Quantum step forward in protecting communications from hackers

Posted on 20 June 2018

Researchers at the University of York have shown that a new quantum-based procedure for distributing secure information along communication lines could be successful in preventing serious security breaches.

A hacker can attack the electronic devices used for information transmission

Securing highly sensitive information, such as hospital records and bank details, is a major challenge faced by companies and organisation throughout the world.

Standard communication systems are vulnerable to hacks, where encrypted information can be intercepted and copied. It is currently possible for hackers to make a copy of transmitted information, but it would not be possible to read it without a method of breaking the encryption that protects it.

This means that information might be secure for a period of time, but there is no guarantee that it would be secure forever, as supercomputers in development could potentially decipher particular encryptions in the future.

Researchers at York investigated a prototype, based on the principles of quantum mechanics, that has the potential to side-step the vulnerabilities of current communications, but also allow information to be secure in the future.

Powerful attack

Dr Cosmo Lupo, from the University of York's Department of Computer Science, said: "Quantum mechanics has come a long way, but we are still faced with significant problems that have to be overcome with further experimentation.

“One such problem is that a hacker can attack the electronic devices used for information transmission by jamming the detectors that are used to collect and measure the photons that carries information.

“Such an attack is powerful because we assume that a given device works according to its technical specifications and will therefore perform its job. If a hacker is able to attack a detector and change the way it works, then the security is unavoidably compromised.”

“The principles of quantum mechanics, however, allows for communication security even without making assumptions on how the electronic devices will work. By removing these assumptions we pay the price of lowering the communication rate, but gain in improving the security standard.”

Two signals

Instead of relying on possibly compromised electronic components at the point at which information needs to be detected and read, the researchers found that if the untrusted detectors existed at a separate point in the communications – somewhere between the sender and receiver - the communication was far more secure.

The detector would receive a combination of two signals, one from the sender and one from the receiver. The detector would only be able to read the result of this combined signal, but not its component parts.

Dr Lupo said: “In our work, not only have we provided a first rigorous mathematical proof that this ‘detector- independent’ design works, but we have also considered a scheme that is compatible with existing optical fibre communication networks.

“In principle our proposal can allow for the exchange of unbreakable codes across the internet without major changes in the actual infrastructure.

“We are still at prototype stage, but by finding ways to reduce the cost of these systems, we are that much closer to making quantum communications a reality.”

The research is funded by the EPSRC Quantum Communications hub and by Quantum Innovation Center Qubiz, and published in the journal Physical Review Letters.