IAF SPACE COMMUNICATIONS AND NAVIGATION SYMPOSIUM (B2)
Advances in Space-based Communication Technologies, Part 2 (5)

Author: Mr. Adarsh Jain
Space Applications Centre (ISRO), India, adarshjain@sac.isro.gov.in

Mr. Nilesh M Desai
Space Applications Centre (ISRO), India, nmdesai@sac.isro.gov.in
Dr. Tirtha Pratim Das
Indian Space Research Organization (ISRO), India, tp_das@isro.gov.in
Mr. N Raghu Meetei
Indian Space Research Organization (ISRO), India, nraghu@isro.gov.in
Mr. R Umamaheswaran
Indian Space Research Organization (ISRO), India, r_umamaheswaran@isro.gov.in

DEVELOPMENTS OF KEY TECHNOLOGIES FOR ISRO'S SATELLITE BASED QUANTUM COMMUNICATION PROGRAM

Abstract

Quantum Key Distribution (QKD), as a disruptive technology, enables distribution of future-proof cryptographic keys between the communicating parties with unconditional data security. The conventional cryptosystems rely on mathematical complexities of certain algorithms and they are under threat with the advent of quantum computers with enormous computing capabilities. Unlike the classical cryptosystems, QKD relies on either or both of the two quantum phenomena, viz. Quantum Uncertainty and Quantum Non-locality. The practical implementation of ground based QKD system using the quantum state(s) of photons is limited to shorter distances due to inherent channel loss in free space or fibre, which leads to reduced key generation rate. This limitation can be overcome with Satellite Based Quantum Communication (SBQC) which provides the solution to establish a long-distance (over few thousands of kilometres) communication using satellites in orbit from LEO/MEO/GEO orbits to optical ground stations located at different places on Earth, and the same can be extended to build a global network using satellite constellations. A full-fledged demonstration of satellite based QKD calls for development of various subsystems at space segment onboard satellite and ground station segments.

In this paper, the authors present the design and development details of various subsystems and technologies viz weak coherent pulse source based QKD transmitter, QKD receiver, timing synchronization and polarization compensation techniques etc., which are required for the development of a satellite based QKD system and associated ground stations. The QKD transmitter based on weak coherent pulses is designed and developed with single photon generation rate of up to 10^7 counts/sec for a mean photon no. of ~ 0.1. A fully automated QKD test set-up, based on the BB84 protocol, has been developed to generate and distribute the polarization-encoded encryption keys seamlessly with secure key generation rate of $\sim 375 Kbps$ after performing post processing steps of error correction and privacy amplification. These keys have been used for demonstration of quantum encrypted live video conferencing, over an Ethernet LAN based public channel. The inter-building free space QKD experiments over a distance of $\sim 300m$ with Alice and Bob systems, are being carried out and key rates of $\sim 250 Kbps$ and QBER of < 5 % is estimated for $\sim 30\%$ transmission efficiency. The synchronization between Alice and Bob is achieved using the timing information derived from the Navigation with Indian Constellation (NavIC/IRNSS). The quantum atmospheric channel modelling is carried out to analyse the communication link performance in terms of link-budget analysis between a LEO satellite and a ground station. The outcomes of these

activities will culminate into the realization of the upcoming satellite based quantum communication between an Indian LEO satellite and Indian ground stations.