Our quantum internet breakthrough could make malicious hacking a thing of the past

September 3 2020, by Siddarth Koduru Joshi

Credit: AI-generated image (disclaimer)

The advent of mass working from home has made many people more aware of the security risks of sending sensitive information via the internet. The best we can do at the moment is make it difficult to intercept and hack your messages—but we can't make it impossible.

What we need is a new type of internet: the quantum internet. In this version of the global network, data is secure, connections are private and your worries about information being intercepted are a thing of the past.

My colleagues and I have just made a breakthrough, published in *Science Advances*, that will make such a quantum internet possible by scaling up the concepts behind it using existing telecommunications infrastructure.

Our current way of protecting online data is to encrypt it using mathematical problems that are easy to solve if you have a digital "key" to unlock the encryption but hard to solve without it. However, hard does not mean impossible and, with enough time and computer power, today's methods of encryption can be broken.

Quantum communication, on the other hand, creates keys using individual particles of light (photons) , which—according to the principles of quantum physics – are impossible to make an exact copy of. Any attempt to copy these keys will unavoidably cause errors that can be detected. This means a hacker, no matter how clever or powerful they are or what kind of supercomputer they possess, cannot replicate a quantum key or read the message it encrypts.

This concept has already been demonstrated in satellites and over fiber-optic cables, and used to send secure messages between different countries. So why are we not already using in everyday life? The problem is that it requires expensive, specialized technology that means it's not currently scalable.

Previous quantum communication techniques were like pairs of children's walkie talkies. You need one pair of handsets for every pair of users that want to securely communicate. So if three children want to talk to each other they will need three pairs of handsets (or six walkie talkies) and each child must have two of them. If eight children want to talk to each other they would need 56 walkie talkies.

Obviously it's not practical for someone to have a separate device for every person or website they want to communicate with over the internet. So we figured out a way to securely connect every user with just one device each, more similar to phones than walkie talkies.

Each walkie talkie handset acts as both a transmitter and a receiver in order to share the quantum keys that make communication secure. In our model, users only need a receiver because they get the photons to generate their keys from a central transmitter.

This is possible because of another principle of quantum physics called "entanglement." A photon can't be exactly copied but it can be entangled with another photon so that they both behave in the same way when measured, no matter how far apart they are—what Albert Einstein called "spooky action at a distance."

Full network

When two users want to communicate, our transmitter sends them an entangled pair of photons—one particle for each user. The users' devices then perform a series of measurements on these photons to create a shared secret quantum key. They can then encrypt their messages with this key and transfer them securely.

By using multiplexing, a common telecommunications technique of combining or splitting signals, we can effectively send these entangled photon pairs to multiple combinations of people at once.

We can also send many signals to each user in a way that they can all be simultaneously decoded. In this way we've effectively replaced pairs of walkie talkies with a system more similar to a video call with multiple participants, in which you can communicate with each user privately and independently as well as all at once.

We've so far tested this concept by connecting eight users across a single city. We are now working to improve the speed of our network and interconnect several such networks. Collaborators have already started using our quantum network as a test bed for several exciting applications beyond just quantum communication.

We also hope to develop even better quantum networks based on this technology with commercial partners in the next few years. With innovations like this, I hope to witness the beginning of the quantum internet in the next 10 years.

More information: Siddarth Koduru Joshi et al. A trusted node–free eight-user metropolitan quantum communication network, *Science Advances* (2020). DOI: 10.1126/sciadv.aba0959

This article is republished from The Conversation under a Creative Commons license. Read the original article.*This story is part of* Science X Dialog, *where researchers can report findings from their published research articles.* Visit this page *for information about ScienceX Dialog and how to participate.*

Provided by The Conversation

Citation: Our quantum internet breakthrough could make malicious hacking a thing of the past (2020, September 3) retrieved 23 April 2024 from https://sciencex.com/news/2020-09-quantum-internet-breakthrough-malicious-hacking.html