, CPS may act as mobile trusted QKD nodes and solve the “last mile” problem.

Until recently little attention has been paid to studying possible applications of QKD technology in CPS systems, with a notable exception of [1]. In this work, we report for the first time an experimental demonstration of securing control and data planes of a moving robot with quantum keys.

Experimental scheme is shown in Fig. 1. Alice and Bob modules of an operating subcarrier wave (SCW) QKD system [2] were supplying quantum keys to workstations PC2 and PC1, respectively. Typical secure key rates in a 1 dB loss channel were 100 kbit/s; the SCW protocol description can be found in [3]. PC1 acted as a base station with a USB-controller (gamepad). At the other side of the channel, a pair of virtual machines at PC2 were modelling two separate entities: a stationary key storage that periodically supplies keys to CPS entering its secure perimeter and a CPS inner processing unit which decrypts the commands received from P1. For the sake of laboratory demonstration, PC2 uploaded the decrypted commands to the robot through a USB interface. A commercial CPS platform Robotino (Festo Didactic) carrying a web-camera was the final component of the setup.

All experiments were performed in real-time environment. The operator was using the gamepad for issuing control commands (two-coordinate movement, rotation angle and velocity) which were encrypted by quantum keys at PC1 and send to Robotino through PC2 via a Wi-Fi connection. As a result, the robot was moving in response to the decrypted commands. Simultaneously, data stream from the web camera was encrypted at PC2 and send through Wi-Fi to PC1, where the operator was monitoring the video. The SCW QKD modules used a separate optical fiber channel for synchronization and the Ethernet connection for open channel data exchange.

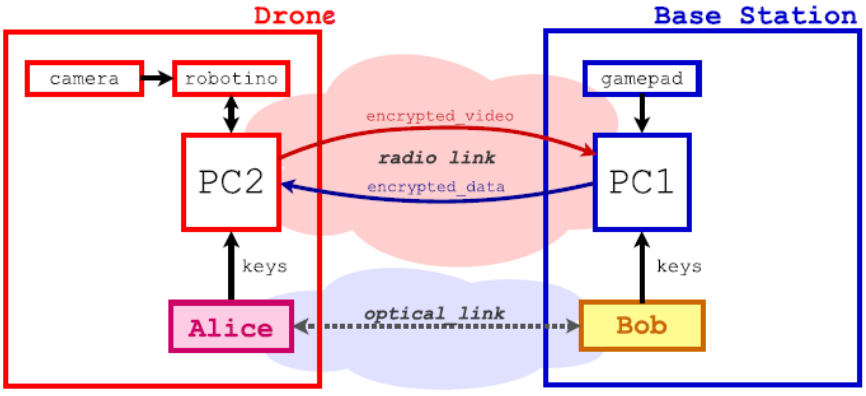

Figure 1. Principal scheme of the experiment.

This setup modelled two ways of using quantum keys. On the control plane, robot movement commands required relatively small amounts of transmitted data (typically 14 bytes each) and were therefore directly encrypted with quantum keys using XOR function. On the data plane, for larger amounts of data, such as the video signal streamed by the robot camera, the quantum bit strings were reduced to 256 bits and used as keys in AES encryption algorithm, which were periodically updated. Related key management was performed at PC1 and PC2 under Linux. ROS (Robot Operation System) framework was handling network data exchange. Photographs of the described setup are shown in Fig. 2.

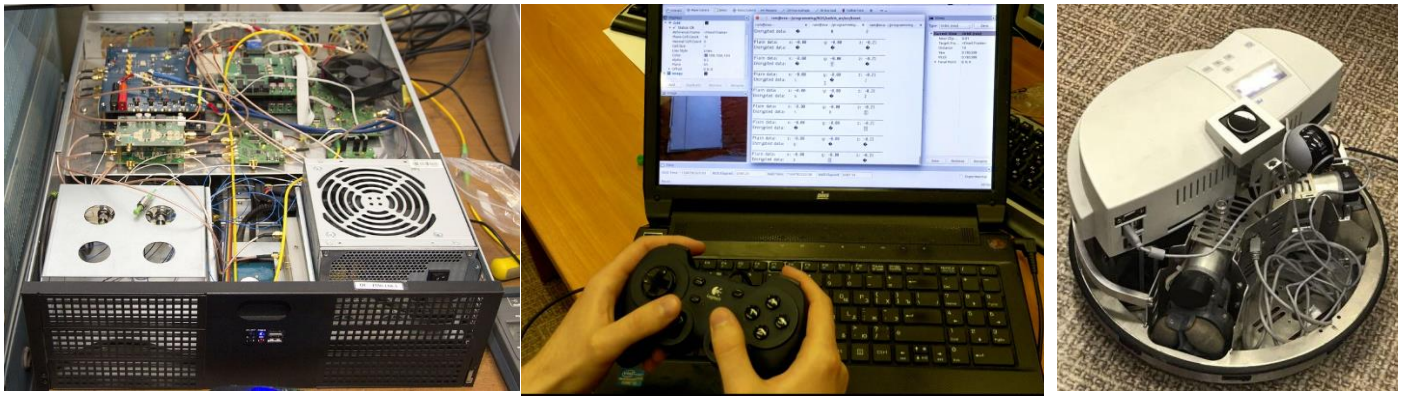

Figure 2. Photos of the implementation: SCW QKD system module, the gamepad issuing movement commands, the mobile robot with a camera operating through a QKD-protected channel.

The next stage of development (currently in progress) is to implement an alternative architecture where PC2 and a compact free-space Alice module are integrated to the robot. Notably, this will require no change in QKD architecture, since SCW systems with phase encoding have been shown to operate reliably in the air [4].

Acknowledgements

This work was financially supported by the Government of the Russian Federation (Grant 08-08).

References

1. A.D. Hill, J. Chapman, K. Herndon, C. Chopp, D.J. Gauthier, P. Kwiat Drone-based Quantum Key Distribution // Paper Tu22, Qcrypt 2017
2. A. V. Gleim, V. I. Egorov, Yu. V. Nazarov, S. V. Smirnov, V. V. Chistyakov, O. I. Bannik, A. A. Anisimov, S. M. Kynev, A. E. Ivanova, R. J. Collins, S. A. Kozlov, and G. S. Buller. "Secure polarization-independent subcarrier quantum key distribution in optical fiber channel using BB84 protocol with a strong reference". Opt. Express, Vol. 24, No. 3, p.2619-2633, (2016)
3. G. P. Miroshnichenko, A. V. Kozubov, A. A. Gaidash, A. V. Gleim, D. B. Horoshko Security of subcarrier wave quantum key distribution against the collective beam-splitting attack // Opt. Express, Vol. 26, No. 9 (2018)
4. Kynev S.M, Chistyakov V.V., Smirnov S.V., Volkova K.P., Egorov V.I., Gleim A.V. Free-space subcarrier wave quantum communication //Journal of Physics: Conference Series, IET – 2017.