Exchanging information securely using quantum communication in future fiber-optic networks

February 28 2019

Searching for better security during data transmission, governments and other organizations around the world have been investing in and developing technologies related to quantum communication and related encryption methods. Researchers are looking at how these new systems—which, in theory, would provide unhackable communication channels—can be integrated into existing and future fiber-optic networks.

Research at the National Institute of Information and Communications Technology in Japan, by a team that includes Senior Visiting Researcher Tobias A. Eriksson, holds promise for solving one of the key challenges for this application: how to achieve secure communication using continuously variable quantum key distribution. Often abbreviated as QKD, this method is the ongoing exchange of encryption keys, generated with quantum technology, for encrypting data being transferred between two or more parties.

In a paper to be presented at the OFC: The Optical Fiber Communications Conference and Exhibition being held 3-7 March in San Diego, Calif., Eriksson and his colleagues say the primary stumbling block for this application is noise generated by fiber amplifiers on current generation single-mode fiber systems. Their research involved exploring how to exploit multicore fiber-optic technology that is expected to be used in future transmission networks.

As the name suggests, multicore fiber-optic systems use multiple fiber cores in a single strand through which data can be transmitted. In today's fiber networks, each strand usually has only one core.

"Secure communication is one of the hardest challenges right now and many of the current encryption methods may someday easily be broken by algorithms designed for quantum computers," Eriksson says. "One reason we haven't seen commercial deployment of QKD is that the technology is not compatible with current network architecture."

As multicore fiber begins to be deployed in the future, Eriksson said, researchers are looking at how that technology could be harnessed to solve the encryption problem.

"The question we asked ourselves is whether the spatial dimensions of multicore fibers can be exploited for co-propagation of classical and quantum signals," Eriksson said. "What we found is that the classical channels can be transmitted completely oblivious of the quantum signals, which in single-mode fiber is not possible since the amplifier noise kills the quantum channels."

Eriksson's team measured the excess noise from crosstalk between the classical and the quantum channels, using 19-core fiber. They found that this approach has the potential to support 341 QKD channels, with 5 GHz spacing between wavelengths of 1537 nm and 1563 nm.

The team's technical results are outlined in a paper to be presented in San Diego at the OFC meeting. The group reported that when the quantum channels are using a dedicated core of a multicore fiber, network operators can avoid the noise generated by core-to-core crosstalk by making sure that the wavelengths of the quantum signals from QKD lie in the guard-band between the classical channels that carry data. This simple solution solves the problem of multiplexing of

quantum and classical channels and avoids introducing new components for the classical communication channels.

Provided by Optical Society of America