IAF SPACE COMMUNICATIONS AND NAVIGATION SYMPOSIUM (B2)
Space-based Optical and Quantum Communications (4)

Author: Prof. Paolo Villoresi
Università degli Studi di Padova, Italy

TRANSFER OF PRECISE TIMING DATA SECURED USING QKD IN A SIMULATED SATELLITE LINK

Abstract

The crucial infrastructure for the navigation of positioning known as Global Navigation Satellite Systems (GNSS) are controlled by Precise Timing Facilities (PTFs). These facilities periodically measure the offset with respect to local atomic clocks, and when these data are compared with that of different PTF, a control signal is extracted. This process is of crucial importance for the correct operation of the network. This aspect has been addressed with a demonstration in which the offsets collected in two PTFs, the Matera Laser Ranging Observatory (MLRO) of the Italian Space Agency in Matera, Italy – MA - and the German Aerospace Center (Deutsches Zentrum für Luft- und Raumfahrt, DLR) in Oberpfaffenhofen, Germany – OP - were protected in their transfer using QKD. The reason was to contrast an attacker who can manipulate or even forge the synchronization data with the possibility to introduce small temporal shifts in the clocks. These variations may result in a slow drift of the global system time, eventually resulting in a disruption of the GNSS service. In particular, in the demonstration realized the simultaneous operation of three experimental parts: (i) a time offset measurement between the PTF clocks in OP and in MA, made possible by all-in-view detection of GNSS signals from the Galileo constellation; (ii) a fiber-based QKD link in MA and a second QKD link in OP; (iii) the real-time, encrypted, and authenticated transmission of time difference data from MA to OP. Two different QKD complete systems, from University of Padua and from company ThinkQuantum srl (Italy) were used for the encryption. While QKD link in space was not available, as no European systems are presently available, and was simulated, the other subsystems were all made functioning in parallel during the experiments, successfully demonstrating the securing of the critical data. This works paves the way to security in the quantum era for critical infrastructures at the continental scale. 1. Agnesi, C. et al. Simple quantum key distribution with qubit-based synchronization and a self-compensating polarization encoder. Optica 7, 284 (2020). 2. Avesani, M. et al. Deployment-Ready Quantum Key Distribution Over a Classical Network Infrastructure in Padua. J. Light. Technol. 40, 1658–1663 (2022). 3. Picciariello, F. et al. Quantum-secured time transfer between precise timing facilities: a field trial with simulated satellite links. GPS Solut. 28, 48 (2024). We acknowledge the partial support by EU Quantum Secure Networks Partnership (QSNP) No 101114043.