UNIVERSITY OF WATERLOO

TECHNOLOGY SUMMARY

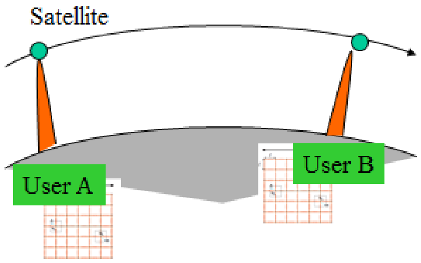

Fig.1 Repeater Network for QKD using satellites as trusted nodes

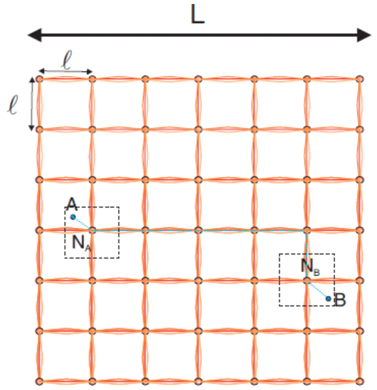

Fig.2 QKD Backbone Network

Reference

8810-7320

Patent status

US & Canada Patents issued

Stage of development

Proof of concept demonstrated

Contact

Scott Inwood
Director of Commercialization
Waterloo Commercialization Office
519-888-4567, ext. 33728
sinwood@uwaterloo.ca
uwaterloo.ca/research

Simplified Trusted Nodes for Quantum Key Distribution (QKD)

Background

Trusted Repeater Networks for QKD are a collection of trusted nodes that are linked up by point-to-point connections. These types of networks have been set up in several independent settings. They aim at providing secret key to distant users (A and B) that are linked each to a trusted node (N_A, N_B), which is connected via a further chain of intermediate trusted nodes (see figure 2). Each QKD link has to execute a full QKD protocol, which creates significant workload for trusted nodes in terms of not only the computational power that needs to be available there, but also in terms of the required high communication bandwidth between trusted nodes.

Description of the invention

The University of Waterloo has developed a QKD protocol for trusted repeater networks that dramatically reduces the required computational workload and high communication bandwidth needed at the intermediate node level. The new invented protocol utilizes the same trusted repeater network/hardware however, as it does not require full secret keys to be established by point-to-point devices, the required computational and communication resources can significantly be reduced. Only end users require the usual computational resources and communication bandwidth.

Advantages

The invention allows the reduction of computational power and communication bandwidth needed at intermediate trusted nodes, thus enabling less expensive trusted repeater QKD networks. For the same reason, it enables the use of satellites as trusted nodes in QKD networks which in turn enables QKD over long distances. The invention is independent of the underlying QKD technology deployed in existing QKD infrastructure which makes it very adoptable. The invention also provides more secure QKD over trusted repeater networks by eliminating the direct access of intermediate nodes to the final secret key shared by the end-users.

Potential applications

The invention has applications in QKD. It specifically enables long distance QKD as it significantly reduces the requirements of trusted nodes for QKD and thus enables satellites to be used as simplified trusted nodes in QKD networks.