Enabling Quantum-secure 5G enabled Mobile Edge Computing (MEC) for manufacturing

CHALLENGE

With maturity of 5G technology and its commercial availability, 5G is becoming the connectivity technology of choice in the autonomous and smart manufacturing industry.

5G offers on-demand, high-bandwidth with low latency (minimal delays on a network or internet connection) connectivity for all connected devices, sensors and robotic apparatus in a manufacturing eco-system. This enables the realisation of advanced, intelligent, autonomous and predictive manufacturing control processes and workflows that are more efficient.

RESULTS AND THE DIGITAL OPPORTUNITY

Another technology often associated with 5G is Mobile Edge Computing (MEC). MEC provides limited but powerful computing power at the edge of the network close to end user devices for low latency computing tasks. This is an important technology for smart manufacturing, especially for time critical manufacturing processes. These processes require low-latency computing on real-time data to proactively react to different situations along the manufacturing line.

Modern analytics algorithms and processes in smart manufacturing such as those used at the National Composite Centre (NCC) are often very complex and computationally demanding as well as requiring processing of large data sets in real time. These requirements cannot be met by the limited computation power of MEC and as such the process has to be divided between MEC and a remote data centre with time sensitive processes. An example is an AI (Artificial Intelligence) Deep Neural Network Model where a machine is being trained to undertake thermal image analysis of material. This computationally intensive training can be done in a remote data centre while the operation of the trained model can be hosted at the edge to operate at low latency.

The interaction between MEC and the remote data centre require an exchange of sensitive data and manufacturing models. This requires a high level of security, especially for highly sensitive manufacturing process data (from a national security or IP (Intellectual Property) perspective).

To address this problem, the Smart Internet Lab at the University of Bristol has created and successfully demonstrated a 5G MEC that supports quantum security for secure communication with a remote data centre. Quantum security utilising the no cloning principle of quantum physics provides an ultra-secure solution for an unbreakable network communication cryptography.

A MEC has been implemented and integrated with the 5G test bed at the University of Bristol and the NCC 5G network and test bed. It can host AI and processing algorithms for low latency control of manufacturing robots at the NCC. It also connects to the 5G network at the NCC to collect data from manufacturing lines, their sensors and robotic facilities. The MEC network also integrates with quantum cryptography interfaces and quantum transponders. This enables quantum secure connectivity between the NCC 5G network and a remote data centre. The MEC utilises advanced algorithms that also partitions data flows based on their security requirement. It is able to transmit data with high security requirements over an optical network from the NCC to a remote data centre (in this case the University of Bristol 5G test bed) utilising quantum cryptography.

Demonstrated for the first time, quantum secure MEC is able to aggregate traffic from a private 5G manufacturing network and transmit to a remote data centre utilising quantum security.

To access the range of DETI and Partner industrial test beds and discuss your requirements, email **deti@nccuk.com**

Partner

University of BRISTOL

NATIONAL COMPOSITES CENTRE