Paper ID: 33546
student

SPACE COMMUNICATIONS AND NAVIGATION SYMPOSIUM (B2)
Space Communications and Navigation Global Technical Session (8-GTS.3)

Author: Mr. István Vercseg
University of West Hungary, Hungary, itsikemn@gmail.com

Dr. Laszlo Bacsardi
Budapest University of Technology and Economics, Hungary, bacsardi@hit.bme.hu

SIMULATION OF INFORMATION TRANSFER ON QUANTUM-BASED SATELLITE NETWORK

Abstract

In our modern world, providing secure communications is harder and harder task, especially when the almost mystical quantum computer teasing us with its slowly approaching presence. While the universal quantum computer is far from completion, there are some working solutions using quantum mechanics. One of those technologies, the quantum-based key distribution (QKD) can protect our communications from any unauthorized third party. The QKD offers the possibility of a key exchange process which cannot be attacked or eavesdropped without the notification of the communication parties, since any attempt of eavesdropping the key will disturb the quantum states revealing the presence of an eavesdropper. The result of the exchange process is a classical string of bits, which can be further applied in nowadays used symmetrical coding protocols. The QKD became a state-of-art technology of our communications world since not only research institutions provide the efficiency of this technology but different companies were established to sell QKD services to their customers. But the usage of fiber-based QKD is limited in wired networks due to the physical properties of the optical fiber. This is why our work is focusing on the analysis of QKD technology in free-space environment, especially via satellites. One of the most interesting question is the following: How efficient could be this technology and what are its bounds in a satellite-satellite network? QuantumSat, our developed simulation framework is capable for simulating secure information transfer via satellites. To ensure security, we applied symmetric cryptography protocols (AES/Rijndael block cipher) for which the symmetric keys were provided by quantum-based key distribution protocols (namely BB84, B92). To help the analyzing of quantum-based satellite network, QuantumSat has two modes. The first mode is simulating one-hop or multi-hop secure communication between satellites, and the second one is to simulate communication between ground stations using satellites. While the former mode distributes individual quantum keys between each satellite that takes part in the communication, the latter mode distributes one key between the ground stations, and only update it when necessary. The simulation is visualized by a scale model animated on Java3D. With this, the user can accurately track the movements of the satellites either on real time or accelerated speed up to 1000x. These functions are designed to get more data more easily, and to test long-term communications. Using our simulation framework, we analyzed the feasibility of such network on different orbits.