1. Summary

The SWAN Prosperity Partnership is an ongoing 5-year research programme that aims to identify, highlight, and mitigate against vulnerabilities in Radio Frequency (RF) interfaces in critical wireless infrastructure. The project brings together expertise from academia, industry, and government to deliver a co-created research programme with real-world applications of national importance against a continually developing threat.

The consortium consists of:

- **Toshiba Europe Limited** (Bristol Research and Innovation Labs): Lead Business Partner; world-leading technology company; wireless and broadcast systems key business area.
- **University of Bristol**: Lead Academic Partner; world-class expertise in physical layer wireless research, RF technologies, 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

2. Introduction and background

Wireless connectivity is vital to society, and any disruption to it could have catastrophic consequences. There is growing evidence that networks are vulnerable to over-the-air cyber attacks, with adversary motives ranging from extortion to state subversion. We refer to this attack vector as the *RF Open Attack Surface.*

Through an integrated programme of activities, SWAN aims to address the following Research Challenges (RCs):

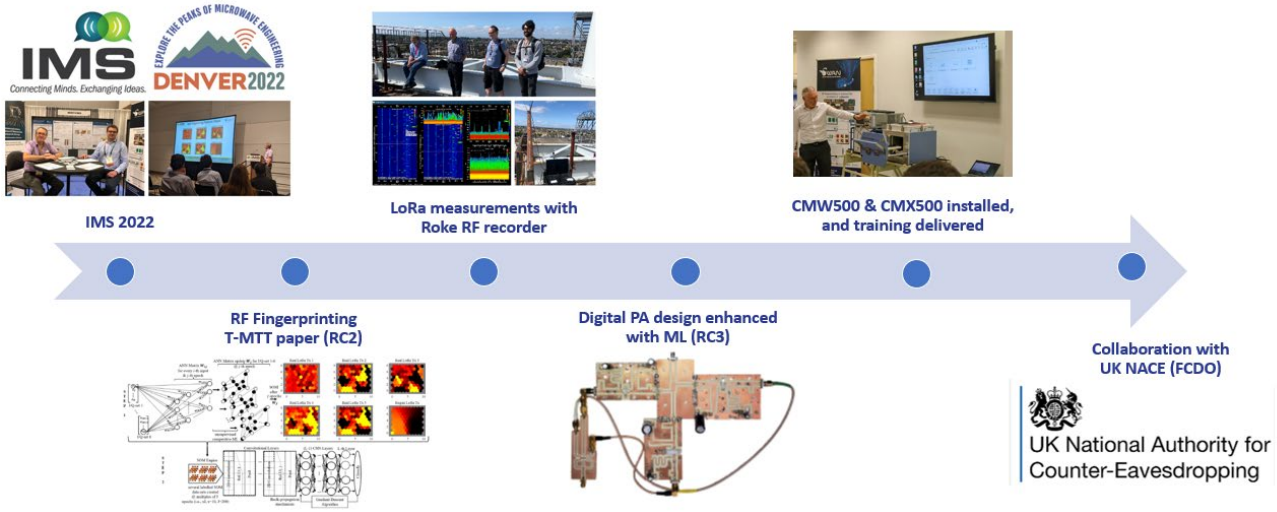
1. Threat Synthesis & Assessment: Identifying vulnerabilities in RF interfaces
2. RF Cyber Detection & Defence: Solutions for detecting attacks at scale
3. Cyber Secure Radio Design: Resilient and frequency agile RF transceivers
4. Secure Dynamic Spectrum Access (DSA): Understanding the vulnerabilities of sharing protocols

3. Project achievements: outputs, outcomes, and impact

Despite the challenges of starting the project during the restrictions of the Covid-19 pandemic, SWAN has been able to make good headway with addressing its Research Challenges. In the initial months of the project, we adapted our research plan to focus more on RC1: Threat Synthesis & Assessment, through remote training and building knowledge of the threat landscape (e.g. Roke's RF STRIDE cards). As restrictions have lessened and access to labs within each of the partners has once again been possible, we have been able to develop our activities on RC2: RF Cyber Threat Detection & Defence and RC3: RF Cyber Secure Radio Design, and focus more on dissemination and benefit realisation. Progress in each RC has been outlined in the table below:

