Evaluating Cooperative Spectrum Sensing: A Hardware-in-the-Loop Approach

Mir Lodro, Simon Armour, Mark Beach

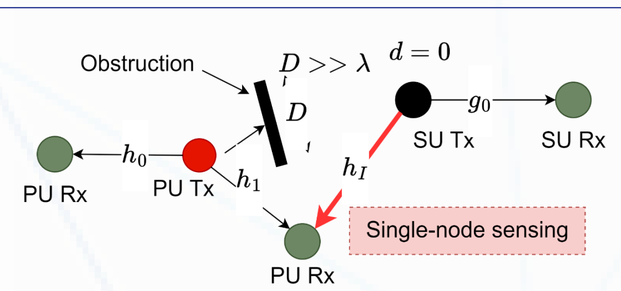
SECURE WIRELESS AGILE NETWORKS

Summary

With the increasing demand for wireless connectivity for both personal use and the internet of things, the demand for spectrum access is driving the need for more flexible and efficient management. This is driving innovation in technologies to support spectrum sharing, with regulators such as the FCC and Ofcom incentivizing adoption. There is also a growing interest to complement geographical databases governing access to provide a more real-time or dynamic view of spectrum utilization. Here the use of Co-operative Spectrum Sensing is considered as a key component for reliable Dynamic Spectrum Access.

Motivation and Background

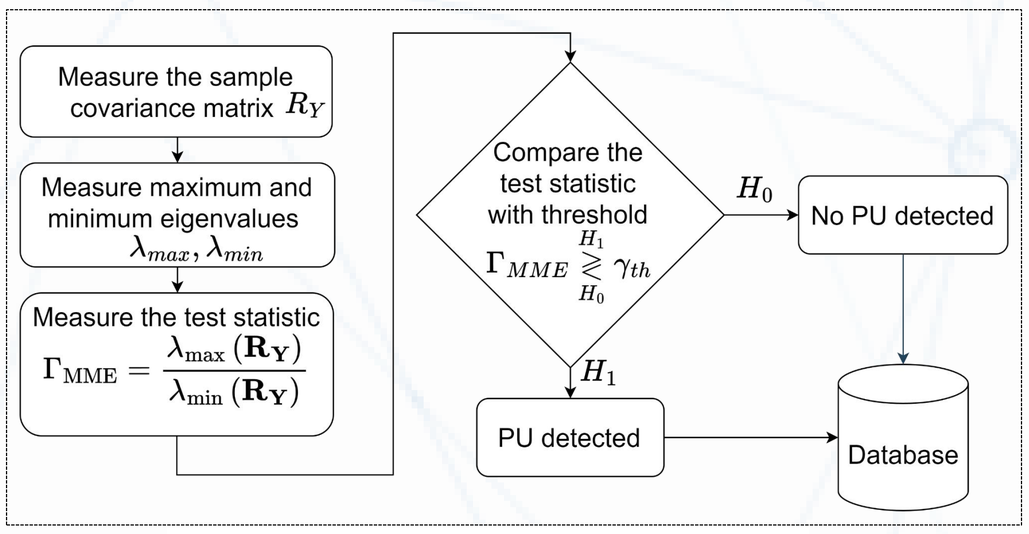
Observing spectrum occupancy from a single location is susceptible to an obscured measurement due to blockages and antenna orientation – the hidden node problem. Spatial diversity through spatially distributed sensors circumvents this problem, and when combining with appropriate signal conditioning can enhance reliability of detection.

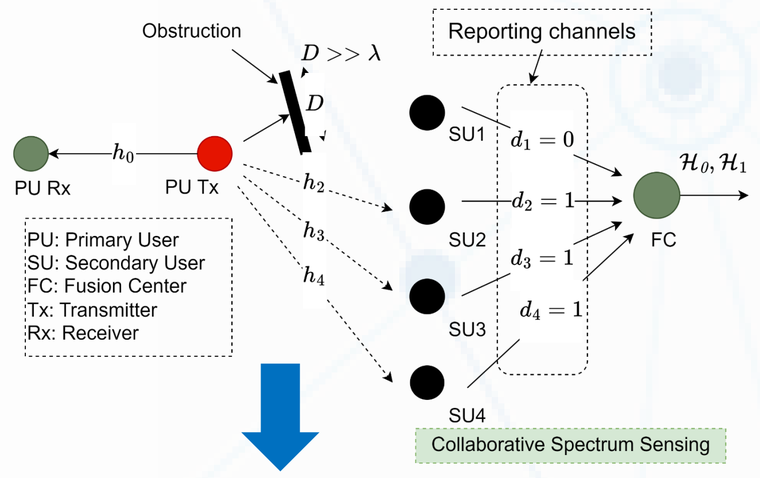


Spectrum Sensing Flowchart

- Variety of methods for sensing
  - ➢ Eigenvalue detection
    - ✓ No PU information
- Spectrum sensing a binary hypothesis problem:

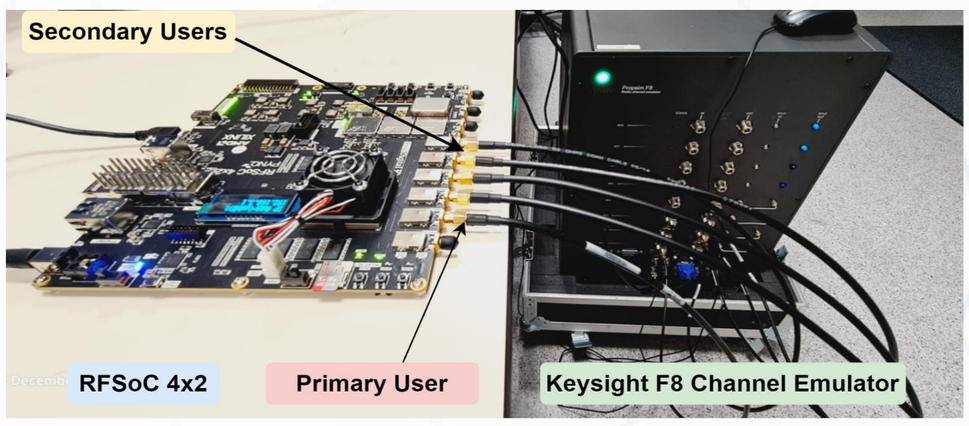
$$\Gamma_{\mathrm{MME}} = \frac{\lambda_{\max}(\mathbf{R_Y})}{\lambda_{\min}(\mathbf{R_Y})} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \gamma_{\mathrm{th}}$$





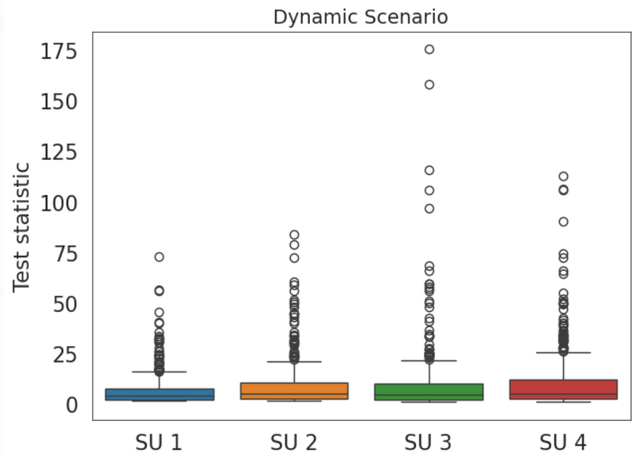
Hardware-in-the-Loop

- HIL testing of co-operative spectrum sensing:
  - Keysight radio channel emulator
  - AMD RFSoC 4x2 wideband transceiver
  - Keysight DSO-X 92004A oscilloscope
  - NI PXIe-8880 embedded controller
- Monte-Carlo simulations are performed at each transmit power level of the RFSoC 4x2
- Channel model for all the secondary users is 3GPP EPA channel with 5 Hz Doppler

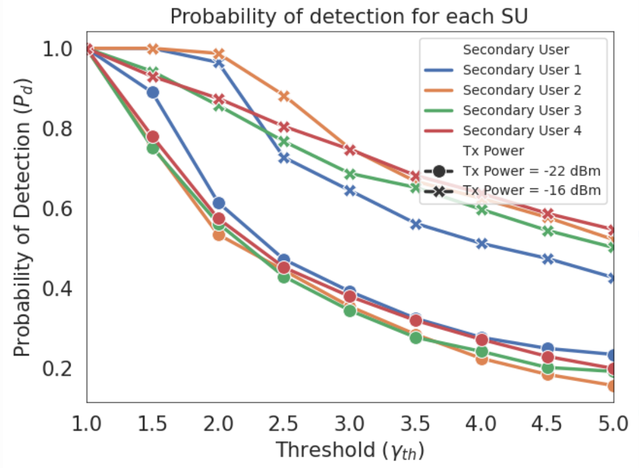


Results and Discussions

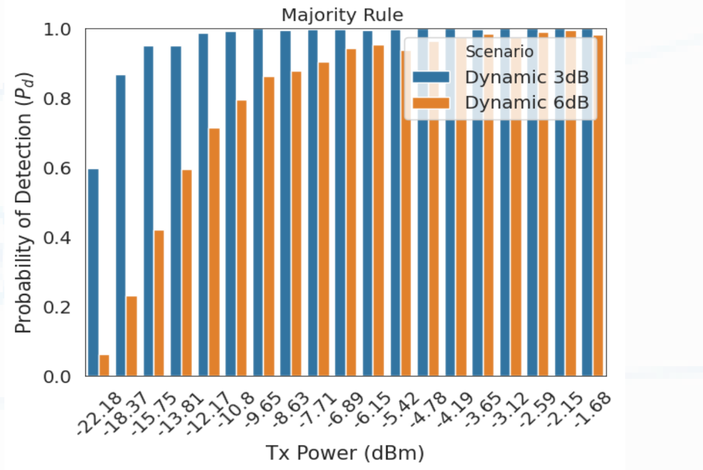
- The test statistic of each SU in the static scenario shows less variation as compared to dynamic scenario
- The probability of detection decreases as the shadow fading increases from 3 dB to 6 dB



Boxplot of MME test statistic of SUs for dynamic scenarios with lognormal shadowing of 3dB.



Probability of detection versus threshold for each SU at two transmit power levels.



Probability of detection vs PU transmit power at 3 dB and 6 dB lognormal shadow fading.

Conclusion and Further Work

- Hardware-in-the-Loop testing of cooperative spectrum sensing is performed using RF channel emulator and RFSoC 4x2 for different levels of shadow fading. The measured probability of detection gets worse as the shadow fading increases.
- Future work includes the diversification of sensor nodes and investigation of collaborative spectrum sensing in a complex spectrum sharing scenarios.

References

[1] M. Ghosh, "Evolution of sharing in 6 GHz," *IEEE Wireless Communications*, vol. 30, no. 5, pp. 4-5, 2023.
[2] M. H Dortch, "Principles for promoting efficient use of spectrum and opportunities for new services," *Federal Communication Commission*, March, 2023.
[3] Ofcom, "Supporting increased use of shared spectrum," November, 2023.
[4] A. Mariani, A. Giorgetti, and M. Chiani, "Robust detection with low-complexity SDRs: A pragmatic approach," in 2018 *IEEE 29th Annual Internation Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*. IEEE, 2018, pp. 1-6.

This research was supported through the UKRI/EPSRC Prosperity Partnership in Secure Wireless Agile Networks (EP/T005572/1).

Communication Systems & Networks Research Group
Merchant Venturers Building, Woodland Road, Bristol, BS8 1TR

@PartnershipSWAN
https://www.swan-partnership.ac.uk/
linkedin.com/company/swan-prosperity-partnership
swan-programme@bristol.ac.uk

Engineering and Physical Sciences Research Council
TOSHIBA
University of BRISTOL
ROKE
GCHQ

Are You Being Spoofed by a UAV?

