HASC
HUB IN ALL-SPECTRUM CONNECTIVITY

AI for Connectivity

INTELLIGENT FUTURE NETWORKS: HASC PROJECT SPOTLIGHT

PROJECT TITLE:

Securing Spectrum Connectivity: Over-the-Air Authentication Using Radio Frequency Fingerprinting

CORE CHALLENGE:

Security

CHALLENGE:

Today's networks trust devices based on passwords and software credentials that can be hacked or stolen.

In the future billions of IoT devices are likely to be used in sectors such as healthcare and in smart cities.

INNOVATION:

By reading a device's unique radio 'fingerprint' at the physical layer, we can verify its identity the moment we add additional security to networks.

This means, ML-enabled, PHY layer radio frequency fingerprint identification (RFFI) for authenticating wireless radio devices. Rather than authenticating users, this technology authenticates devices.

IMPACT:

As we connect more and more devices (including IoT, smartwatches and phones and smart home devices) we need new ways to protect networks from fake or malicious devices.

Traditional security methods (like passwords) can be hacked but using a device's own physical signal as its ID is much harder to fake. This development will help citizens remain secure.

HASC
HUB IN ALL-SPECTRUM CONNECTIVITY

AI for Connectivity

INTELLIGENT FUTURE NETWORKS: HASC PROJECT SPOTLIGHT

With thanks to...

LEAD UNIVERSITIES:

University of Liverpool, Queen's University Belfast, & Heriot-Watt University

PRINCIPAL INVESTIGATOR:

Junqing Zhang

UKRI Engineering and Physical Sciences Research Council

The Hub is supported by substantial investment from the Engineering and Physical Sciences Research Council (EPSRC), part of UK Research and Innovation, and the UK Department of Science, Innovation and Technology. Grant References: EP/Y037197/1/ EP/X040569/1

University of Liverpool · Queen's University Belfast · Heriot-Watt University