1. Cyber Intrusion Detection in IoT Sensor Networks through ML/DL/AI

By 2050, more than 60% of the world's population is expected to live in urban areas. Well-designed smart cities improve the lives of residents and visitors by making city systems more efficient, using new technologies as part of the Internet of Things (IoT) and big data to solve economic, social and environmental challenges. Examples of such IoT technology include Long Range Wide Area Network (LoRaWAN), which has been designed to wirelessly connect battery operated 'things' to the internet in regional, national or global networks, and targets key IoT requirements such as bi-directional communication, end-to-end security, mobility and localization services. Such systems are vulnerable to cyber attack through spoofing, flooding, eavesdropping, etc.

Here methods, such as machine learning (ML), deep learning (DL) as well as application of artificial intelligence (AI) will be evolved to efficiently detect cyber intrusion at the open radio frequency (RF) attack surface. This PhD will specifically address cyber attack at the RF Physical (PHY) / Medium Access Control (MAC) layer by examining the received waveforms and incoming data packets through ML/DL/AI to differentiate rogue devices, classify attacks and evolve mitigation strategies, through detailed considerable of the propagating channel, analogue transceiver characteristics as well as historical behaviour of a sensor, including spatial-temporal variations.

2. RF Fingerprinting for Cyber Intrusion Detection

Smart cities and associated network technology is giving rise to entirely new technology sectors that are expected to transform our lives in the future; these include fully autonomous vehicles, industrial internet, swarm robotics, smart grid, m-health and other forms of automation. Much of this transformation is predicated on large numbers of connected wireless sensors and communication nodes. The wireless infrastructure however could present a weakness and is potentially vulnerable to a number of attacks including hostile devices injecting data masquerading as it were from legitimate sensors, with the aim of destabilising the overall system.

This PhD project will develop methods for identifying devices in the network through various unique characteristics they exhibit – so called 'fingerprinting'. Characteristics used for fingerprinting devices may include such features as their RF hardware characteristics, their wireless channel response or their protocol behaviour. Once fingerprinted, devices may be subsequently classified as legitimate and trusted parts of the network or suspicious actors or known hostiles. Once devices are classified as trusted or otherwise, attacks may be mitigated. The field of Machine Learning may provide effective methods for fingerprinting and classification.
This project would suit a student with aptitude and interests in RF design, wireless propagation, wireless protocols and/or machine learning.

3. Exploiting the Composite Antenna Wireless Channel for Cyber Defence

With the antenna located at the at the front-end of the transceiver, it makes it an important line of defence of the receiver to jamming and spoofing, and the susceptibility of the transmitter to eavesdropping. Antenna element design, array design, operating bandwidth, signal polarisation and radiation pattern control all contribute. On top of this, there is the way the antenna interacts with the propagation environment from Line-of-Sight applications to Non-Line-of-Sight scenarios.

This work will combine antenna design with factors such as beamshaping and polarisation agility implemented with RF hardware and baseband signal processing to, say, control the antenna's beam direction away from eavesdroppers and jammers and towards the desired target. This will involve theoretic study; antenna design and propagation modelling; and eventually lead to practical (system-level) validation.

4. Secure PHY Layer Techniques for Wireless Connectivity

The inherent broadcast nature of wireless communications makes it vulnerable to eavesdropping. Security techniques in upper layers require high computational complexity and cause large overheads. Current wireless PHY-layer security has two main directions: (i) to generate, manage and distribute keys based on the spatio-temporal characteristics of the wireless channel, and, (ii) the secrecy capacity and wiretap channel model proposed by Wyner on basis of Shannon capacity. However, only a few of existing PHY-layer security schemes can be used in MIMO systems.

Index modulation (IM) has emerged as a key technique in 5G wireless networks because of its high spectral and energy efficiency. The two well-known applications of IM are (i) IM-OFDM, and, (ii) spatially modulated MIMO (SM-MIMO). IM waveforms enhance (i) PHY-layer security through securing the IM in IM-OFDM, and, (ii) PHY encryption through SM-MIMO. This PhD will further develop and assess the robustness of such techniques.