Evangelos Xenos

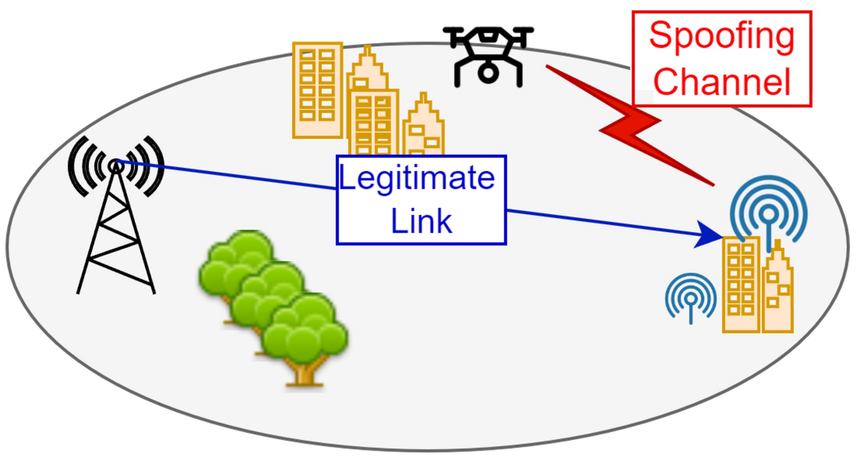
Supervisors: Dr. Andrew Austin, Dr. Simon Armour & Prof. Mark Beach

Aims & Objectives:

- Obtain, process and analyze real-measured and simulation data to model airborne activity threats.
- Enhance understanding of A2G propagation characteristics in urban scenarios and apply knowledge in future deployments.
- Find a quick and easy way to determine if a ground receiver is being spoofed by an airborne adversary (e.g., a drone).

1. Introduction

Drones are becoming very easy to acquire and deploy and lack of regulations enforced make them a cheap way to disrupt sensor networks.

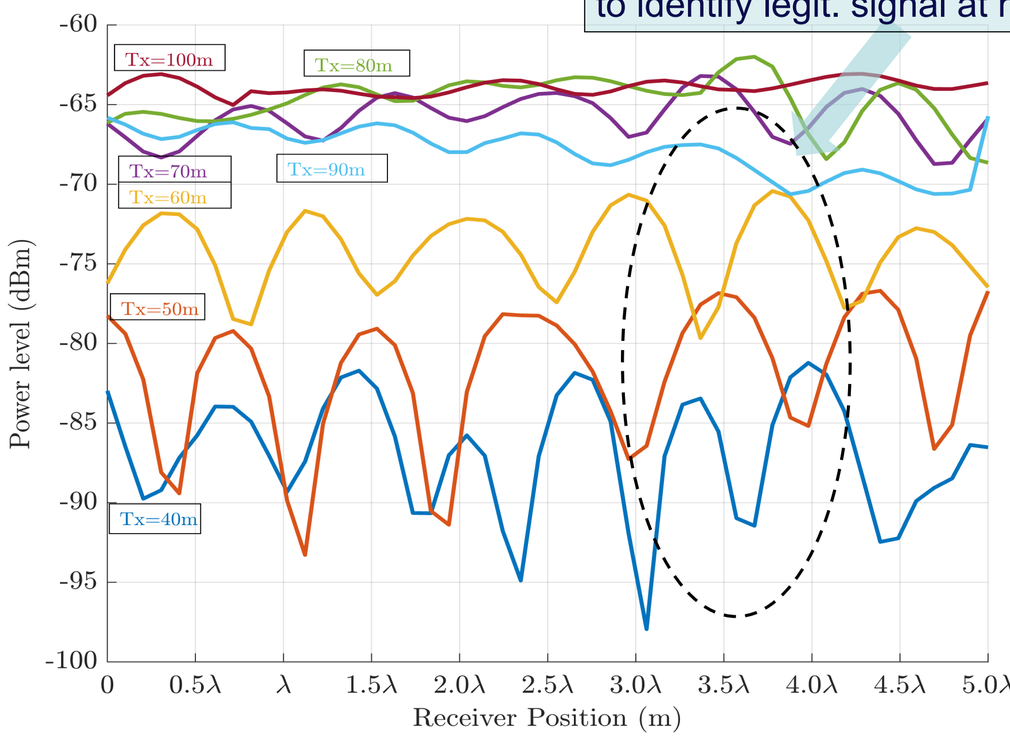


2. Methodology

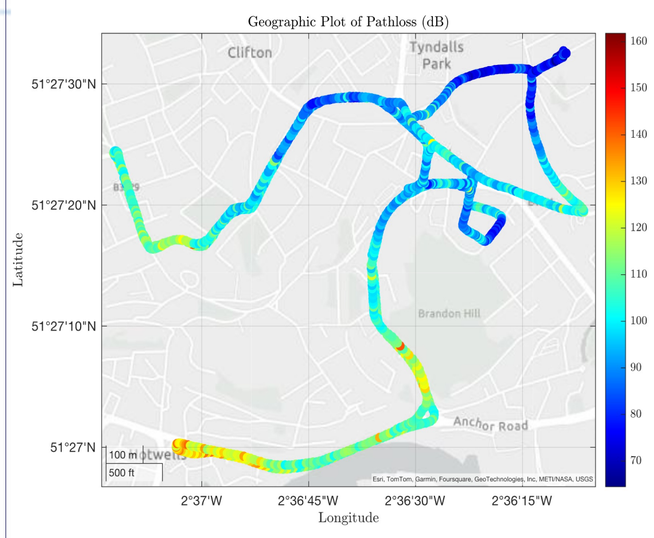
- Simulate realistic environments for Bristol with Ray Tracing and follow-up the simulation with real measured data.
- Tx @HH Wills, FR3 5.7GHz, sectored, and mobile Rx with omni and directional antennas, sampled every 0.25m.
- Compare outcomes over a LoS terrain accounting for buildings, elevation and clutter, both statistically and analytically.
- Determine properties that could distinguish the legitimate signal from a malicious one.

3. Analysis & Results

Increasing TX height: increases power (expected) and decreases fade depth - harder to identify legit. signal at higher altitude

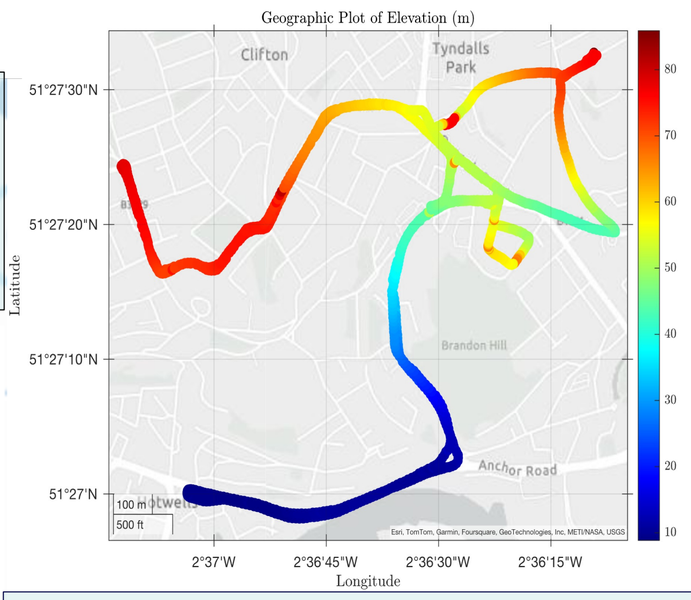


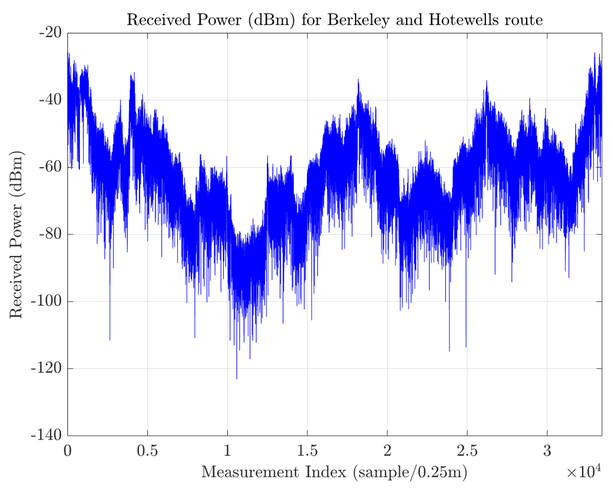
Ray Tracing Simulation result



Ground measurements of signal propagation, from an elevated Tx (h=126m) to a mobile Rx across the city of Bristol.
Properties such as Pathloss, Received power, Rx ground elevation and GPS coordinates were extracted to create comprehensive relations between PL and elevation difference between Tx & Rx.

Tx elevation creates a similar scenario to flying a drone within an urban scenario providing detail on propagation and fading channel characteristics (measured data).





Investigation to identify mutual characteristics between RT simul. and real measurements. Understand fading envelopes with elevation relation and mask malicious signal as the expected legitimate.

4. Conclusions & Future Work

- RT indicates fading envelopes can be used to identify UAV spoofing.
- Drone deployment and measurement of channel and fading characteristics in suburban scenarios and free space.
- Investigation of additional PHY properties exploitation to identify malicious signals over legitimate on Rx end.

Ground Measurements were conducted in collaboration with Richard Rudd (Plum consulting), on urban propagation and slant clutter modelling for Recommendation ITU-R P.2108 in Bristol 20-22 Jan. 2025.

This research was supported through the UKRI/EPSRC Prosperity Partnership in Secure Wireless Agile Networks (EP/T005572/1).

Communication Systems & Networks Research Group
Merchant Venturers Building, Woodland Road, Bristol, BS8 1TR

@PartnershipSWAN
https://www.swan-partnership.ac.uk/
linkedin.com/company/swan-prosperity-partnership
swan-programme@bristol.ac.uk

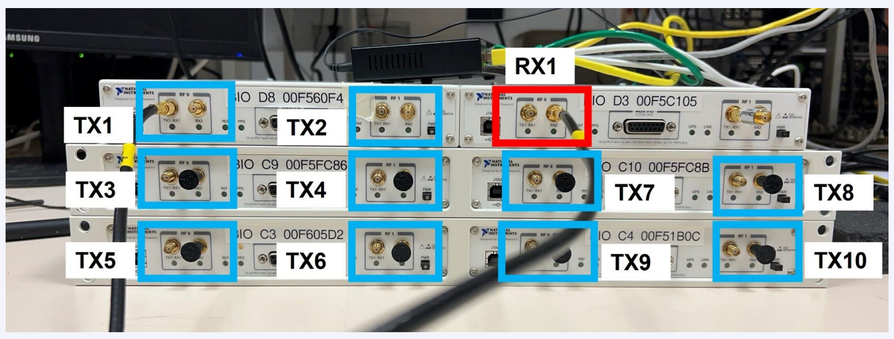
Assessing Wireless Standards for IoT Security Using Deep Learning-Based Radio Frequency Fingerprinting

Mr. Hao Li, Dr. Jiteng Ma, Dr. Shuping Dang, Prof. Robert Piechocki, Prof. Mark Beach
hao.li@bristol.ac.uk

