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 [1], [2] & [3].

[1] E. Aras, N. Small, G. S. Ramachandran, D. Stéphane, W. Joosen, D. Hughes, (2018), "Selective Jamming of LoRaWAN using Commodity Hardware," *MobiQuitous 2017*, Melbourne, VIC, Australia, November 7–10, 2017, pp. 363–372, https://doi.org/10.1145/3144457.3144478

[2] E. Aras, G. S. Ramachandran, P. Lawrence and D. Hughes, "Exploring the Security Vulnerabilities of LoRa," *2017 3rd IEEE International Conference on Cybernetics (CYBCONF)*, Exeter, UK, 2017, pp. 1-6, doi: 10.1109/CYBConf.2017.7985777.

[3] M. Ingham, J. Marchang, D. Bhowmik, (2020), "IoT Security Vulnerabilities and Predictive Signal Jamming Attack Analysis in LoRaWAN", *IET Information Security*, 14 (4), pp. 368-379, https://doi.org/10.1049/iet-ifs.2019.0447

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.

[1] S. U. Rehman, K. W. Sowerby, S. Alam and I. Ardekani, "Radio frequency fingerprinting and its challenges," 2014 IEEE Conference on Communications and Network Security, San Francisco, CA, USA, 2014, pp. 496-497, doi: 10.1109/CNS.2014.6997522.

[2] Shouyun Deng, Zhitao Huang, Xiang Wang, Guangquan Huang, "Radio Frequency Fingerprint Extraction Based on Multidimension Permutation Entropy", *International Journal of Antennas and Propagation*, vol. 2017, Article ID 1538728, 6 pages, 2017. https://doi.org/10.1155/2017/1538728

[3] T. Jian et al., "Deep Learning for RF Fingerprinting: A Massive Experimental Study," in IEEE Internet of Things Magazine, vol. 3, no. 1, pp. 50-57, March 2020, doi: 10.1109/IOTM.0001.1900065.

3. 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 [1]. 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 [2] & [3]. This PhD will further develop and assess the robustness of such techniques.

[1] Wyner, A.D., 1975. The Wire-Tap Channel. Bell system technical journal, 54(8), pp.1355-1387.

[2] Lee, Y., Jo, H., Ko, Y. and Choi, J., 2017. Secure index and data symbol modulation for OFDM-IM. IEEE Access, 5, pp.24959-24974.

[3] Liu, C., Yang, L.L. and Wang, W., 2017. Secure spatial modulation with a full-duplex receiver. IEEE Wireless Communications Letters, 6(6), pp.838-841.

4. Cascaded Neural Network Design for the Detection of RF Cyber Attacks

Most smart applications utilizing deep learning rely on classical neural network architectures that carry out training or process input data by a single phase. Different from these classical architectures, cascaded neural network architectures split the entire computing procedure into several stages, form a number of sub-networks, and cascade these sub-networks in certain ways. Cascaded neural network architectures have been proven to be more efficient than classical neural network architectures in some cases and, more importantly, can enhance the interpretability of neural computing. To date, wireless security has become a key problem for six-generation (6G) communication networks and the Internet of Things (IoT). Due to the advantages brought by

cascaded neural networks, this project aims to design proper cascaded neural networks to capture subtle indications of different kinds of radio-frequency (RF) cyber attacks and detect them with a high level of accuracy.

Skills:

1. Solid background in wireless communications, network security, or digital signal processing;
2. Good understanding of machine learning and neural computation;
3. Good programming skills and experience in MATLAB or Python programming;
4. Ability to think and work independently;
5. Good verbal and written communication skills.

[1] S. Dang, M. Wen, S. Mumtaz, J. Li and C. Li, "Enabling Multi-Carrier Relay Selection by Sensing Fusion and Cascaded ANN for Intelligent Vehicular Communications," in IEEE Sensors Journal, doi: 10.1109/JSEN.2020.2986322.

[2] J. Li, S. Dang, M. Wen, Z. Zhang and Q. Li, "Smart Detection Using the Cascaded Artificial Neural Network for OFDM with Subcarrier Number Modulation," in IEEE Wireless Communications Letters, doi: 10.1109/LWC.2021.3062686.

[3] V. Hoang and K. Jo, "3-D Human Pose Estimation Using Cascade of Multiple Neural Networks," in IEEE Transactions on Industrial Informatics, vol. 15, no. 4, pp. 2064-2072, April 2019, doi: 10.1109/TII.2018.2864824.

[4] D. Hunter, H. Yu, M. S. Pukish, III, J. Kolbusz and B. M. Wilamowski, "Selection of Proper Neural Network Sizes and Architectures—A Comparative Study," in IEEE Transactions on Industrial Informatics, vol. 8, no. 2, pp. 228-240, May 2012, doi: 10.1109/TII.2012.2187914.

5. Physical Layer Security Techniques for the Detection of RF Cyber Attacks

Description: Security measures in RF communications technologies are normally associated with passwords or other security tokens that operate at the media access control or application level. These help secure the higher layers of the OSI stack however the physical layer of most radio systems remains at risk to an attack even if this is simple jamming of the signal. Detection and mitigation measures remain an important research challenge.

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 malicious jamming and spoofing of wanted communications, and the susceptibility of the transmitter to eavesdropping by an adversary. Antenna element design, array design, operating bandwidth, signal polarisation and radiation pattern control all contribute to hardening of the receiver system to a malicious RF attack. In this study, the ability of the receiver to identify whether it is being spoofed via the signal characteristics received at the antenna is to be investigated. The expectation is that some identification of the position (maybe range or angle from the receiver) is possible so that devices can differentiate between valid sources and impostors, owing to the increased threats borne of inexpensive software defined radios (SDR's) this topic is of high interest and is the subject of ongoing research [1] [2]. Initial study would look at the feasibility using a complex antenna network, primarily as the benchmark on accuracy, and then apply a variety of techniques to far-less sophisticated platforms to identify the level of reduction in the ability to differentiate friend from foe. This will involve theoretic study; antenna design and signal modelling; and eventually lead to practical (system-level) validation.

Ideally, we would expect an applicant to have a background or knowledge of one or more of the following: radio propagation, signal processing, system design, mathematical.

[1] Multi-Antenna Scheme for Early Detection and Mitigation of Intermediate GNSS Spoofing. J.Magiera MDPI Sensors May 2019

[2] Autonomous Spoofing Detection and Mitigation with a Miniaturised Adaptive Antenna Array. A Konovaltsev 2014

6. A topic of the candidate's choice that aligns with the SWAN Research Challenges