IAF SPACE COMMUNICATIONS AND NAVIGATION SYMPOSIUM (B2)
Interactive Presentations - IAF SPACE COMMUNICATIONS AND NAVIGATION SYMPOSIUM (IP)

Author: Mr. Javier Jordán-Parra
i2CAT, Spain, xavier.jordan@i2cat.net

Ms. Marina Garcia-Romero
i2CAT, Spain, marina.garcia@i2cat.net
Dr. Sergi Figuerola
i2CAT, Spain, sergi.figuerola@i2cat.net
Dr. Joan Adrià Ruiz de Azúa Ortega
i2CAT, Spain, joan.ruizdeazua@i2cat.net
Prof. Josep Paradells
UPC - Politechnical University of Catalonia, Spain, josep.paradells@entel.upc.edu

PERFORMANCE EVALUATION OF LONG-RANGE QUANTUM KEY DISTRIBUTION NETWORKS WITH SATELLITE TRUSTED NODES

Abstract

Security is a major concern of digital society, and quantum key distribution (QKD) can contribute with an unconditional secure mechanism for symmetric key distribution. Satellites can overcome the range limit of quantum communications based on fiber networks. This paper presents a method for performance evaluation of QKD based on satellites, exemplified with a case study that considers small satellites (CubeSats) in low Earth orbits (LEO), to illustrate a flexible configuration of the quantum range extender use case.

Performance evaluation will be conducted at two but complementary levels: first the evaluation of the key generation capacity at a link level (satellite to ground QKD node), with calculation of secret key length per pass. The system evaluation is derived from orbital propagation data and calculus of QKD performance is done considering finite key statistics approach. This evaluation aims to match with the shortness and variability of visibility intervals typical of LEO orbits.

The second evaluation level is the performance of key-relay capacity per pair of distant ground nodes willing to connect securely. Here the satellite acts as a flying trusted node, performing a public-XOR-scheme: the composition of xored key material is produced on the satellite and published to the remote pair of ground QKD nodes to obtain the other side QKD key. Key-relay capacity is tight to the rate generation at link level, but also depends on other parameters, such as differences in key rate generation per QKD segment, the satellite and terrestrial network topology (e.g. number and localization of nodes) or satellite orbital parameters such as inclination. Those different aspects condition and may lower the effective secret key length below initially estimated, and affects the portion that can be finally xored and distributed.

The results support the feasibility of the proposed case study and show the impact of relevant systems and orbital parameters in the key generation performance at link and key-relay level, such as system characteristics, uplink or downlink configuration, satellite altitude and orbital inclination. The estimated performance per different passes is then scaled to a year along with some sensitivity scenarios, to better illustrate the overall system performance and its dependence on certain system characteristics. The presented results may guide the design of future QKD satellite mission proposals and foster the deployment of global QKD networks thanks to satellite based QKD acting as quantum range extenders.