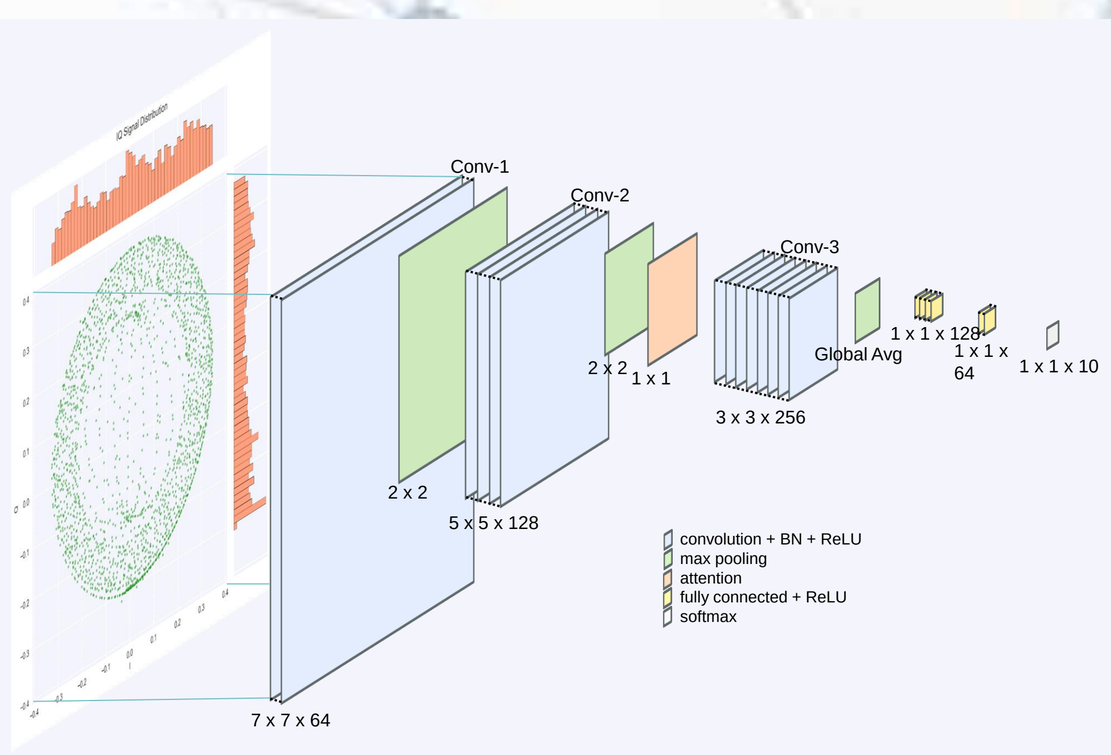
Introduction :

Radio Frequency Fingerprinting (RFFI), a physical-layer authentication method, utilizes hardware-specific features such as Carrier Frequency Offset (CFO), IQ Imbalance, and Power Amplifier Nonlinearity for device identification. Unlike cryptographic methods, RFFI requires no modifications to the transmitter and is well-suited for resource-constrained IoT devices. Existing RFFI research primarily focuses on single protocols, lacking systematic comparison across multiple protocols. This study addresses this gap by evaluating the preambles of WiFi, LoRa, and Bluetooth using a unified USRP X310 platform and a standardized Convolutional Neural Network (CNN) architecture, revealing significant differences in classification accuracy and robustness across protocols.

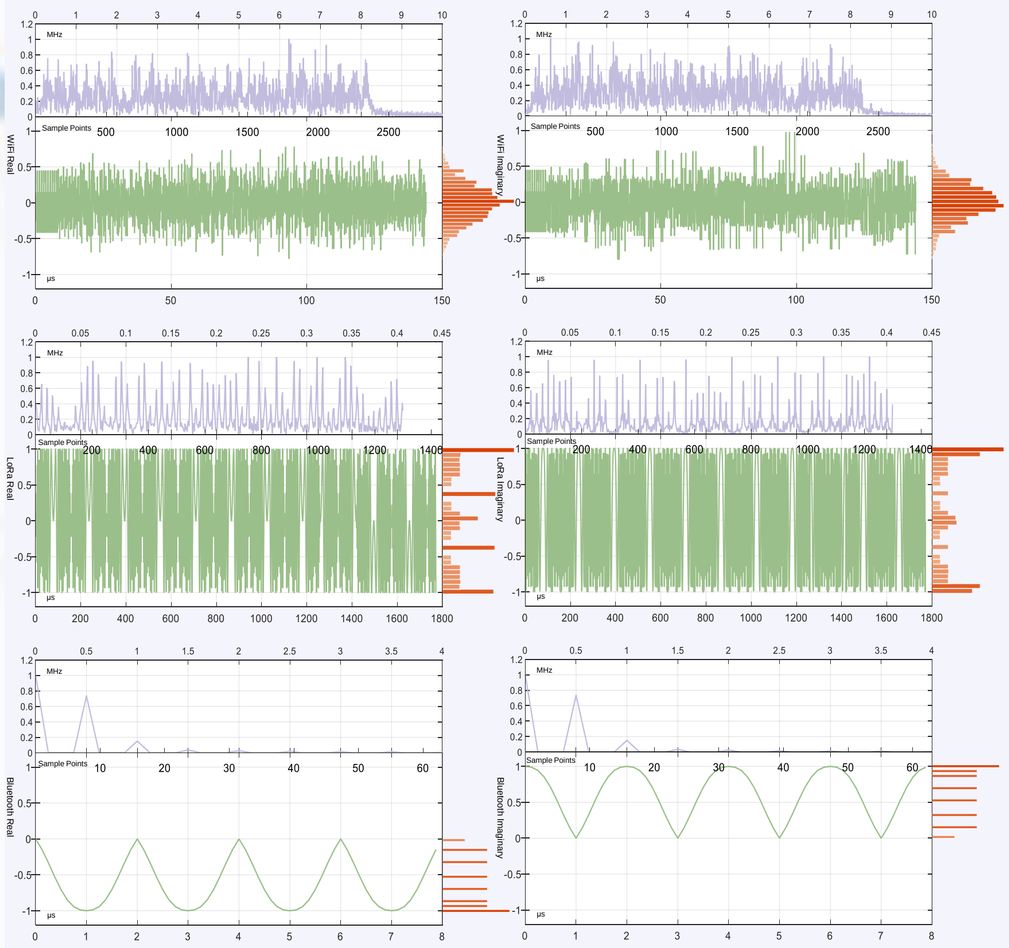
Platform :



The experiment was conducted on a USRP X310 platform, consisting of six USRP X310 devices, with one as the receiver and five as transmitters, forming 10 transmission channels connected via cables.

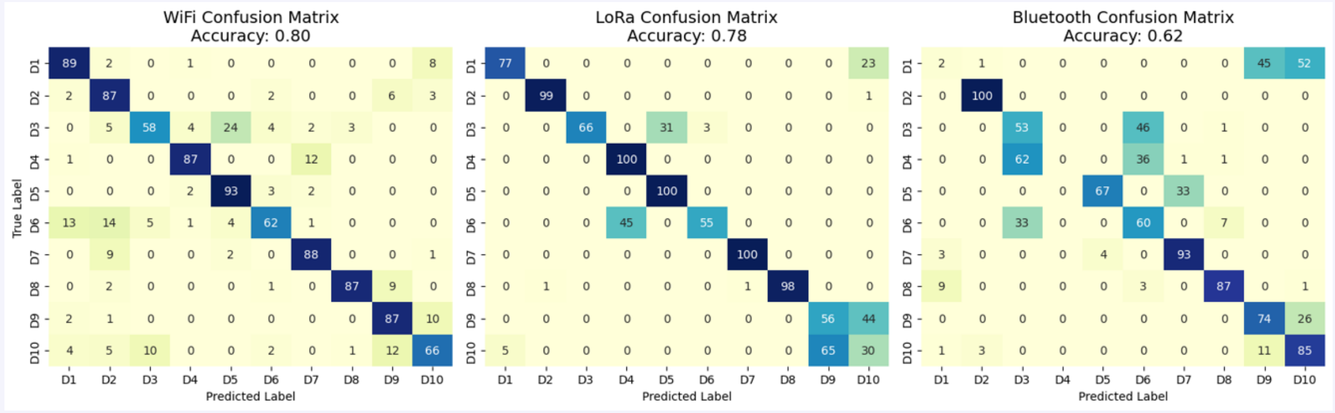


Experiment :



Category	WiFi	LoRa	Bluetooth
Bandwidth	20 MHz	812.5 kHz	1 MHz
Samples per Symbol	80	128	8
Total Samples	7,200	2,450	1,600
Resampling Rate	200 samples/symbol		
Training Samples	200 per device/protocol		
Test Samples	100 per device/protocol		

Results :



- WiFi: Achieved the highest classification accuracy at 80%
- LoRa: Demonstrated strong robustness despite fewer samples, with an accuracy of 78%, comparable to WiFi.
- Bluetooth: Showed lower performance due to its simple preamble structure and limited feature dimensions, with an accuracy of only 62%.

Future work :

- Design signal patterns to highlight hardware fingerprints.
- Develop channel-robust models and data processing techniques.
- Enhance real-time channel awareness and training through edge computing.
- Modify hardware to enhance fingerprint distinguishability.

This research was supported through the UKRI/EPSRC Prosperity Partnership in Secure Wireless Agile Networks (EP/T005572/1).

Communication Systems & Networks Research Group
Merchant Venturers Building, Woodland Road, Bristol, BS8 1TR

@PartnershipSWAN
https://www.swan-partnership.ac.uk/
linkedin.com/company/swan-prosperity-partnership
swan-programme@bristol.ac.uk

Radio Frequency Signal Identification using Machine Learning Techniques (ML for PHY)

Charles Khoury

SECURE WIRELESS AGILE NETWORKS

Introduction and Motivation

Machine learning enhances **RF fingerprinting** by leveraging unique hardware signatures for secure authentication, making it valuable for **keyless entry systems** and wireless security. It also improves **modulation classification** for robust signal recognition. Unlike traditional methods, ML adapts to real-world RF conditions, offering higher accuracy, resilience, and efficiency in dynamic and low-SNR environments.

Continuation on Self Organising Maps

RC2 started with the work on LoRa. The following shows a list of improvements:

- Auto-Splicing, meaning that future capture can automatically translated into datasets
- Direct SOM to Neural Network Pipeline, previously SOMs we saved as images for the datasets
- SOMs for both I and Q data respectively

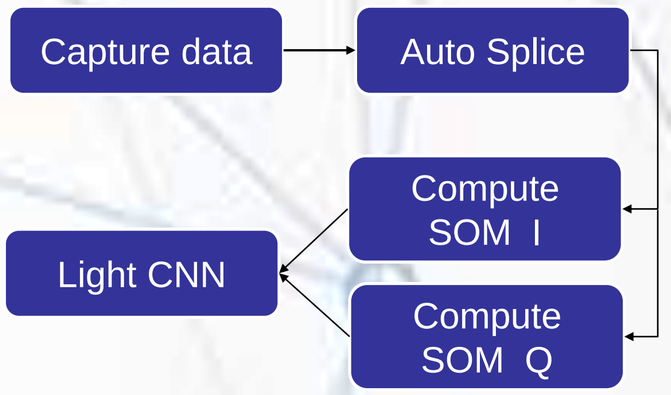


Figure: New SOM Workflow

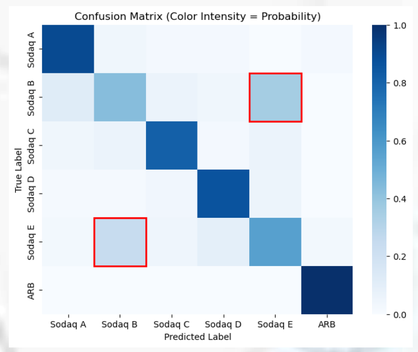


Figure: Confusion Matrix SODAQ and ARB

Complex Valued Neural Network

Complex-Valued Neural Networks (CVNNs) have emerged as a promising field of research in **machine learning for the physical layer (PHY)**, particularly in **RF signal processing**. Unlike traditional real-valued networks, CVNNs natively handle complex-valued signals, preserving **phase and amplitude information** critical for **modulation classification, RF fingerprinting, and channel estimation**.

Introduced for MECOM is a Hybrid Complex Convolutional Recurrent Network based on split LSTM cell. The results show that complex networks are improve on their real counterpart achieving optimality in less epochs.

Research also shows that split architecture offer a compromise between accuracy and implementation compared to natively complex architecture.

