Spatial Fingerprinting for Future Self Securing Networks

UK IC Postdoctoral Research Fellow
Timothy Pelham, PhD, MIET, MIEEE
Communications Systems & Networks Research Group.
Faculty of Engineering and Science, University of Bristol

LyceanEM

Overview

The electromagnetic environment represents a consistently open RF attack surface. Spatial fingerprinting is proposed as a fusion of spatial intelligence, onboard electromagnetic modelling and machine learning to allow nodes within a network to identify and localise transmitters in their locality. This capability forms the basis of reciprocal trust networks between nodes in a node work, enabling self-securing behaviour, and the identification and localisation of unauthorised transmitters attempting to penetrate the network. This process is demonstrated using modelled and measured data of LoRa network packets with an Anechoic Chamber, allowing for complete modelling of the scattering environment within the spatial intelligence node, and localisation of the transmitters.

Method

The Spatial Intelligence Node is populated by an Nvidia Orin AGX, providing 275 TOPS at 60W, 3 Oak-D W cameras, and 2 USRP B210 software defined radios, providing 4x4 MIMO. This allows for spatial mapping within the Anechoic Chamber based upon the radio emissions of the LoRa module (LoPy 4 module on a Pytrack 2.0 X carrier board) at 867MHz. Rotation of the LoRa antenna allows for spatial and RF fingerprinting of multiple LoRa modules, and combined characterization of the consistent scene within the anechoic chamber [1].

