1. Summary

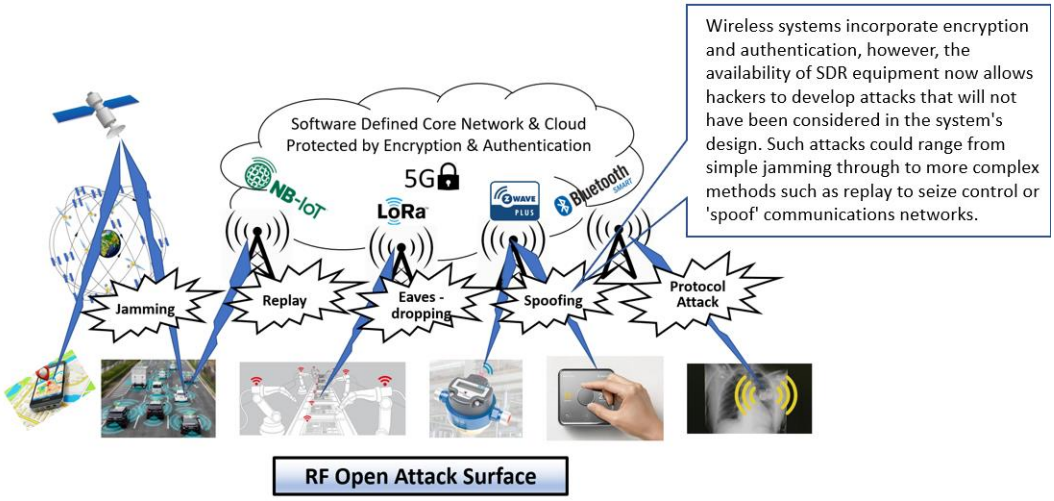
Wireless access is essential to the networks that underpin modern life, but many networks which rely on Radio Frequency (RF) interfaces are especially vulnerable to cyber-attacks or other failures. Jointly funded by EPSRC, Toshiba Europe Limited (TEUR), Roke Manor Research Limited, GCHQ, and the University of Bristol, the SWAN Prosperity Partnership focuses on the creation of Secure Wireless Agile Networks (SWAN) that are resilient to both cyber-attacks and accidental or induced failures.

2. Introduction and background

SWAN aims to create hardware and software enabling technologies for radio systems that can be truly software defined, and Secure by Design down to the basic levels of system functionality, such as operating frequency bands, modulation, and multiple-access protocols, as well as the surrounding frameworks needed to make resilient and secure systems.

SWAN's key aims are:

- To identify vulnerabilities in RF interfaces;
- To develop techniques to detect and mitigate against the effects of cyber-attacks and other subversion;
- To create enabling technology for Software Defined Radios (SDR) following Secure by Design principles;
- To develop systems that are more resilient and secure, to enable robust Dynamic Spectrum Access (DSA).



As a Prosperity Partnership project, SWAN brings together key expertise from academia, industry, and government to deliver a co-created and evolving research programme that will have real-world industrial applications of national importance against a type of threat that is continually developing.

Throughout the 5-year programme, SWAN will deliver impact through our business partners, Toshiba and Roke, embedding technology and know-how in products; a series of multi-faceted external dissemination activities; influencing standards, policy and regulation; as well as encouraging the adoption of Secure by Design within engineering curricula through university degree programme accreditation.

3. Project achievements: outputs, outcomes, and impact

From the project's kick-off in February 2020 until now the global pandemic has been source of multiple challenges. The project teams have had to adapt to new ways of working, with limited access to labs. We have experienced delays with recruitment, of both Post-Doctoral Research Associates and PhD students. With financial restrictions in place due to the pandemic, we have also seen delays to secondments and PhD sponsorships that our partners had pledged as part of the co-created programme of research.

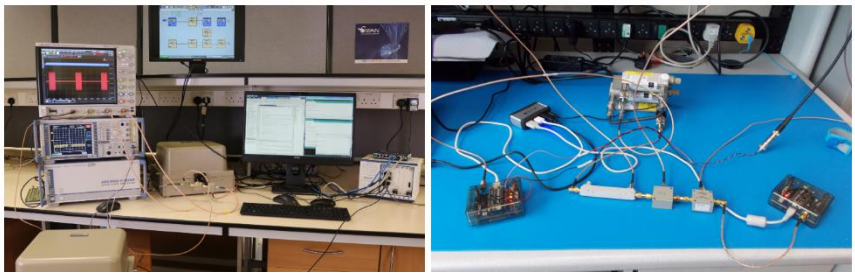
In spite of this, the management team have been able to ensure consistent engagement. We have mitigated against the impacts of reduced spending capabilities by finding alternative ways for partners to contribute, and have successfully applied for an extension to our training grant (EP/T518219/1) to accommodate the delays to student recruitment. The new risks posed by Covid-19 have been carefully monitored and mitigated using risk registers that are updated on a regular basis by the management team.

As restrictions have relaxed our researchers have been able to access the lab on a more regular basis. The project has been able to make several important technical breakthroughs in recent months, with significant headway made into one of SWAN's Research Challenges: RF Cyber Threat Detection and Defence.