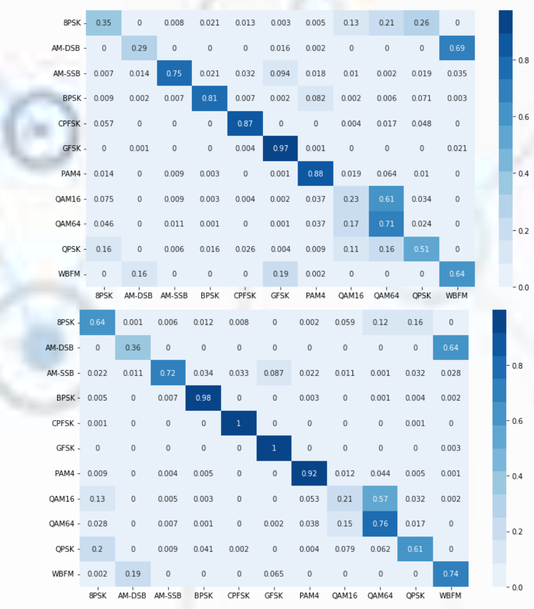


Figure: Confusion Matrix for 0dB SNR (Top) and 18dB SNR (Bottom)

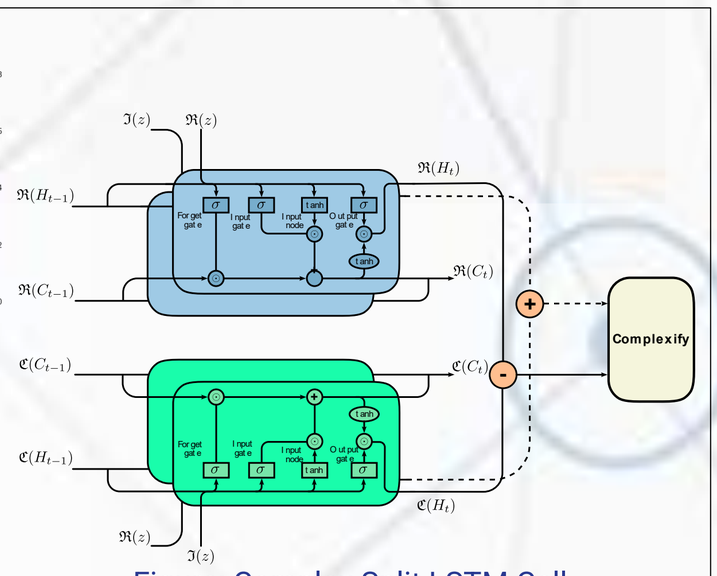


Figure: Complex Split LSTM Cell

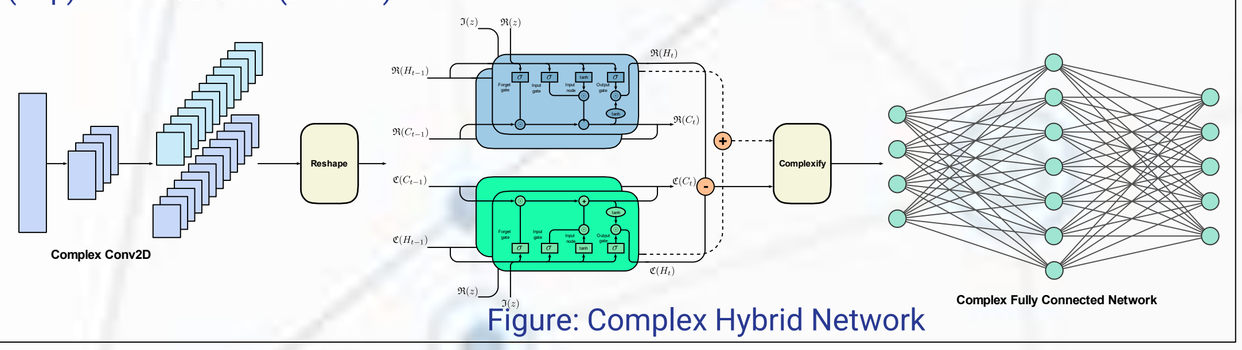


Figure: Complex Hybrid Network

Radio Frequency Fingerprinting

A new dataset is developed to evaluated the accuracy of RF Fingerprinting algorithms. Firstly, data from 4 genuine transmitter is recorder using a Software Defined Radio (SDR). This capture is then replayed using another SDR and the results are recorded.

A novel unsupervised learning is created to address the need for dynamic address fingerprinting. The algorithm is trained on the data captured from the legitimate transmitter.
Then, unsupervised learning is used to distinguished between the legitimate transmitters and the replay attacker.

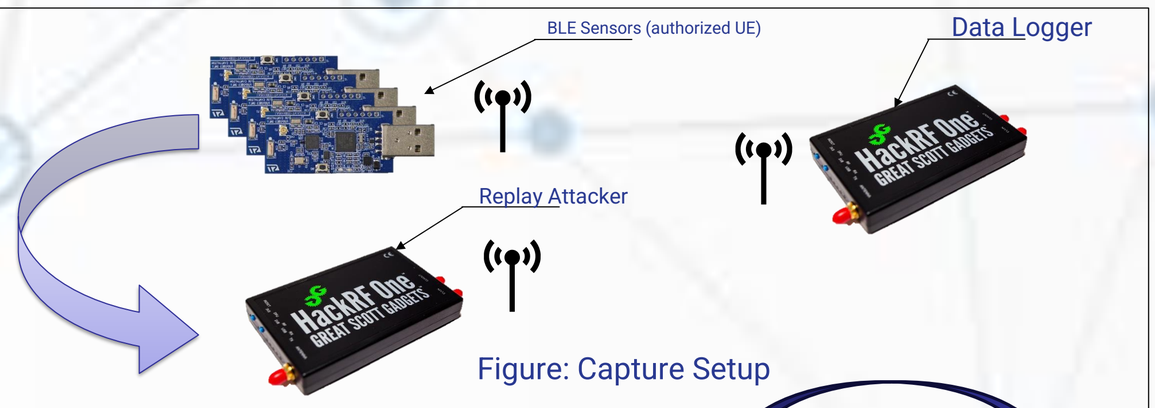
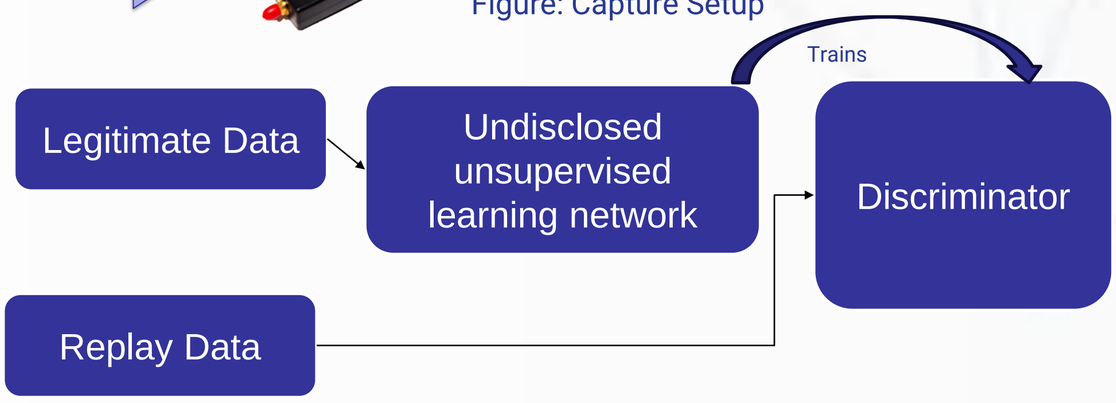


Figure: Capture Setup



This research was supported through the UKRI/EPSRC Prosperity Partnership in Secure Wireless Agile Networks (EP/T005572/1).

Communication Systems & Networks Research Group
Merchant Venturers Building, Woodland Road, Bristol, BS8 1TR

@PartnershipSWAN
https://www.swan-partnership.ac.uk/
linkedin.com/company/swan-prosperity-partnership
swan-programme@bristol.ac.uk

Engineering and Physical Sciences Research Council · TOSHIBA · University of BRISTOL · ROKE · GCHQ

Radio Frequency Signal Identification using Machine Learning Techniques (ML for PHY)

Charles Khoury

SECURE WIRELESS AGILE NETWORKS

Introduction and Motivation

Machine learning enhances **RF fingerprinting** by leveraging unique hardware signatures for secure authentication, making it valuable for **keyless entry systems** and wireless security. It also improves **modulation classification** for robust signal recognition. Unlike traditional methods, ML adapts to real-world RF conditions, offering higher accuracy, resilience, and efficiency in dynamic and low-SNR environments.

Continuation on Self Organising Maps

RC2 started with the work on LoRa. The following shows a list of improvements:

- Auto-Splicing, meaning that future capture can automatically translated into datasets
- Direct SOM to Neural Network Pipeline, previously SOMs we saved as images for the datasets
- SOMs for both I and Q data respectively

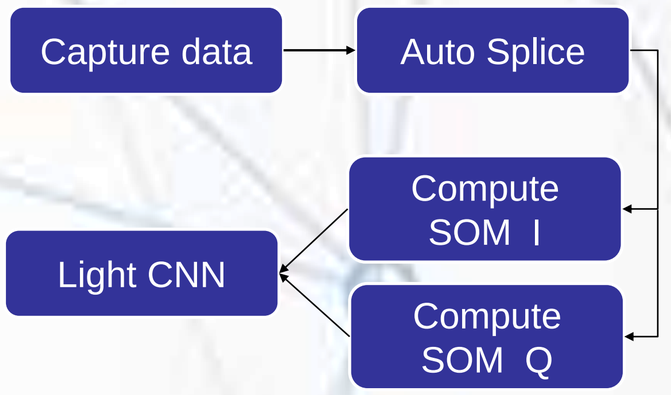


Figure: New SOM Workflow

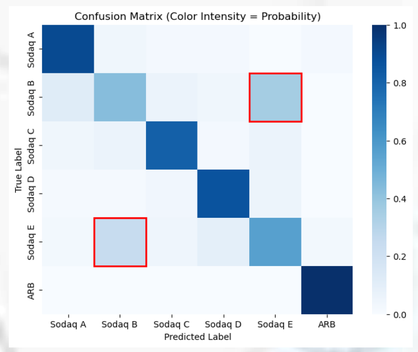


Figure: Confusion Matrix SODAQ and ARB

Complex Valued Neural Network

Complex-Valued Neural Networks (CVNNs) have emerged as a promising field of research in **machine learning for the physical layer (PHY)**, particularly in **RF signal processing**. Unlike traditional real-valued networks, CVNNs natively handle complex-valued signals, preserving **phase and amplitude information** critical for **modulation classification, RF fingerprinting, and channel estimation**.

Introduced for MECOM is a Hybrid Complex Convolutional Recurrent Network based on split LSTM cell. The results show that complex networks are an improvement over their real counterpart achieving optimality in less epochs.

Research also shows that split architectures offer a compromise between accuracy and implementation compared to natively complex architecture.