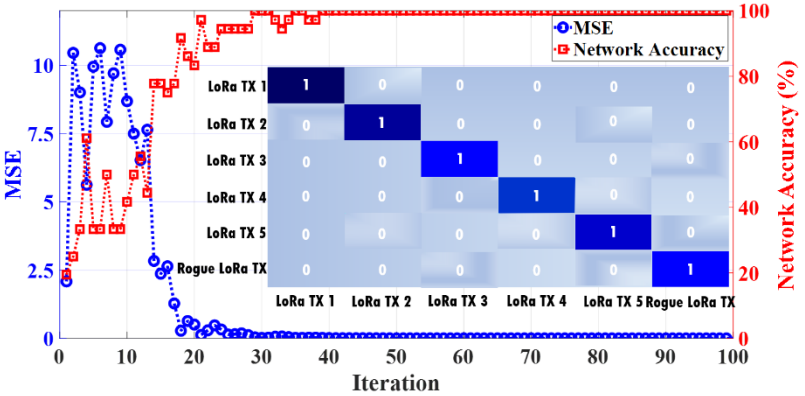
Research Challenge 1: Threat Synthesis & Assessment
Outputs: Staff training (with partners and externally), RF STRIDE cards, RF Vulnerabilities White Paper Progress to date: Research team and partners have benefited from 9 training sessions in cyber security and threat assessment. Knowledge of key methods shared (Roke RF STRIDE cards), case studies assessed.
Research Challenge 2: RF Cyber Detection & Defence
Outputs: Three-pillared LoRaWAN test facility, RF fingerprinting method, LoRa simulator Progress to date: Three-pronged LoRaWAN test facility developed: a lab-based penetration test-bed (UoB); a second testbed in parallel using different modules (Roke); and a third 'LoRa in the wild' testbed deployed throughout the Clifton campus at UoB facilitated by GCHQ. LoRa simulator and method of RF fingerprinting applied to LoRa using ML developed (video). Disseminated via prestigious journals and conferences.
Research Challenge 3: Cyber Secure Radio Design
Outputs: Blocker Resilient / High-Dynamic Range Receivers (HDRAS), Agile Digital Power Amplifiers (ADPAs) Progress to date: Considerable progress has been made in developing enabling technologies for a cyber secure radio architecture. Receiver technology has not been well addressed by the UK research community. In addition to jammer resilience, use in Dynamic Spectrum Sharing is an evolving need (6G and Ofcom). This has been characterised by the work of our aligned PhD students Ozan & Ma (Toshiba sponsored). Work is also being carried out on secure radio architectures by EPSRC studentship students (Xenos & Kayal).
Research Challenge 4: Secure Dynamic Spectrum Access
Outputs: Economic case for Secure Dynamic Spectrum Access (DSA) Progress to date: Aligned PhD student Simon Wilson has developed a tool characterising the economics for spectrum sharing with fixed links (4.2GHz), with London as the case study.

Headline Achievements in 2022



(RC2) RF fingerprinting: refining and disseminating outputs

In our 2021 Annual Report, we introduced the initial stages of development of our novel RF fingerprinting method, which uses signal processing and machine learning in the detection of rogue LoRa sensors. Since this report, we have expanded this technology further, refining our fingerprinting method to explore its effectiveness on correlated LoRa devices. In our latest transactions paper, published in the IEEE Transactions of Microwave Theory & Techniques, we provide a rigorous analysis of data orthogonalisation for self-organising maps (SOMs) in machine learning cyber intrusion detection, comparing it with traditional cyber intrusion detection techniques via a convolutional neural network (CNN). We propose an efficient way to produce SOMs of LoRa transmitters (TXs) and a potential rogue node prior to CNN classification. This approach minimises the mean square error (MSE) within the CNN using our specially constituted SOM engine for precisely profiling each LoRa TX with 100% accuracy.



As a key technology developed by SWAN, this work has been showcased at IEEE IMS 2022 (Denver, US), a major sector event with 440+ international companies exhibiting. A dataset paper has also been submitted to the IEEE Communications Magazine call for Data Sets for Machine Learning in Wireless Communications and Networks. Fingerprinting findings have been brought to other government sectors through GCHQ to explore solutions to specific security problems, with recent links to the UK National Authority for Counter-Eavesdropping.

(RC3) Resilient RF architecture design: digital PA and transmitter attack detection & prevention

Work on the design of a digital RF Power Amplifier (PA) for SWAN's cyber secure radio architecture has been co-produced with Toshiba and SWAN PhD student Jiteng Ma. The digital PA was selected for its agility and ability to adapt to spectrum and bandwidth. The benefits of this approach come at the expense of design complexity,

which is being overcome with ML. The format of the Prosperity Partnership scheme has lent itself well to resolving this issue, providing space and time needed to engineer a solution.

Alongside the work on the digital PA, Toshiba have also been leading additional work on transmitter (TX) resilience. Cyber-attacks on the receivers have been well documented. Recent studies have shown that attacks on the transmitter are also possible, where malicious interference injected into the transmitter output generates distortion of a transmitted signal, therefore preventing a receiver from cleanly demodulating the signal. In partnership with Toshiba, a novel architecture is being developed which will not only detect this form of attack but also mitigate it. This architecture is currently being evaluated in hardware at Toshiba's labs in Bristol.

Test-bed expansion: integrating new equipment and extending into 4G/5G

Building on the developments reported on our three-pronged LoRaWAN test facility in last year's Annual Report, this year we have continued to expand our test-bed work, embarking on several data collection exercises. Roke has been heavily involved in the LoRa testbed work, both with developing their own testbed to benchmark the one at Bristol, and lending equipment to take part in data collection. In addition, Roke has contributed aligned research time through private venture work in the cyber secure radio space including research into vulnerabilities of advanced FEC to jamming and detecting anomalous signals.