Selected project highlights:

RF penetration testbeds:

The ever-increasing use of low-power wireless communications for sensing and monitoring applications, including in critical infrastructure, demonstrates a need to make this technology robust against cyber-attacks.

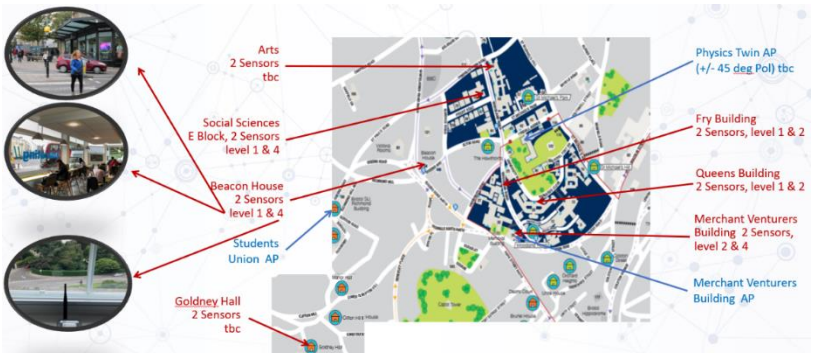


The RF penetration testing facilities at the University of Bristol and in Roke

Within SWAN, we have chosen LoRaWAN, a proprietary low-power wide area technology developed for the Internet of Things (IoT), as a candidate for detailed evaluation given its increasing prevalence within remote telemetry applications.

Throughout the last year, the SWAN research team have been developing three pillars of a LoRaWAN test facility: an initial penetration testbed set up in the CSN lab in the University of Bristol; a second LoRa testbed set up in parallel using different modules based out of partner company Roke's headquarters in Romsey; and a third 'LoRa in the wild' testbed deployed throughout the Clifton campus at the University of Bristol.

The RF penetration testing facilities at both Bristol and Roke use screened enclosures for conductive testing, allowing us to subject various candidate wireless technologies to cyber attack, including synchronised jamming and customised waveform design. Within the Bristol setup we can also capture RF waveforms and convert these back to IQ baseband for further analysis, such as RF fingerprinting.



'LoRa in the wild' – Clifton campus testbed

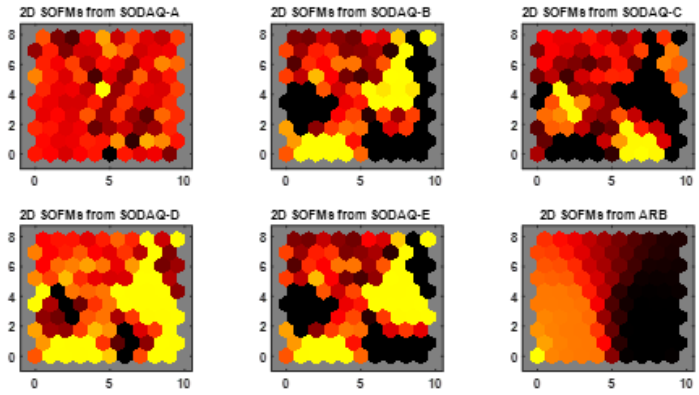
Our lab-based testbeds are complemented by a rollout of LoRaWAN deployments in the Clifton campus at the University of Bristol, thanks to the underpinning work by Wael Boukley Hasan funded through NSTIx. Here we have three access point locations and over 20 static deployments of sensors. For each of our static sensor locations, we have a sensor at street level, capturing wireless variations due to the motion of people and vehicles, as well as a sensor higher in the building away from localized motion. This allows us to capture the reported signal to noise ratio (SNR) level from multiple static

sensors at multiple locations for both busy and quiet times in the city over many months. This dataset will allow us to determine if a simple measure such as SNR is a sufficiently good marker for rogue sensor deployment detection in some less critical applications.

Developing machine learning (ML) techniques for RF fingerprinting:

By developing methods of RF fingerprinting that can be applied to LoRa, the SWAN research team hopes to be able to create unique identifiers, analogous to biological fingerprints, that will enable networks to detect potential intrusions (see video). Through signal processing and the application of machine learning, the individual characteristics of the analogue components within each of the LoRa modems can be readily identified. This RF fingerprint can be used to identify if a sensor has been replaced by a rogue device, thus aiding cyber detection without seeking modifications to the underlying product. Further, this technique is resistant to 'MAC spoofing', a method commonly employed by adversaries.

SWAN's postdoctoral researchers are developing a two-pronged methodology for RF fingerprinting of the start-up chirps from a LoRa modem. Firstly, a self-organising feature map (SOFM) is trained using unsupervised competitive learning of neural network (NN) clusters to produce two-dimensional (2D) discretised representations of the input space (as illustrated, right).



An example of the 2D self-organising feature maps

Secondly, an optimised deep convolutional neural network (CNN) architecture with batch normalisation at every convolutional layer is proposed. Further research for increasing the robustness of this approach will incorporate adding additive white Gaussian noise (AWGN) and channel impairments for the emulation of OTA transmission.