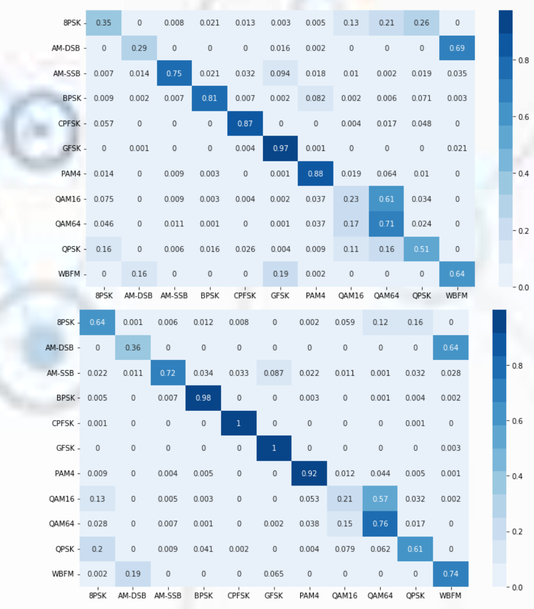


Figure: Confusion Matrix for 0dB SNR (Top) and 18dB SNR (Bottom)

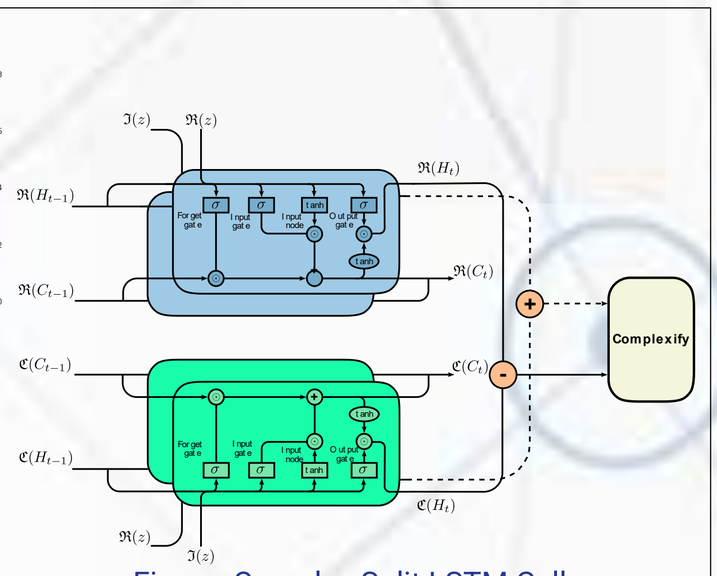


Figure: Complex Split LSTM Cell

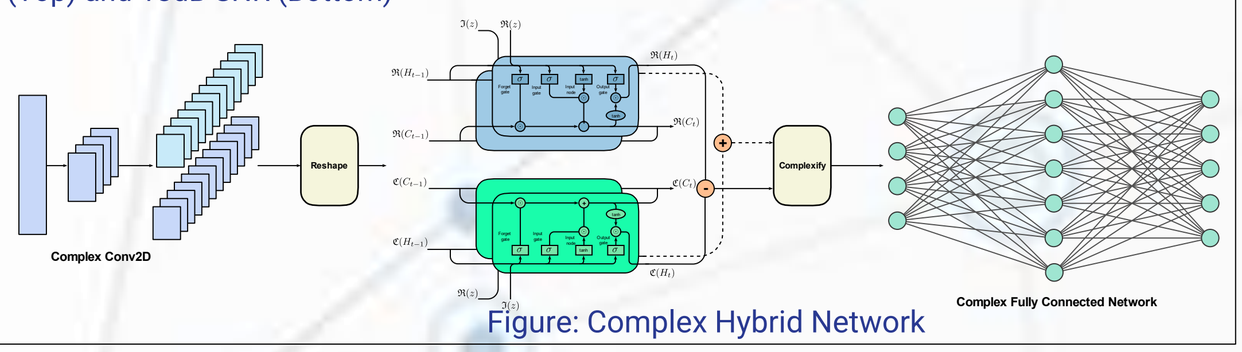


Figure: Complex Hybrid Network

Radio Frequency Fingerprinting

A new dataset is developed to evaluated the accuracy of RF Fingerprinting algorithms. Firstly, data from 4 genuine transmitter is recorded using a Software Defined Radio (SDR). This capture is then replayed using another SDR and the results are recorded.

A novel unsupervised learning is created to address the need for dynamic address fingerprinting. The algorithm is trained on the data captured from the legitimate transmitter.
Then, unsupervised learning is used to distinguished between the legitimate transmitters and the replay attacker.

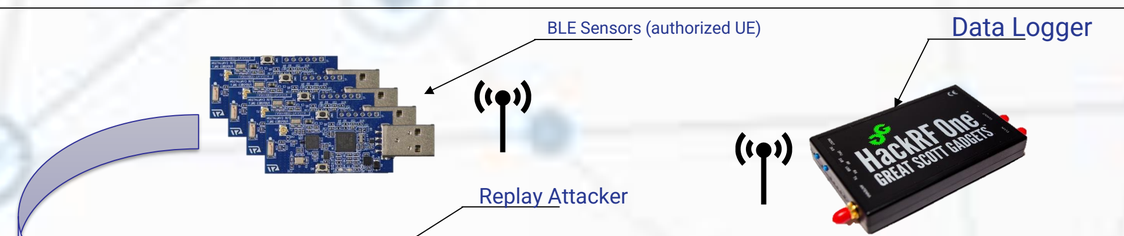


Figure: Capture Setup

This research was supported through the UKRI/EPSRC Prosperity Partnership in Secure Wireless Agile Networks (EP/T005572/1).

Communication Systems & Networks Research Group
Merchant Venturers Building, Woodland Road, Bristol, BS8 1TR

@PartnershipSWAN
https://www.swan-partnership.ac.uk/
linkedin.com/company/swan-prosperity-partnership
swan-programme@bristol.ac.uk

Engineering and Physical Sciences Research Council · TOSHIBA · University of BRISTOL · ROKE · GCHQ

SECURE WIRELESS AGILE NETWORKS

RF STRIDE

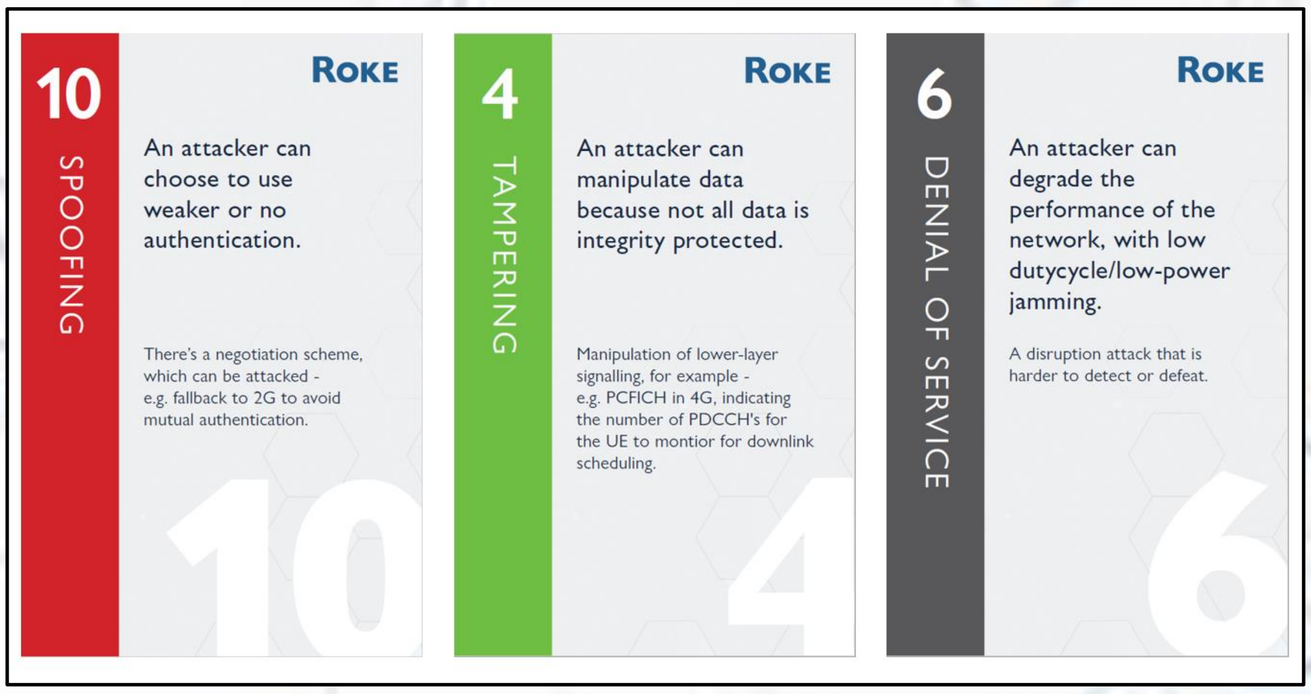
Stephen Wales (Roke), Mark West (Roke

- Describes a set of generic threats and examples
- Applied to compute systems and networks
  - Adopted by Microsoft in 2002
  - Popularised through a set of playing cards

	Threat	Property Violated	Threat Definition
S	Spoofing identity	Authentication	Pretending to be something or someone other than yourself
T	Tampering with data	Integrity	Modifying something on disk, network, memory, or elsewhere
R	Repudiation	Non-repudiation	Claiming that you didn't do something or were not responsible; can be honest or false
I	Information disclosure	Confidentiality	Providing information to someone not authorised to access it
D	Denial of service	Availability	Exhausting resources needed to provide service
E	Elevation of privilege	Authorisation	Allowing someone to do something they are not authorised to do

SWAN has taken the STRIDE Framework and applied to RF Cyber

- A set of playing cards developed
  - Each Suit corresponds to a type of threat
  - The Number represents severity



	Threat	Property Violated	RF Example
S	Spoofing identity	Authentication	Base Station or Access Point appearing as legitimate device
T	Tampering with data	Integrity	Man in the Middle Attack – receiving and manipulating signal or its contents before re-transmitting
R	Repudiation	Non-repudiation	Rogue device not responding correctly to wireless protocols
I	Information disclosure	Confidentiality	In Wireless Systems more commonly known as Eavesdropping – listening and decoding information
D	Denial of service	Availability	In Wireless Systems more commonly known as Jamming, which can be unsophisticated, but can extend to exhaust resources through flooding of control messages
E	Elevation of privilege	Authorisation	In computer systems an example is gaining admin rights. There is a weaker relevance to wireless systems, but loading malware onto devices is an example

This research was funded by Roke Manor Research Ltd as part of the UKRI/EPSRC Prosperity Partnership in Secure Wireless Agile Networks (EP/T005572/1).
© Roke Manor Research Ltd

Communication Systems & Networks Research Group
Merchant Venturers Building, Woodland Road, Bristol, BS8 1TR

@PartnershipSWAN
https://www.swan-partnership.ac.uk/
linkedin.com/company/swan-prosperity-partnership
swan-programme@bristol.ac.uk

Engineering and Physical Sciences Research Council
TOSHIBA
University of BRISTOL
ROKE
GCHQ

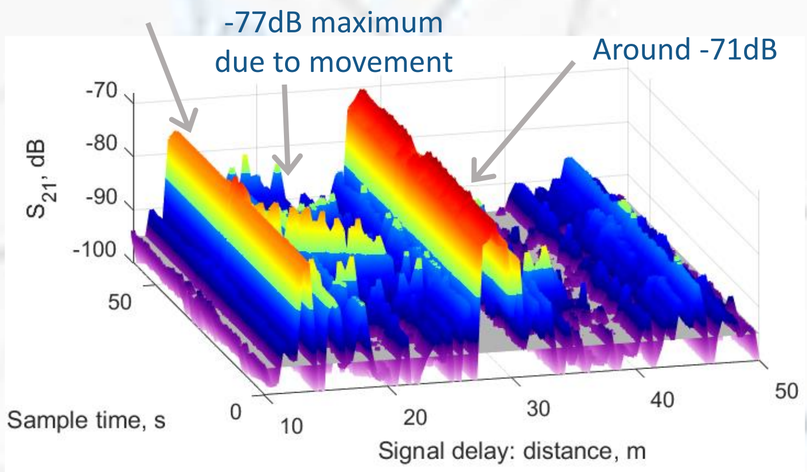
STAR – Simultaneous Transmit and Receive

Stephen Wales (Roke,) Geoffrey Hilton (UoB), Mark Beach (UoB)

- Collaborative work between University of Bristol and Roke
- Focus has been achieving high depths of cancellation over wide bandwidths
- UoB has developed analogue cancellation techniques
- Roke has developed digital cancellation techniques
- Brought together in a number of demonstrations

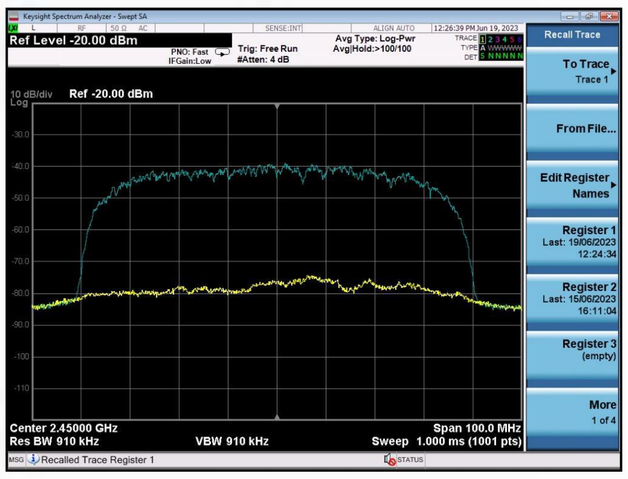
- Analogue Canceller: 4 tap analogue delay line with cable delays
- Channel Characterisation Measurements
  - Determine best tap delays
  - Develop algorithm for setting amplitude/phase weights

