EPSRC Prosperity Partnership
Annual Report 2023
Grant Reference:EP/T005572/1
Training Grant Reference: EP/T518219/1

University Lead: Professor Mark Beach (University of Bristol)
Business Lead: Dr Magnus Sandell (Toshiba)

Project Title: Secure Wireless Agile Networks (SWAN)

Scan to view our new video
youtu.be/9VIuQt_tCRg

Summary

The SWAN Prosperity Partnership aims to develop Secure Wireless Agile Networks which are resistant to cyber-attacks and failures. This 5-year programme unites academia, industry, and government to innovate secure, resilient, agile, and sustainable wireless technology for future communication systems. Our collaborators include:

- **Toshiba Europe Limited:** Lead Business Partner; world-leading technology company, industrial IoT and open innovation, smart factories and manufacturing, quantum secure communication.
- **University of Bristol**: Lead Academic Partner; world-class expertise in physical layer wireless research, RF technologies, RF Open Attack Surface, RF Cyber Detection & Mitigation and Dynamic Spectrum Access.
- **Roke Manor Research Ltd**: Industrial partner; research and development capabilities across communications, networks and sensors with defence applications.
- **GCHQ**: Government partner; intelligence and security organisation; key advisor on UK government priorities and real-world technology applications.

Introduction and background

Secure wireless access is essential to the networks that underpin modern life, but many networks which rely on radio frequency (RF) interfaces are especially vulnerable to cyber-attacks or other failures. Disruption and attacks to networks could have catastrophic consequences for many industries such as robotics, power-plants and aviation. The SWAN Partnership is an effective collaboration with expert industry partners which provides us a head start in leading the technology for future safe communications. The SWAN programme is underpinned and focussed on 4 core research challenges:

1. **Threat Synthesis & Assessment: Identifying vulnerabilities in RF interfaces**
2. **RF Cyber Detection & Defence: Solutions for detecting attacks at scale**
3. **Cyber Secure Radio Design: Resilient and frequency agile RF transceivers**
4. **Secure Dynamic Spectrum Access (DSA): Robust 'active' primary user detection via collaborative sensing**

By understanding the vulnerabilities and how we can assess them, we can develop a sophisticated defence system against cyber-attacks.

Project achievements: outputs, outcomes and impacts

In the last year, SWAN has achieved significant strides in progressing the understanding and solutions of its research challenges. Our team persists in evaluating Radio Frequency (RF) vulnerabilities, exploring threats, and innovating new solutions to avert potential widespread damage. Collaborating with industry partners, we've introduced pioneering designs and methods which opens up new solutions for cybersecurity defence.

Research Challenge 1: Threat Synthesis & Assessment

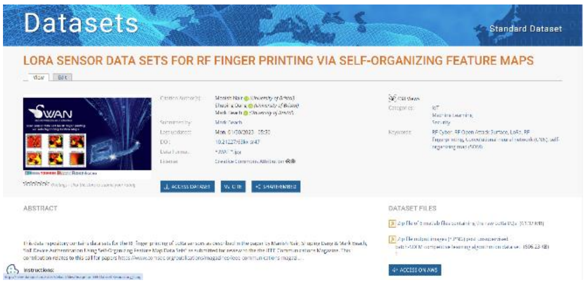
Progress to date: We are collaborating with the National Timing Centre developing alternative time distribution approaches to supplement our inherent reliance on Global Navigation Satellite Systems (GNSS). Working on raising the awareness of the vulnerabilities of time and frequency that is distributed by GNSS, as engineers need to understand the importance of time / synchronisation and how to manage any disruption. Here, there is some scope to design a specialised air interface for robust time distribution as well as applying GNSS jamming mitigation through spatial filtering mitigation (adaptive antenna arrays with null-steering).

We are also exploring vulnerabilities of 5G sidelinks by carrying out 5G experimentation with modem devices that support such modes. In parallel, SWAN researchers have been exploring the O-RAN Alliance and open RAN (O-RAN) architectures. 3GPP cellular deployments, in particular 5G, expose more attack surfaces which makes security modelling and management increasingly challenging. Due to low cost and accessibility of hardware and software, spoofing attacks on such systems may allow information leakage or DoS attacks facilitated by a rogue base station. Here, The Open RAN Alliance attempts to rectify and encourage manufacturers to build modular systems, as the open architecture will foster cheap and accessible solutions at sub-system level that are also available to attackers.

Research Challenge 2: RF Cyber Detection & Defence

Progress to date: We have been applying machine learning for base station (BS) authentication, thus providing a mechanism at the physical layer to prevent a rogue BS joining a network before higher layer signalling is initiated and association established. In our use case using a private 5G system, a rogue BS is introduced. Here, through waveform capture (see left), intrusion is detected. As mentioned above, O-RAN potentially opens up multiple attack surfaces which can be exploited by malicious actors. SWAN has been examining current O-RAN design principles and building an O-RAN system in the lab which may prove valuable for threats and mitigation strategies. Here, the RAN Intelligent Controller (RIC) is an enabler or gateway for adding smartness for Cyber Security and slicing enabled by AI / Machine Learning, with potential for a use case collaboration via DSIT Future Open Network project platforms.