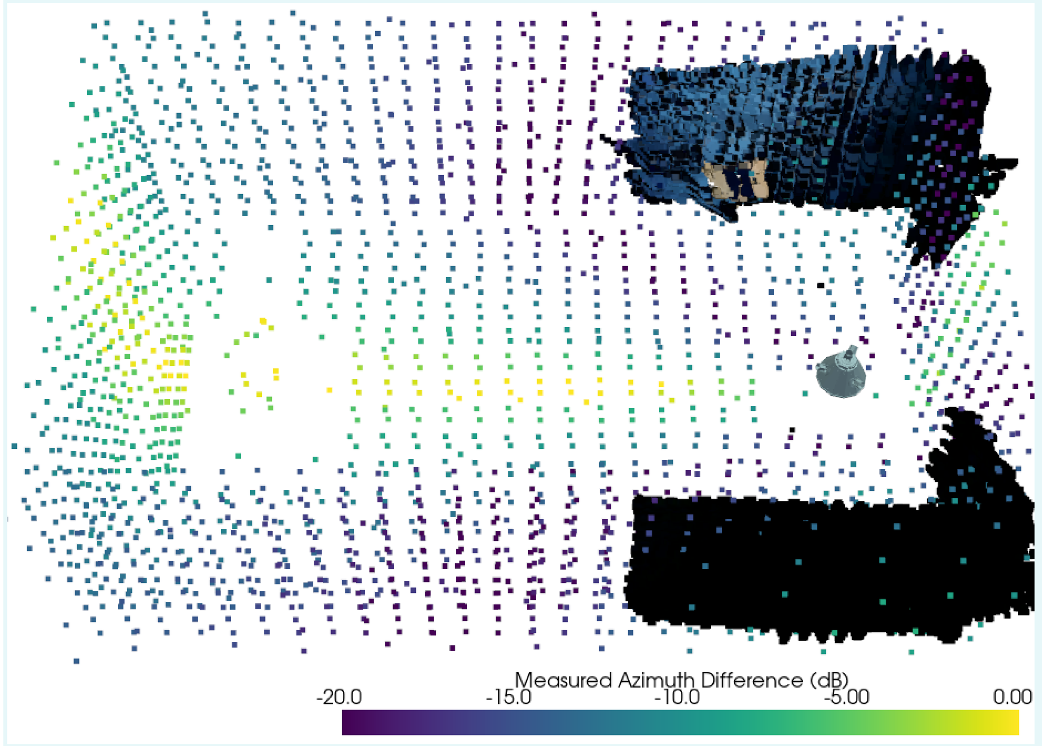


Figure 2 : Spatial Map with Localisation

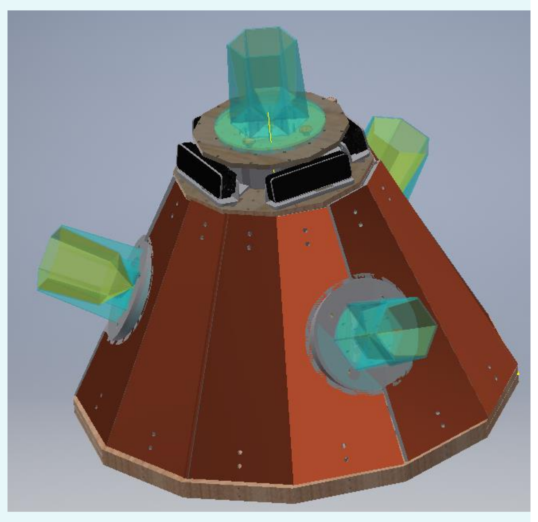


Figure 1 : Spatial Intelligence Node

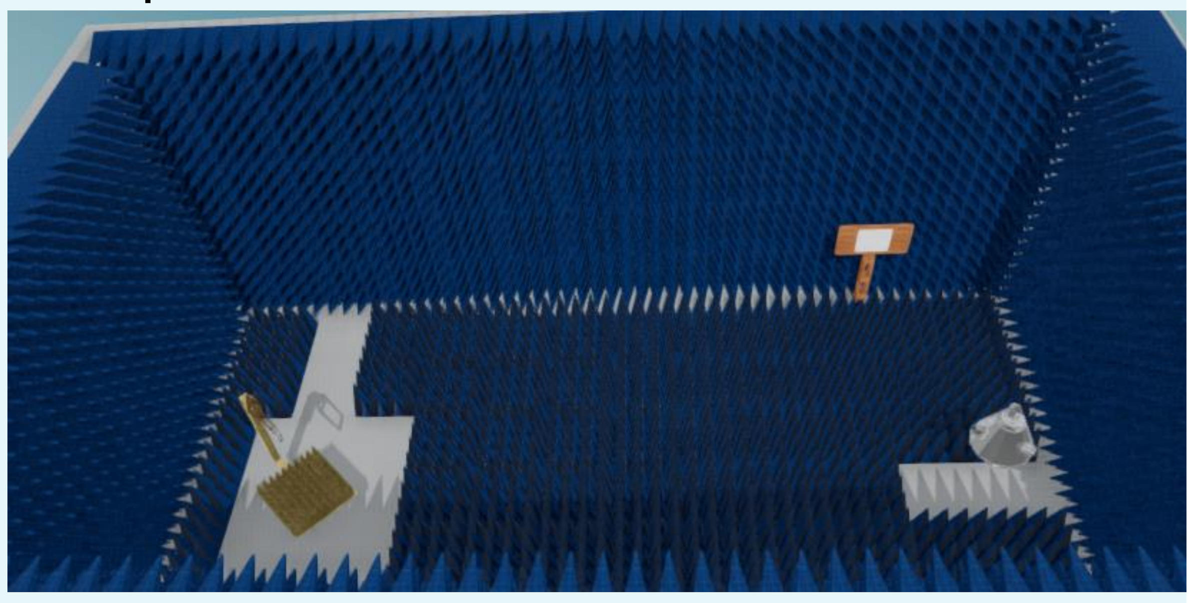


Figure 3 : Anechoic Chamber Digital Twin

Results

The combination of RF Fingerprinting using self organizing maps (SOM) has been demonstrated within SWAN to provide classification accuracy of >99% [2]. However the SOM and RF represent a composite of transmitter and channel, and in a dynamic environment, it is spatial awareness which is required to predict the channel in sufficient accuracy to remove the channel component from the fingerprint, providing reliable classification independent of location and channel fading.