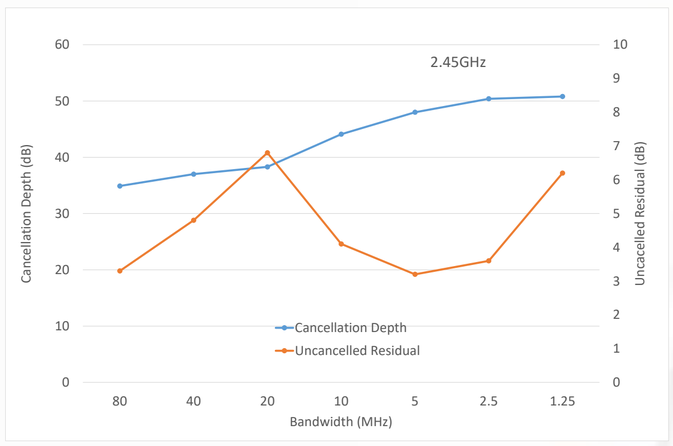
Usually -76dB rising to -74dB when close proximity



- Digital Canceller implemented on FPGA of Ettus X310 SDR
  - Multi-tap canceller operating at 100Msamples/s

Digital Canceller Performance



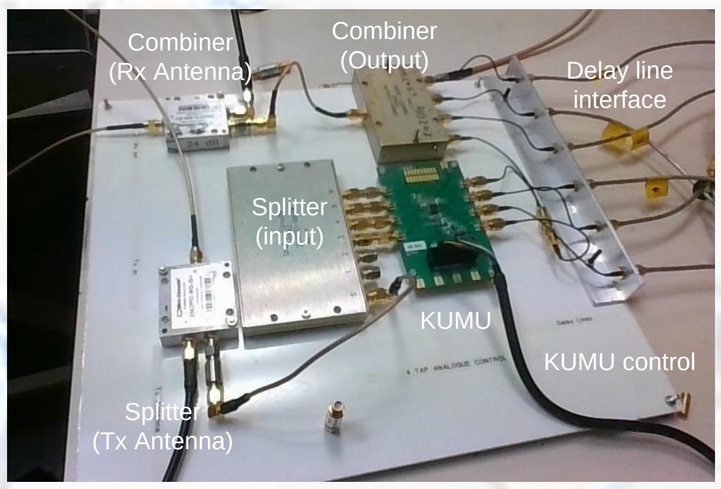


Performance in Context

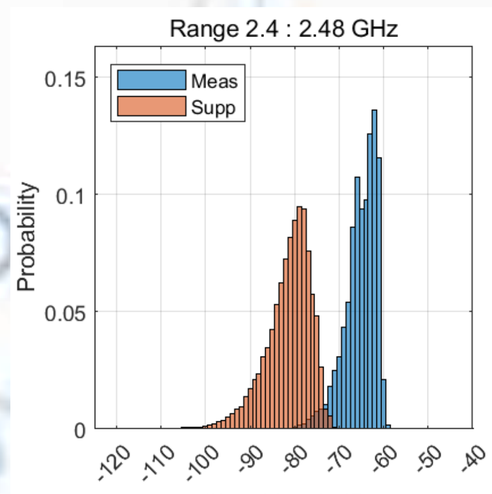
- Figure of Merit in dBm-MHz due to Kolodziej
  - System Isolation: ISO – 102dB
  - Receiver Sensitivity Degradation: RSD
  - Bandwidth (MHz): BW – 80MHz
  - Transmit Power (mW): PTX – 30dBm
- FOM= (ISO/RSD)xBWxPTX
- FOM: 138.5 dBm-MHz

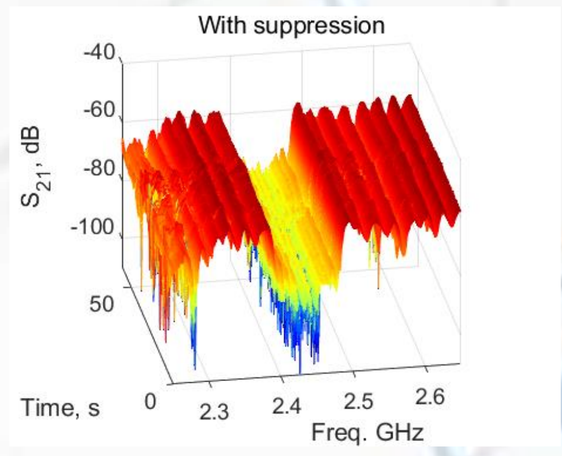
K. E. Kolodziej, "In-Band Full-Duplex Wireless Systems Overview," *ICC 2021 - IEEE International Conference on Communications*, Montreal, QC, Canada, 2021, pp. 1-6, doi: 10.1109/ICC42927.2021.9500649

Analogue Canceller



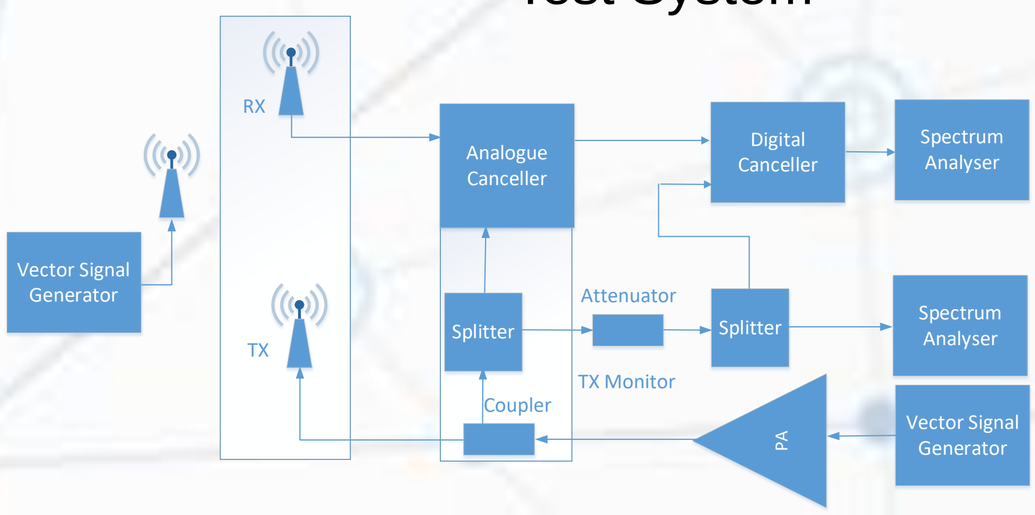
Analogue Canceller Performance

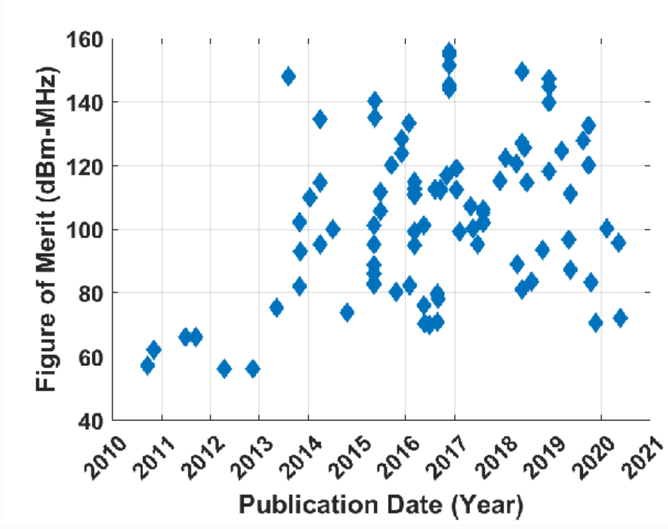




- Analogue Canceller Required to Reduce Self-Interference to within Dynamic Range of SDR

Test System





This research was funded by Dstl under the EW and Cyber Framework
© Roke Manor Research

Communication Systems & Networks Research Group
Merchant Venturers Building, Woodland Road, Bristol, BS8 1TR

@PartnershipSWAN
https://www.swan-partnership.ac.uk/
linkedin.com/company/swan-prosperity-partnership
swan-programme@bristol.ac.uk

Reconfigurable Microwave Filter for Tunable Transceiver

Ruipeng Zhang (MSc student), Jiteng Ma, Hao Li, Sean Gu, Gavin Watkins, Andrew Austin, and Shuping Dang (A conference paper from this work has been submitted to 2025 IEEE Wireless Power Technology Conference and Expo)

Introduction:

As the demand for wireless connectivity continues to grow, radio spectrum resources are becoming increasingly crowded, making efficient and secure communications a top priority. As a key component in modern wireless communication systems, tunable filters play an important role in enabling dynamic spectrum access and enhancing communication security. The proposed design enables a tunable frequency range (1.44-2.7 GHz), adjustable bandwidth (110-400 MHz) and the measured insertion loss is 4.1-7.2 dB, which can enable a wider tuning range and improving spectrum utilization. This enables a tunable transceiver that suppresses interference and achieves spectrum agility and will greatly improve the security of wireless systems.

Motivation:

- Spectrum resources are becoming increasingly crowded, and fixed frequencies cannot meet with dynamic spectrum environments.
- Fixed frequency communications are difficult to resist certain interference and attacks.
- The development of cognitive radio requires spectrum sensing and dynamic spectrum access.

Resonator Analysis:

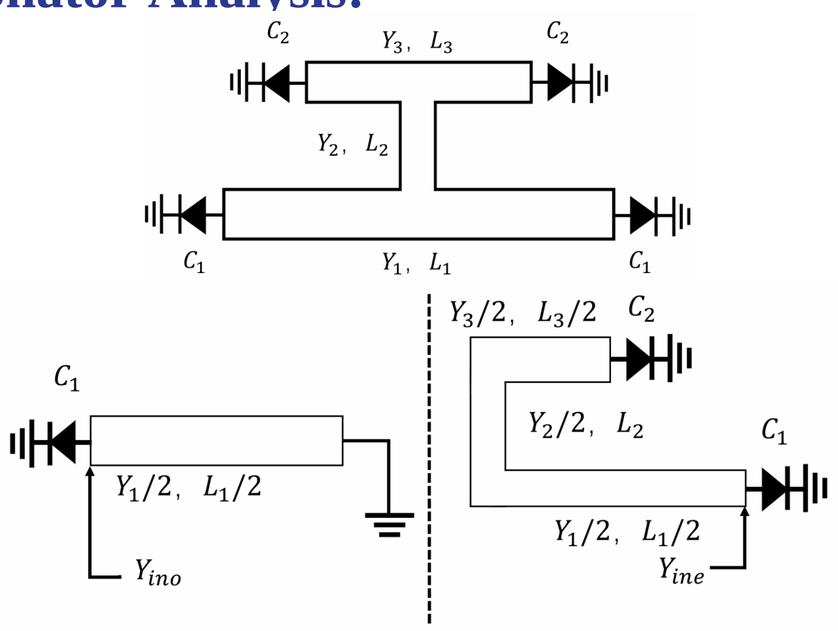


Figure 1 Structure of the proposed T-shape resonator and the Odd/Even mode.

According to the symmetrical structure of the resonator, we can analyze the structure by Odd-even mode analysis in Fig.1:

$$\frac{Y_1}{2\pi C_1} = f_{odd} \tan\left(\frac{2\pi f_{odd} L_1}{v_p}\right), \quad (1)$$

$$f_{even} = \frac{Y_1}{2\pi C_1} \frac{Y_r + Y_s \tan\left(\frac{2\pi f_{odd} L_1}{v_p}\right)}{Y_s - Y_r \tan\left(\frac{2\pi f_{odd} L_1}{v_p}\right)}, \quad (2)$$

where

$$Y_r = Y_2 Y_3 (w_{even} C_2 + Y_3 \tan(\beta L_3)) + \frac{Y_r^2}{2} \tan(\beta L_2)\,(Y_3 - w_{even} C_2 \tan(\beta L_3)), \quad (3)$$

$$Y_s = Y_1 \tan(\beta L_1)\, Y_2 (Y_3 - w_{even} \tan(\beta L_3)), \quad (4)$$

There are two resonance points in this structure, which are controlled by capacitors C_1 and C_2 respectively, as shown in Fig. 2. Therefore, it is necessary to adjust the values of C_1 and C_2 at the same time.