In addition, Francesco Raimondo (SWAN Senior Research Assistant), has been working with Toshiba Europe to develop the UMBRELLA testbed (right), one of the largest world-leading open programmable Industrial Internet of Things (IIoT).



Datasets

Standard Dataset

LORA SENSOR DATA SETS FOR RF FINGER PRINTING VIA SELF-ORGANIZING FEATURE MAPS

Citation Author(s): Manish Nair (University of Bristol), Shuping Dang (University of Bristol), Mark Beach (University of Bristol)

Submitted by: Mark Beach

Last updated: Mon, 01/30/2023 - 05:50

DOI: 10.21227/[illegible]

Data Format: [illegible]

License: Creative Commons Attribution

Categories: IoT, Machine Learning, Security

Keywords: RF Cyber, RF Open Attack Surface, LoRa, RF Fingerprinting, Convolutional neural network(CNN), self-organizing map (SOM)

ABSTRACT

This data repository contains data sets for the RF finger printing of LoRa sensors as described in the paper by Manish Nair, Shuping Dang & Mark Beach, "IoT Device Authentication Using Self-Organizing Feature Map Data Sets" as submitted for review to the the IEEE Communications Magazine. This contribution relates to this call for papers https://www.comsoc.org/publications/magazines/ieee-communications-magazi...

Instructions:

DATASET FILES

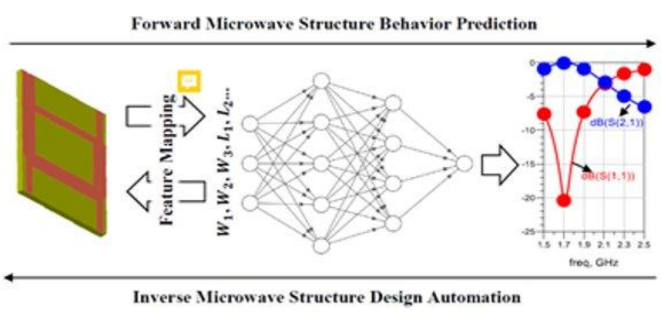
Zip file of [illegible] matlab files containing the raw LoRa I/Qs ([illegible])

Zip file output images (*.PNG) post unsupervised self-SOM competitive learning algorithm on data set (506.23 KB)

The team has also carried out further RF fingerprinting thus building on previous SWAN research, with I/Q sampling to create images to expand the dimensionality of an image based device classification process, including the dissemination via the IEEE Communications Magazine and a special issue on Data Sets for Machine Learning (see left).

Further, Roke has also developed a reinforcement learning based approach to controlling an electronic surveillance receiver. This has attracted further external interest and is now a potential product line. Toshiba has assessed how the operation of a RF PA in a WiFi router or smart phone could be impacted by RF cyber attacks in terms of the emission of spurious waveforms as well as enhancing the energy efficiency of a broadband RF amplifiers.

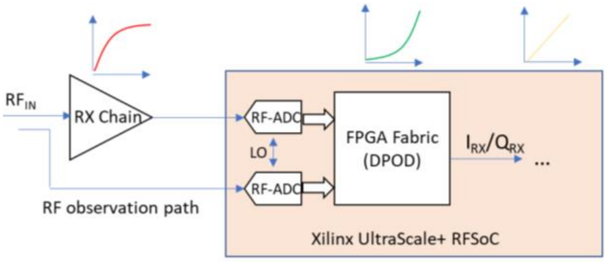
Research Challenge 3: Cyber Secure Radio Design



Forward Microwave Structure Behavior Prediction
Feature Mapping
$W_1, W_2, W_3, L_1, L_2, \ldots$
dB(S(2,1))
dB(S(1,1))
0
-5
-10
-15
-20
-25
1.5
1.7
1.9
2.1
2.3
2.5
freq, GHz
Inverse Microwave Structure Design Automation

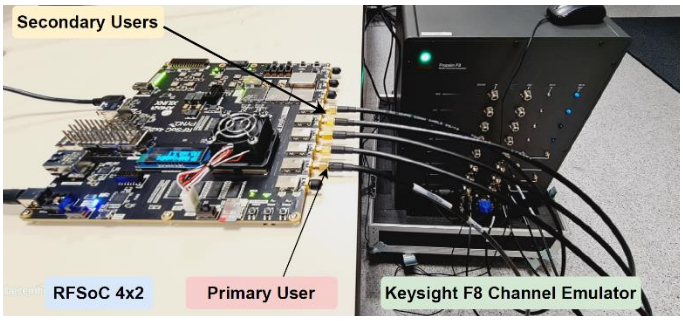
Progress to date: Facilitating new ways of conducting innovative RF design (left) through the use of machine learning to speed-up the design of complex RF circuitry has been advanced within SWAN.

SWAN's RF technology enablers include a novel Digital Power Amplifier (DPA) utilizing binary weighted switching amplifiers alongside load modulation. This digital architecture allows characteristics to be "tuned" to frequency bands of interest and thus offering improved frequency agility whilst maintaining DC to RF energy efficiency. Further, techniques to enhance the resilience of RF frontends (receivers) to both intentional and non-intentional jamming have included both waveform cancellation methods (aka Simultaneous Transmit And Receive (STAR)) as well as post digital correction for receiver non-linearities (see right: block diagram of the test-bed under evaluation).



