SPACE COMMUNICATIONS AND NAVIGATION SYMPOSIUM (B2)
Advanced Technologies for Space Communications and Navigation (7)

Author: Dr. Sarah Wittig
ESA, The Netherlands

CONCEPT FOR SINGLE-SATELLITE GLOBAL QUANTUM KEY DISTRIBUTION USING A SOLID STATE QUANTUM MEMORY

Abstract

By exploiting fundamental aspects of quantum physics, it is possible to generate keys for cryptography in such a way that eavesdropping can be detected, and therefore secrecy is guaranteed. This ‘quantum key distribution’ (QKD) is one solution to the threat posed to current cryptography methods by development of the quantum computer. QKD is a very active field of research and also has been commercially exploited, however the range of terrestrial systems are limited due to exponential loss of coherence. There are many proposals, and recently also an in-orbit demonstration, using satellites as a part of the link in order to extend the range of QKD.

Existing concepts for global coverage are based on trusted nodes within the channel as End-to-End (E2E) constellations are technically challenging and financially not viable. On the other hand proposals for E2E encryption using a single satellite do not provide global coverage.

In our opinion it is imperative that the encryption is E2E and does not rely on trusted nodes, as this leaves the system vulnerable and defeats the purpose of QKD. In this paper, we propose an E2E concept for global QKD, based on a single satellite enabled by an on-board quantum memory. The memory stores a quantum state of light which was obtained from a ground station, proceeds for some time along its orbit, then releases and transmits the stored state to a second ground station. With a multimode memory, a sufficiently long key can be established within a single pass over each ground station, thus achieving global coverage albeit with a time delay.

The concept has only recently emerged as feasible due to the development of efficient solid state quantum memories with storage times on the order of hours based on rare-earth ion-doped crystals (REIC). In addition to the long storage times, the engineering challenge of building a ruggedized quantum memory unit is somewhat easier for a solid-state based system, as compared to alternative quantum memories based on cold atom clouds or trapped ions. However, there have been no developments to date to advance the TRL of REIC quantum memories beyond laboratory demonstrations. Here we propose a system architecture and mission concept for a satellite containing a REIC quantum memory, and present a roadmap for required technology developments that would enable such a mission.