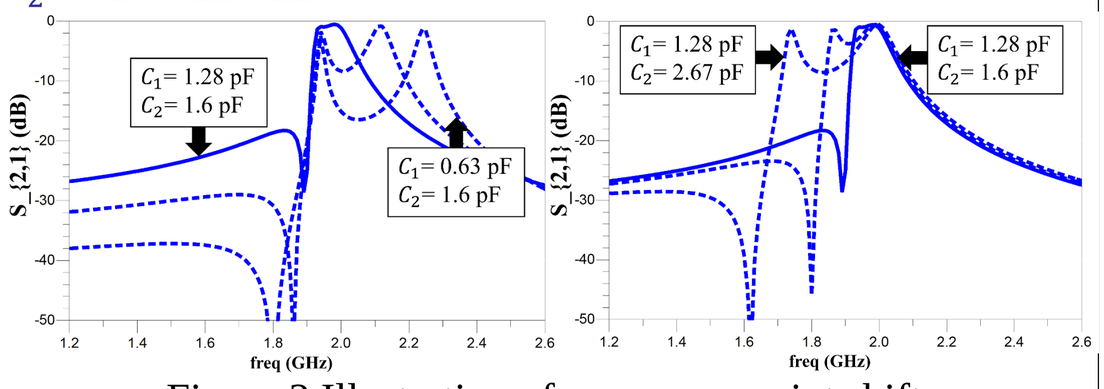


Figure 2 Illustration of resonance point shift.

Results:

Figure 3 EM simulation (S21 and S11).

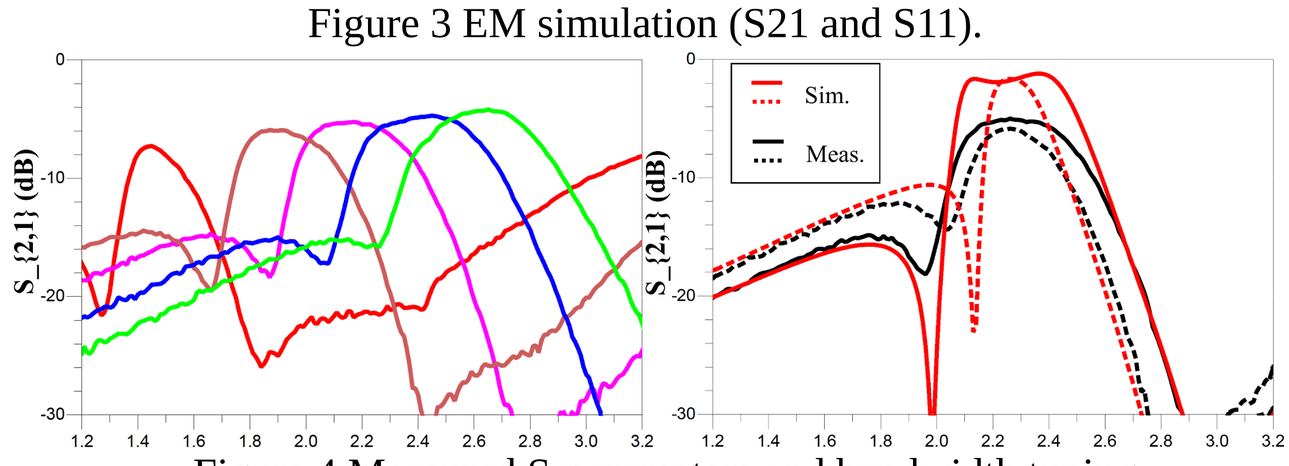


Figure 4 Measured S-parameters and bandwidth tuning.

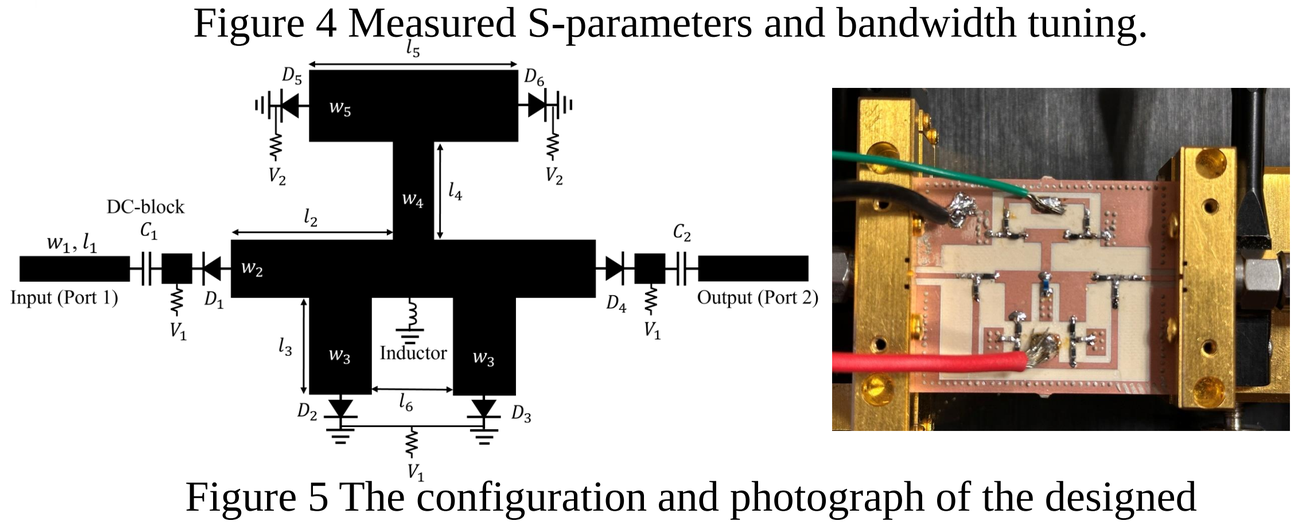


Figure 5 The configuration and photograph of the designed fabrication (39.3 x 28.7 mm)

By adjusting the bias voltages V1 and V2 of the diodes, the bandwidth and the centre frequency of the filter can be changed.

In EM simulations, the adjustment range of the center frequency is 1.6–2.7 GHz and 3-dB bandwidth can be tuned within 110–400 MHz. The measured center frequency can be adjusted within 1.44–2.7 GHz. The EM simulation insertion is 1.2-2.5 dB, and the measured insertion loss is 4.1-7.2 dB.

Conclusion and future work:

- The designed filter provides enhanced frequency and bandwidth flexibility through the dual resonance points of the T-shaped resonator, thereby improving the security of wireless systems .
- The discrepancy between the EM simulations and the measured results may be attributed to limitations in machining accuracy or in accuracies in the SPICE models of certain components, which is worth further investigating and mitigating.
- Machine learning may be employed to train the system, enabling it to rapidly adjust to the desired operating frequency and bandwidth, thereby minimizing energy loss.

This research was supported through the UKRI/EPSRC Prosperity Partnership in Secure Wireless Agile Networks (EP/T005572/1).

Communication Systems & Networks Research Group
Merchant Venturers Building, Woodland Road, Bristol, BS8 1TR

@PartnershipSWAN
https://www.swan-partnership.ac.uk/
linkedin.com/company/swan-prosperity-partnership
swan-programme@bristol.ac.uk

Covert Communication through Orthogonal Polarisation using Composite Antennas

SECURE WIRELESS AGILE NETWORKS

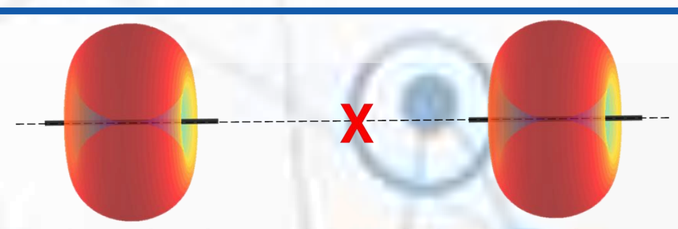
PhD Scholar - Sanchita Kayal
Supervisor - Dr. Geoffrey Hilton, Prof. Mark Beach

Main Aim :

Investigation of RF mechanisms for covert communication, enabling transmission through selective time-polarisation while embedding within innocuous RF signals.

Leveraging two key concepts;

- Physics of **Polarisation Diversity.**
- Embedding secret data through modulation – **Watermarking.**



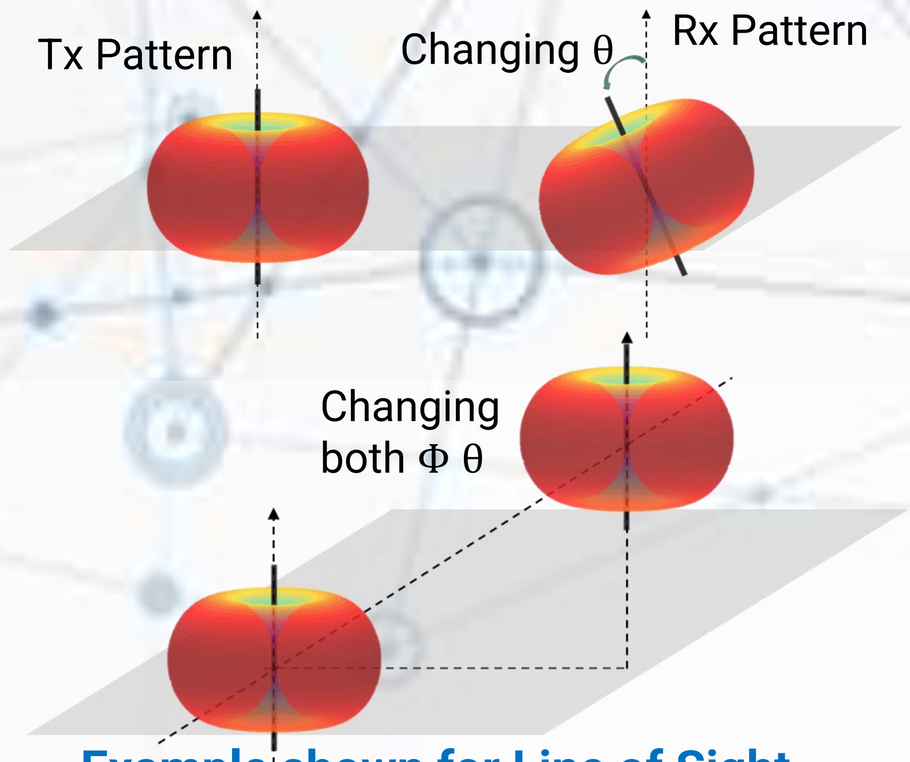
Transmitter is Invisible to the receiver

- This the key idea of this work towards secured communication posing in the physical layer channel.
- Data reception is only possible, when both the channels are available to pick up.