Research Challenge 4: Secure Dynamic Spectrum Access

Progress to date: Dynamic spectrum access (DSA) is attracting interest as an efficient means for spectrum sharing by regulators. To overcome the inadequacies offered by the classical application of fixed geographical databases, robust and reliable spectrum sensing offers a potential solution. Here, cooperative spectrum sensing is a method that enhances reliability by utilizing hard- and soft-combining schemes to mitigate Spectrum Sensing Data Falsification (SSDF). In malicious RF cyber-attack on DSA enabled systems, hostile operatives intentionally transmit false sensing data, thus reducing spectrum availability and potentially introduce additional interference to primary users communications.



A hardware-in-the-loop evaluation of cooperative spectrum sensing using eigenvalue detection has recently been deployed in the lab, with initial sensing reliability ascertained over fading channels. Sensor nodes are based on the AMD RFSoC 4x2, with real-time channel emulation using a Keysight F8 channel emulator for the 3GPP extended pedestrian A (EPA) channel model with a 5Hz Doppler and varying levels of log-normal shadow fading as shown in the figure. Spectrum use detection through maximum-minimum eigenvalue (MME) has been bench-marked, with a particular focus on the probability of detection for varying degrees of log-normal fading received at the multiple (independent) sensing nodes.

Dissemination: Inside & Outside Government – SWAN members were present at multiple events to showcase the ongoing outcomes of our research:

Event	Link	Date	Reach
Ofcom	https://twitter.com/BristolCSN/status/1641822097545609216	March '23	National
Ukraine Delegation	https://twitter.com/BristolCSN/status/1633421472038281218	April '23	International
UKRI/EPSRC Prosperity Partnership Showcase	https://www.linkedin.com/feed/update/urn:li:activity:7067525817811021827	May '23	National
Smart Internet Lab Conference	https://www.linkedin.com/feed/update/urn:li:activity:7080583156700966912	June '23	National
DSIT Technical Advisory Team	https://www.linkedin.com/feed/update/urn:li:activity:7136345752674394112	Nov '23	National
Compound Semiconductor Applications Catapult	https://www.linkedin.com/feed/update/urn:li:activity:7141512226032537601	Dec '23	National

New collaborations

GCHQ and Foreign, Commonwealth and Development Office (FCDO) have initiated a new collaboration with academic staff associated with SWAN using the prosperity partnership as a catalyst. Some of the aims of this work focuses on operational constraints, creating new technologies and processing data in a different way. This new research programme will be taken forward over the next few years and would not have happened without the SWAN partnership being so active in this area and bringing the relevant experts together to tackle emerging challenges.

As part of a Department for Science Innovation and Technology (DSIT) 'Pulse' package to accelerate innovation activities and boost high growth sectors, SWAN was recently awarded £99,965. The funding will be used to focus on additional research activities such as RF Cyber Awareness in key UK sectors such as Agri-tech, and Enhanced Receiver Technologies within our work with Roke on enabling technology for Simultaneous Transmit and Receive (STAR).

Staff Highlights

New Starters - We have directly addressed the concerns raised at the mid-term review around staffing; all vacant posts are now filled with 5 members of research staff in post bring additional expertise to the partnership. In addition, Dr Andrew Austin has joined as a co-investigator following the departure of Kevin Morris to the University of Leeds. This puts the SWAN project team in a very strong position to fully address our project aims and objectives.

External Prize - Jiteng Ma (SWAN PhD Student) has recently won the COST CA20120 INTERACT Machine Learning Competition. The competition focused on ML-based indoor localization using MIMO CSI measurements, with NET challenge addressing calibrated predictive quality of service using on-field KPI measurements. Jiteng used a large ML model based on a Transformer encoder and ResNet as well as introducing data augmentation techniques in their solution.

Industry Engagement - Evangelos Xenos (SWAN PhD student), recently visited BT Adastral Park (Ipswich) to test and identify the performance characteristics of a newly prototyped communications phased antenna array, which is also the largest commercial antenna created for such purposes. Sanchita Kayal (SWAN PhD student) has been conducting a series of RF propagation measurements of reflections from surfaces in order to accurately identify how reflective surfaces may alter waveform polarisation. This has resulted in recent conference paper submissions to both IEEE AP-S/URSI 2024 and URSI UK Symposium 2024 as well as a platform for joint work within SWAN.

Research Papers – Highlights of recent publications include**:**

- A 47 % Fractional Bandwidth Sequential Power Amplifier with High Back-off Efficiency (IEEE, MENACOMM).
- A Learning-Based Methodology for Microwave Passive Component Design (IEEE Transactions on Microwave Theory and Techniques).
- Federated Radio Frequency Fingerprinting with Model Transfer and Adaptation (NetSciQCom 2023).
- IoT Device Authentication Using Self-Organizing Feature Map Data Sets (IEEE Communications Magazine)