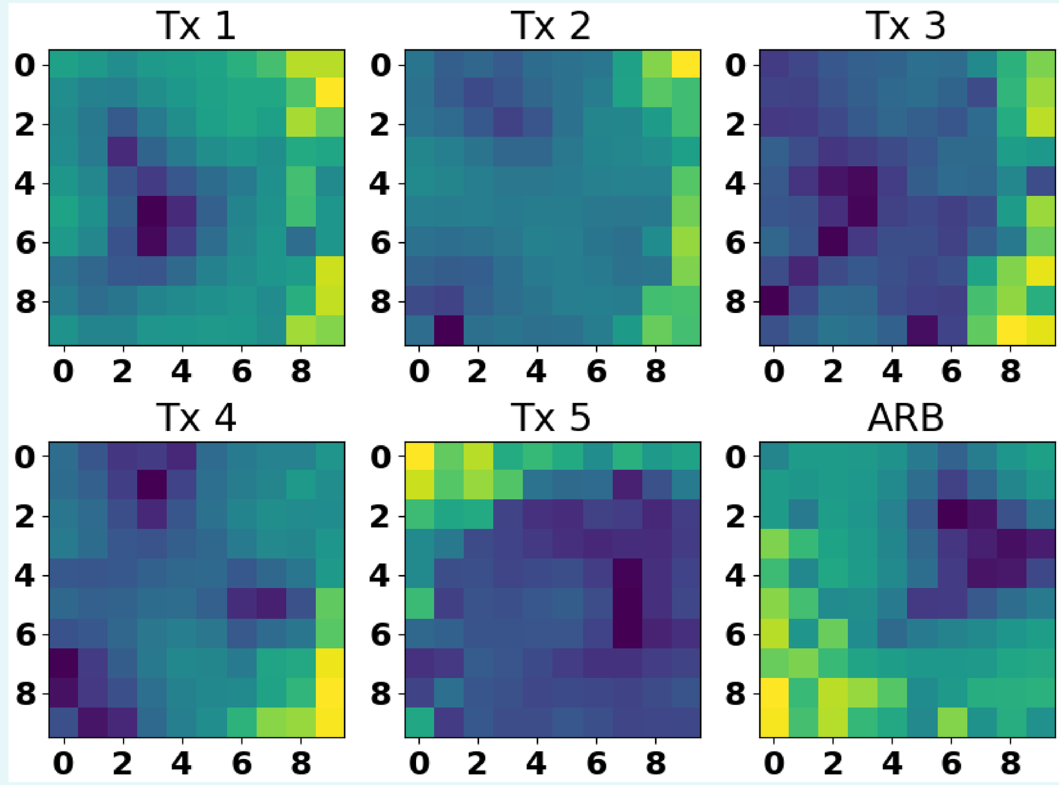


Figure 4 : Self Organizing Maps of LoRa Transmitters

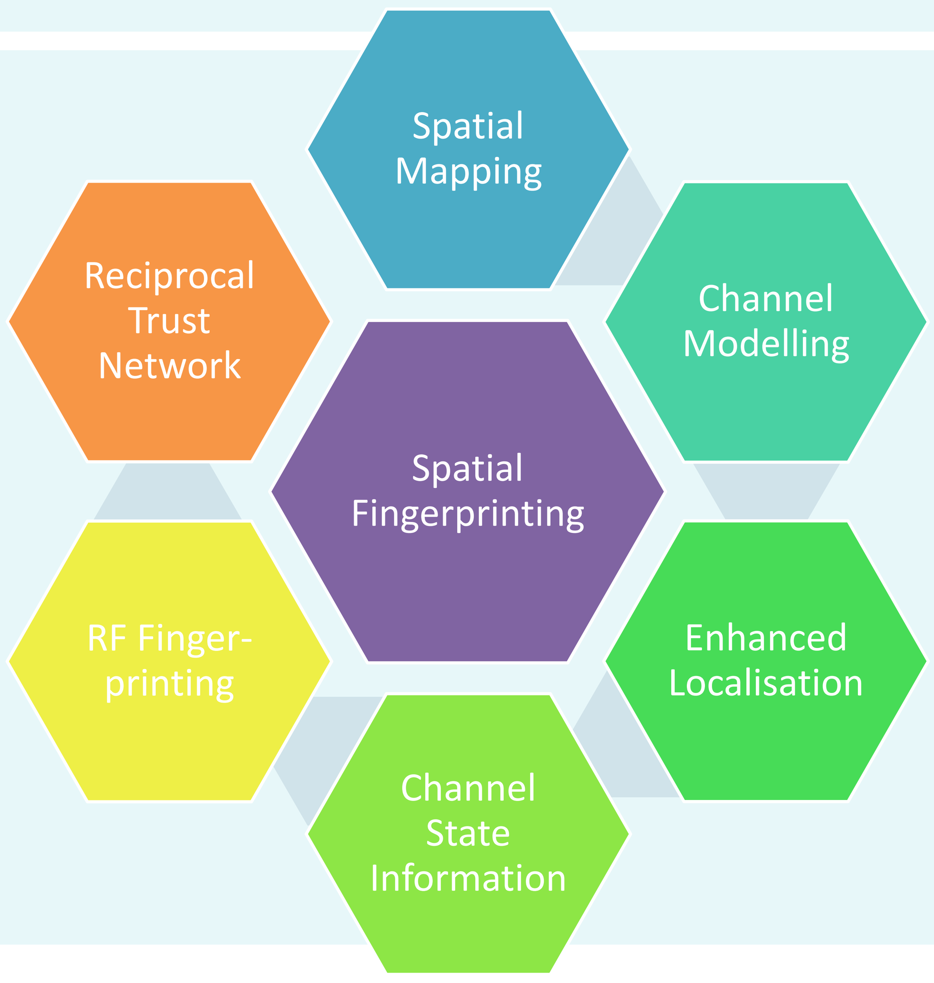
Table 1 : Method-Moment Correlation with Measured Data

Angle Set	Azimuth		Elevations	
	IEC	Huygens	IEC	Huygens
		Line of Sight		
-45°	0.5455	0.74	0.57	0.68
0°	0.2393	0.31	0.34	0.89
45°	0.7685	0.90	0.29	0.23
		Scattering Plate		
-45°	0.91	0.85	0.75	0.63
0°	0.92	0.91	0.80	0.84
45°	0.72	0.65	0.45	0.55

Conclusions and Further Work

Correlation between chamber measurements and the channel model using both ideal electric current sources to represent the antenna and Huygens sources demonstrates good agreement, with Huygens sources offering improved fidelity when there are no scatterers in the environment. For spatial intelligence nodes using embedded processing ideal electric current sources represent a computationally efficient method for reproducing the RF channel and providing the channel awareness required to use RF Fingerprinting in dynamic environments, and removing the embedded localization in training datasets.

In the future, spatial intelligence will be applied to mobile datasets, including the recently generated open dataset of LIDAR, Computer Vision, and Global Navigation Satellite System recordings, to investigate the potential for identifying and discarding RF Cyber attack.



[1] Pelham, T. G., Freire, A. L., Hilton, G., & Beach, M. (2021). Polarimetric Scattering with Discrete Raytracing for OTA Analysis. In *15th European Conference on Antennas and Propagation, EuCAP 2021* [9410981] (15th European Conference on Antennas and Propagation, EuCAP 2021).
[2] M. Nair, T. A. Cappello, S. Dang and M. A. Beach, "Rigorous Analysis of Data Orthogonalization for Self-Organizing Maps in Machine Learning Cyber Intrusion Detection for LoRa Sensors," in IEEE Transactions on Microwave Theory and Techniques, vol. 71, no. 1, pp. 389-408, Jan. 2023, doi: 10.1109/TMTT.2022.3223122.

Royal Academy of Engineering

This research was supported by SWAN: Secure Wireless Agile Networks, and the Royal Academy of Engineering and the Office of the Chief Science Adviser for National Security under the UK Intelligence Community Postdoctoral Research Fellowship programme.

University of BRISTOL