The project has recently acquired a 4G/5G base station and network emulator (Rohde & Schwarz CMX500 & CMW500) RF penetration test facility for handset/modem evaluation (funded by UoB), which will enable the project to bring its research programme into the next phase. Training on this new equipment, available to team members across the partnership, has been supplied in two courses by Rohde & Schwarz.

Dissemination and engagement

SWAN has disseminated its findings at several key conferences and events this year, including:

Event	Type	Date	Reach
IMS 2022 Denver	Workshops, paper presentations, demo stand	June 2022	International
IEEE VTC Fall 2022	Workshop keynote	September 2022	International
IEEE SSPD 2022	Paper presentation	September 2022	International
CW Radio SIG LoRa event	Workshop talk	September 2022	National
DSTL OFEME 2022	Poster presentations	November 20222	National

The team have also held several internal talks and workshops across the consortium, with guest speakers from external collaborators. Multiple lab visits have taken place, showcasing the SWAN test-bed to teams from industry, including BT, Vodafone, Samsung, and the Compound Semiconductor Applications Catapult. The project has also been able to expand its engagement with teaching, with planned undergraduate projects using Raspberry Pi kits to demonstrate SWAN's prototype lightweight IoT. The partnership continues to make use of its active

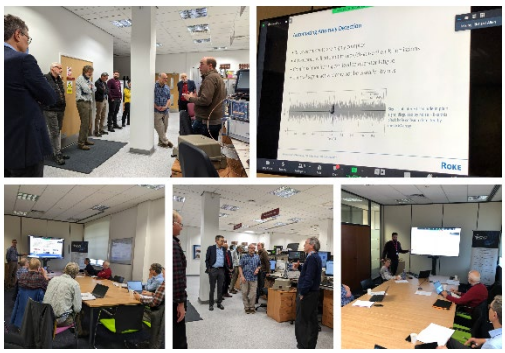
network to disseminate findings via a quarterly newsletter; a website featuring publications, resources, blogs, and opportunities; and active Twitter and LinkedIn pages to widen engagement across the sector.

4. New collaborations

SWAN's new collaborative activities with parties outside the consortium this year include:

- Contributing to PETRAS' Governance Board in July 2022 as part of an ongoing collaboration
- Participating in a 6G Keysight event in August 2022
- Presenting to the Foreign and Commonwealth Development Office at Hanslope Park in October 2022, part of an ongoing collaboration focused around SWAN's RF fingerprinting work

In the last year, two bi-annual External Advisory Board meetings have taken place. As a result of our last meeting in November 2022, advisors from companies working with national critical infrastructure brought forward real-world applications for SWAN's technologies, with potential for collaborative work in one of SWAN's WPs in 2023.



5. Staff Highlights

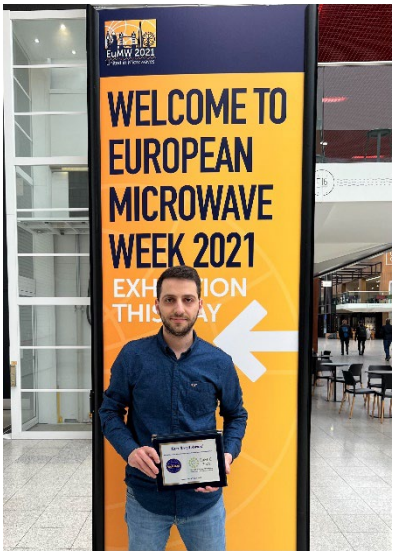
Key staff changes and awards since December 2021:

Next destinations:

- Dr Vaia Kalokidou (SRA) went on to join the Satellite Catapult (Jan 2022)
- Dr Chuanting Zhang (SRA) returned to China to continue his career in academia/industry (Sept 2022)
- Prof Kevin Morris (Co-I) took up a post as Head of School at the University of Leeds (Aug 2022)
- Dr Manish Nair (SRA) returned to India to continue his career in academia/industry (Jan 2023)

New joiners:

- Sanchita Kayal joined as PhD student, funded via SWAN's training grant (Sept 2022)
- Francesco Raimondo joined as an SRA, bringing expertise from aligned project SYNERGIA (Nov 2022)
- Robert Zakrzewski joined as an RA, also bringing aligned knowledge from SYNERGIA (Dec 2022)



Awards:

- PhD student Sarmad Ozan won the delayed Tom Brazil Essay competition prize at EuMIC2021.
- Dr Timothy Pelham was awarded an Nvidia Accelerator Grant for equipment and training towards his spatial fingerprinting research (RAEng Fellowship), and will be presenting a poster to Peers and MPs in Westminster in March 2022 as a finalist for STEM for Britain 2023.
- Dr Tommaso Cappello and Prof Mark Beach are part of the consortium that has been successfully award the DCMS FONRC grant REASON (PI Dimitra Simeonidou), building on SWAN's agile RF research.