Training and career development of the SWAN team:

We have continued to host training webinars with SWAN's partners and external collaborators throughout 2021. The following training activities have taken place this year:

- Physical Layer Attacks on LTE (Roke)
- Hardening COTS Wireless Communications and Networking Technologies for Mission Critical Applications – A Case Study of 4G/LTE (General Dynamics)
- Lightweight AI in low-power IoT security: A joint PETRAS-SWAN event
- Internal workshops at both Toshiba and Roke in December 2021

After early delays due to restrictions resulting from the Covid-19 pandemic, we have changed one of our initial deliverables, the RF Hackathon, to focus instead on our internal RF penetration testbeds. This reflects the strategic direction of the project, and also allows for knowledge transfer and co-creation between partners.

Engagement and dissemination:

Throughout the year, the SWAN team have shared their initial findings with the wider research community, security experts, and policy makers, at key events on both a national and international scale. Selected highlights include:

- IoT Security Foundation Virtual Conference (November 2021) – Recorded Presentation
- Brooklyn 6G Summit (October 2021) – Virtual Demo
- 6G: Software Defined Radio and RF Sampling (September 2021) – Recorded Presentation

We have continued to build our network across these communities through a quarterly newsletter reaching a mailing list of key stakeholders; a website featuring publications, resources, blogs, and opportunities; and active Twitter and LinkedIn accounts to widen our engagement across the sector.

SWAN's third External Advisory Board

In the last year, two bi-annual External Advisory Board meetings have taken place. Our last meeting in September 2021 was our first hybrid in-person meeting since restrictions relaxed. This was an excellent opportunity to share our recent findings with our EAB members and showcase the work of SWAN's research team and PGRs. Howard Benn (Samsung) served as Acting Chair, standing in for John Haine.

4. New collaborations

The SWAN team have continued to build several new collaborative relationships with parties outside the consortium, including: PETRAS, General Dynamics, the National Nuclear Laboratory, Dstl, BT, NI, DCMS, UK SPF and Digital Catapult. These relationships have the potential to develop into collaborative activities in the year ahead, including delivering additional training webinars, joint events, and PhD student mentorship. Highlights from aligned projects include:

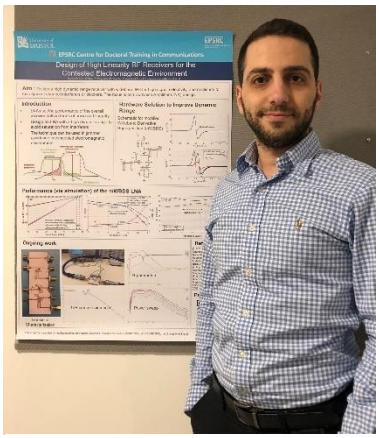
- Dstl CEME (Contested Electro Magnetic Environment) via BAE: this collaboration with the School of Maths focusses on theoretical & practical limits of wireless connectivity. Extension to include RF power amplification state of the art limits.
- DCMS / SPF 6G: a series of workshops on academic research towards 6G, highlighting strengths and novelty. Mark Beach served as a member of an expert group recommending 'interventions' to position the UK as a leader in 6G technologies and applications. DCMS commissioned report now available to view.

5. Staff Highlights

SWAN benefits from a team of highly skilled researchers and PhD students from across the partnership. Since the December 2021, SWAN has welcomed several new team members, including:

- Dr Magnus Sandell became SWAN's Business PI in Toshiba, SWAN's Lead Industrial Partner in March 2021. Magnus replaced Dr Woon Hau Chin who joined Viavi Solutions as the Director of Research and Technology.
- Dr James Luke joined Roke in January 2021 as Innovation Director and acts as the business and strategic lead for Roke within SWAN, replacing Dr Andrew Rogoyski who joined the Surrey Institute for People-Centred AI.
- Dr Shuping Dang joined the CSN Research Group at the University of Bristol as a Lecturer in AI and ML in Wireless Networks in June 2021. He is one of the two academic post holders aligned to the project.
- Michael Mikita joined the team as SWAN's Specialist Research Technician in June 2021.
- Evangelos Xenos is the first of the two studentship recipients funded through our training grant.
- Dr Chaunting Zhang will be joining in January 2022 (subject to visa and work permit) as a Senior Research Associate, replacing Dr Eyad Arabi who moved on to a new role with CML Microcircuits UK Ltd in June 2021.

We are currently in the process of recruiting another Post-Doctoral Research Associate in RF Cyber Security to replace Dr Vaia Kalokidou who will be leaving the project in January 2022. Though we have been able to secure one of the two PhD studentships from our training grant, the second offer recipient has sadly been forced to decline due to the situation with Covid-19 restrictions in their home country. We have gone back out to advert for the second studentship and hope to have someone in place by January 2022.



Sarmad Ozan with his winning poster

Several staff members aligned to SWAN have received awards this year:

- PhD student Sarmad Ozan won one of the top poster prizes at the Dstl's 2021 OFEME Symposium for his poster 'Design of High Linearity RF Receivers for the Contested Electromagnetic Environment'.
- Dr Timothy Pelham was awarded a UK IC Postdoctoral Research Fellowship for his work spatial fingerprinting for self-securing wireless networks, which will be tied to SWAN's programme of work.