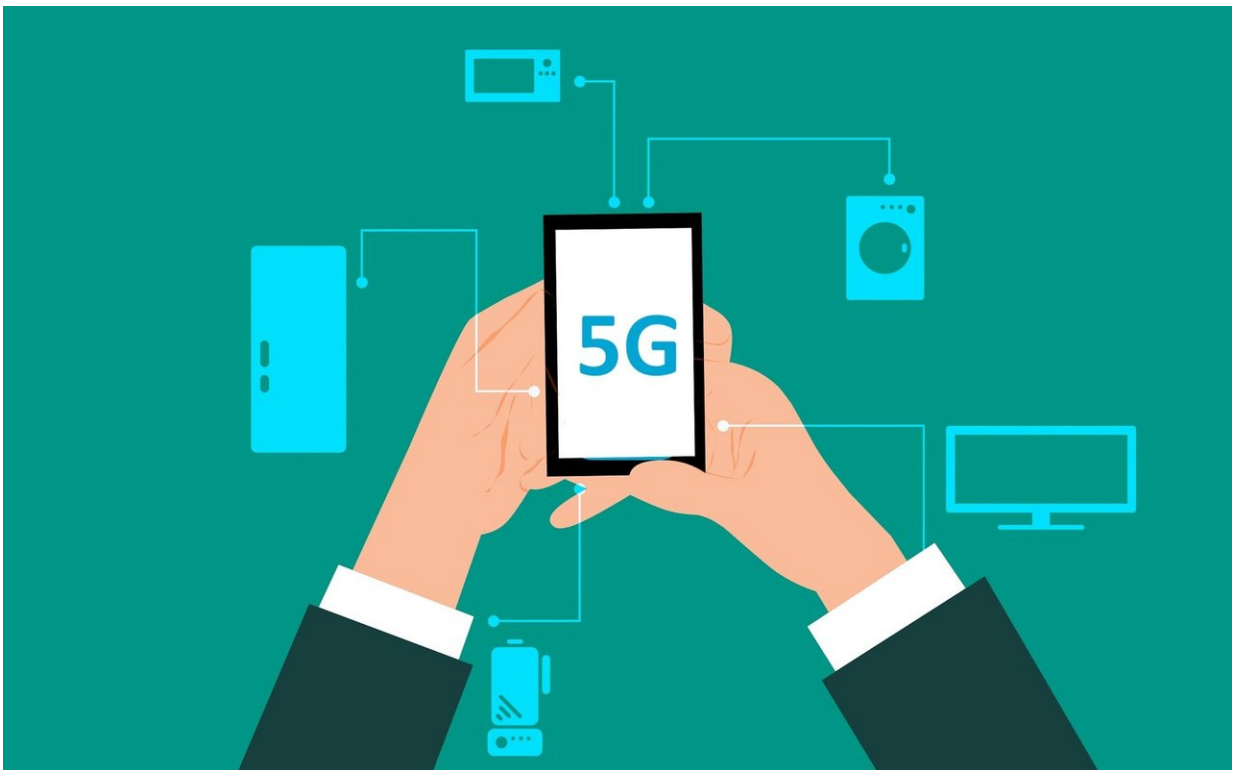


Breakthrough research using quantum cryptography addresses security in 5G networks

March 7 2019



Credit: CC0 Public Domain

New research has demonstrated a ground-breaking solution for securing future critical communications infrastructures, including emerging 5G networks.

The research addresses widely reported concerns on security vulnerability of 5G networks which are predicted to transform the telecommunications industry in the next ten years. The work was carried out by the High Performance Networks (HPN) Research Group at the University of Bristol's Smart Internet Lab and following a competitive peer review selection process.

The findings are presented today (7 March) at a highly prestigious post-deadline paper in the Optical Fibre Communication Conference (OFC), San Diego, USA.

The proposed solution will enable 5G network operators to offer ultimately secure 5G services while guaranteeing ultra-low-latency and high-bandwidth communications. This is due to the novel combination of quantum and infrastructure virtualization technologies.

Recent advances in [software engineering](#) and commodity computing technologies have revolutionised the telecommunications industry in the past ten years. Entire classes of network communication services that have traditionally been carried out by proprietary, dedicated hardware, are now virtualised and hosted in commodity computing servers. This is commonly referred to as "Network Softwareisation".

The move of critical network communication functions into software, distributed across the internet however, imposes significant security risk for telecommunications networks and specifically for 5G networks that rely entirely on such software architecture. Any malicious attempt to tamper with these virtualized network functions can potentially put the whole internet and its users at risk.

The new research addresses this problem with a new, fully programmable network virtualization platform leveraging on quantum technologies for securing function virtualisation and service

orchestration.

The proposed quantum secured 5G virtualization platform is capable of working across multiple 5G operators' networks (i.e. EE, O2, Vodafone etc.). It uses advanced and standard compliant virtualization technology for creating on-demand complex and collaborative 5G network services across operators' domains, while utilising quantum cryptography and optical interconnection infrastructure to secure services and guarantee 5G Key Performance Indicators (3GPP KPIs).

Professor Reza Nejabati, Head of the HPN Research Group, said: "Hardware and software technologies reported in this paper can potentially revolutionise 5G networks. They empower [network](#) operators to leverage the flexibility and programmability offered by virtualization technology in order to create new types of internet services while taking advantages of transmission at the speed of light and also securing the system using quantum technology".

Professor Dimitra Simeonidou, Director of the Smart Internet Lab, added: "5G networks will transform communications, industry and society in the next decade. However, security is a key concern for 5G deployment and is expressed widely in global media. The University of Bristol has pioneered research on 5G and quantum for a number of years and more recently led a number of landmark demonstrations of 5G benefits. With this new work, we bring together our research strengths to provide an ultimate security solution for 5G networks."

More information: First Demonstration of Quantum-Secured, Inter-Domain 5G Service Orchestration and On-Demand NFV Chaining over Flexi-WDM Optical Networks, Proc. OSA Optical Fibre Communication (OFC) Conference, PDP, San Diego, CA, USA, March 2019

Provided by University of Bristol

Citation: Breakthrough research using quantum cryptography addresses security in 5G networks (2019, March 7) retrieved 9 April 2024 from <https://techxplore.com/news/2019-03-breakthrough-quantum-cryptography-5g-networks.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.