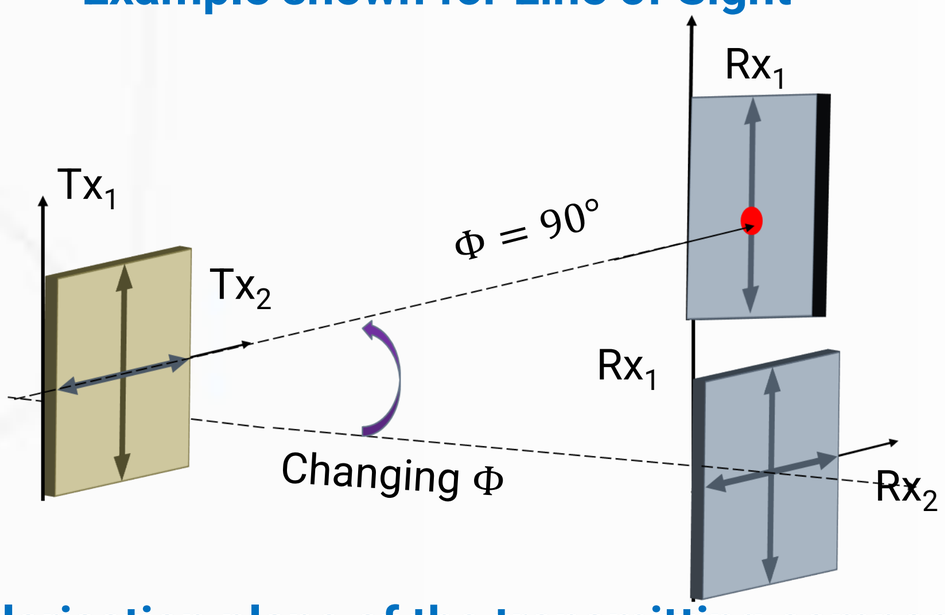
Theoretical Background (Polarisation Diversity) :

- Polarisation mismatch arises from

1. **the tilt angle** in between Transmitting and the receiving antennas
2. **relative position; antennas are** at different planes



Example shown for Line of Sight



Polarisation plane of the transmitting composite antennas w.r.t. Receiving one

- Single pair of Transmitting and receiving antenna shows polarisation mismatch loss as;

$$Polarisation\ Loss\ Factor = Cos^2\theta$$

- Composite antennas will make the scenario more complicated; hence critical to get aligned with both polarization simultaneously.
- Only a particular direction with a limited angle span will facilitate the proper alignment.

Methodology :

- Deploying **RF Composite Channel** for simultaneous independent data transmission.
- The fundamental modulation scheme for both channels will be Quadrature Phase Shift Keying (QPSK).
- One channel will serve as a **reference signal** for the intended receiver, carrying general data as **a decoy for potential eavesdroppers**.
- While other hiding secret data- **manipulating reference baseband** symbols.
- The concealment hinges on the phase difference and amplitude of the two individual signals.
- **Composite channels** are not viable from all angles/ positions.
- Thus, secured data retrieval is associated with three main operations.

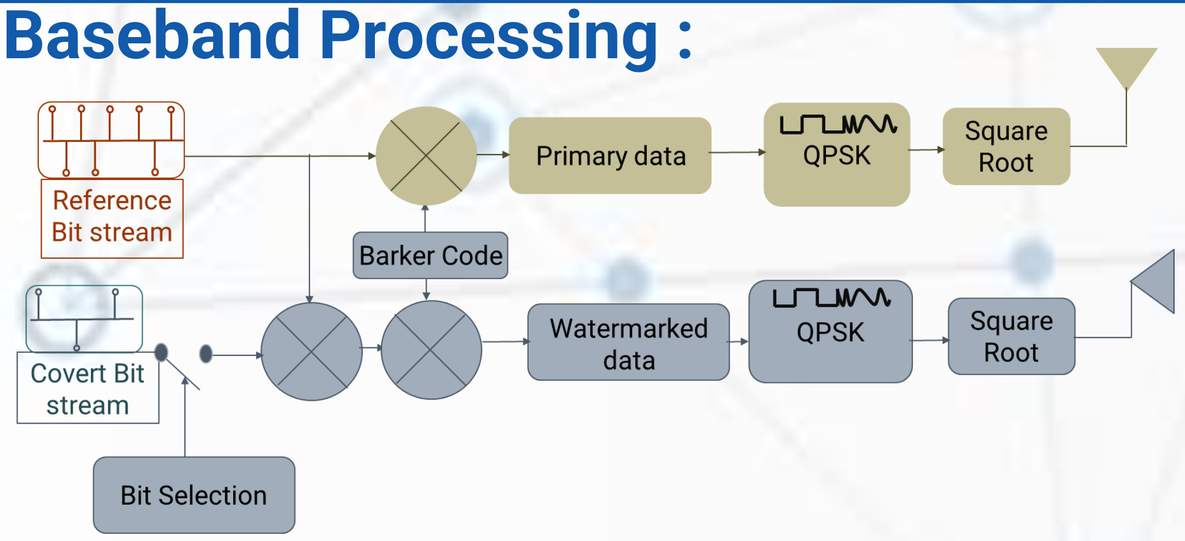
1. Receiver must be aware of dual channel transmission.
2. It should receive composite channels with precise polarization alignment.
3. Receiver should posses the knowledge of post-reception bit processing scheme.

Secured communication lies in;

Anti-Reception: Concealing the communication channel itself.

Anti-Detection: Watermarking the secret data to avoid detection.

Baseband Processing :



Future Work :

- Measurements will be undertaken in the anechoic chamber; analysis will be applied in further processing.
- It will then focus on **multipath environments.**
- **This implications in multipath scenarios will become more complicated.**

This research was supported through the UKRI/EPSRC Prosperity Partnership in Secure Wireless Agile Networks (EP/T005572/1).

Communication Systems & Networks Research Group
Merchant Venturers Building, Woodland Road, Bristol, BS8 1TR

@PartnershipSWAN
https://www.swan-partnership.ac.uk/
linkedin.com/company/swan-prosperity-partnership
swan-programme@bristol.ac.uk

Engineering and Physical Sciences Research Council · TOSHIBA · University of BRISTOL · ROKE · GCHQ

Resilient receivers: Waveform cancellation and Linearisation for High Dynamic Range front-end

Francesco Raimondo (UoB), Steve Wales (Roke), Mark Beach (UoB)

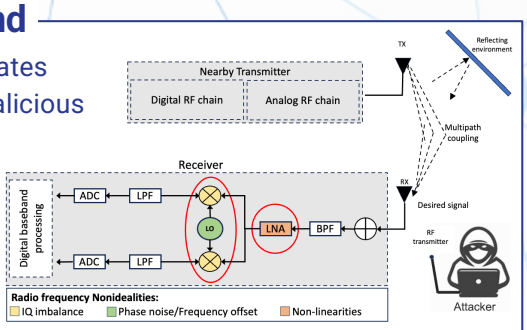
SECURE WIRELESS AGILE NETWORKS

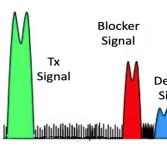
Summary

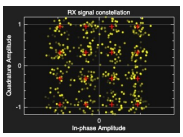
Resilient receivers leveraging analogue waveform cancellation and digital linearization are pivotal for enhancing the performance of high-dynamic range (HDR) front-end systems. These techniques mitigate distortion, improve signal integrity, and extend the receiver's operational range. By combining analogue waveform cancellation with digital linearization, this approach effectively addresses non-linearities, ensuring robust reception in complex, high-interference environments, and optimizing overall system efficiency.

Motivation and Background

- The increasing complexity of modern communication systems necessitates receivers capable of handling high-dynamic range, in the presence of malicious or unwanted interference.
- Receivers that can maintain high signal fidelity are crucial for wireless communications, military radar, and medical imaging.
- Waveform cancellation and digital linearization can process weak signals amidst stronger, interfering signals while preserving accuracy and reliability.
- The trend toward integrating entire receiver architectures onto a single system-on-chip (SoC) offers advantages in power efficiency, size, and cost.



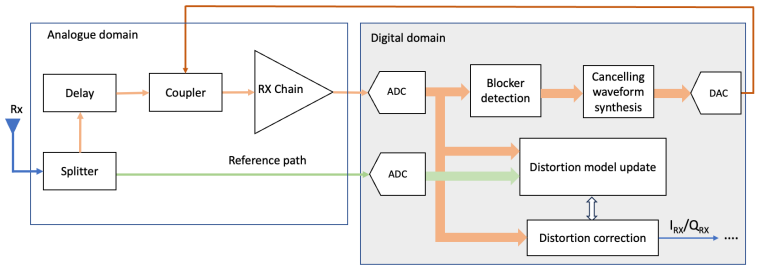


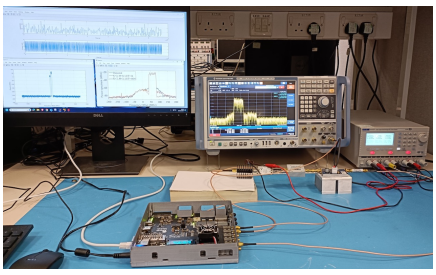


IQ constellation degradation

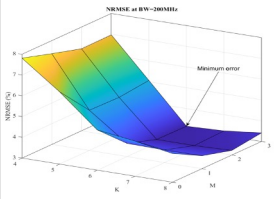
Methodology and Results

- The system isolates blockers and generates a cancellation signal merging it with the input signal to reduce blocker levels.
- The digital domain handles blocker detection, synthesis, and distortion correction.
- The complexity is shared among the CPU performing model parameter computations and the FPGA executing real-time operations.
- Polynomial models are evaluated for nonlinearity, balancing computational load, energy efficiency and FPGA resources.

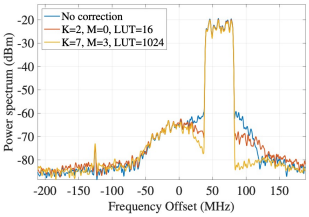




Setup including FPGA board and Analogue RF chain



Model parameters search



Distorted and the corrected signal

Conclusions and Future work

- The integration of analogue waveform cancellation and digital linearization within an RF system-on-chip shows potential in improving receiver performance in high-interference environments.
- Future work focus on further developing adaptive filtering algorithms for quicker responses, optimizing for real-time performance with minimal latency, and expanding the RF-SoC to support multi-channel.

References

[1] Marttila et Al. Reference receiver enhanced digital linearization of wideband direct-conversion receivers.

[2] Peng et Al. Design and implementation of software-defined radio receiver based on blind nonlinear system identification.

[3] Morgan et Al. A generalized memory polynomial model for digital predistortion of rf power amplifiers.

This research was supported through the UKRI/EPSRC Prosperity Partnership in Secure Wireless Agile Networks (EP/T005572/1).

Communication Systems & Networks Research Group
Merchant Venturers Building, Woodland Road, Bristol, BS8 1TR

@PartnershipSWAN
https://www.swan-partnership.ac.uk/
linkedin.com/company/swan-prosperity-partnership
swan-programme@bristol.ac.uk

Engineering and Physical Sciences Research Council
TOSHIBA
University of BRISTOL
ROKE
GCHQ

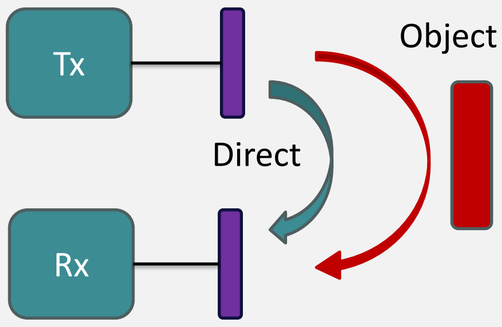
Sensing the Local RF Environment

Geoff Hilton, Andrew Austin & Mark Beach

SECURE WIRELESS AGILE NETWORKS

This research has been developed to help support a number of collaborative projects between the University of Bristol and Roke Manor Research.

1. Introduction



The ability to sense both fixed and dynamic changes in the RF characteristics of the environment that are local to the transmitter and/or receiver is key to optimising communications systems. Furthermore, there is a push towards developing combined sensing and communications platforms.

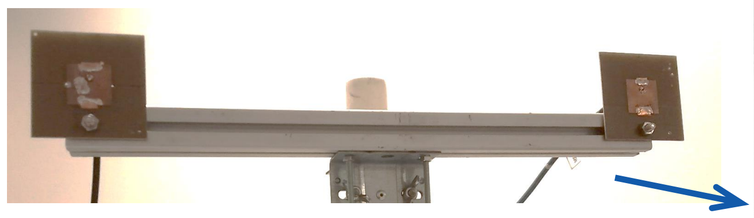
Wideband sensing can be used to accurately determine the location of close-proximity scatters within a constantly changing local environment, but the bandwidth that is available will be limited to the operating band of the communications systems (i.e. 80MHz for the 2.4GHz ISM band). The range resolution, which is a function of the operating frequency bandwidth, is therefore impacted by this.

Here, the experimental development of a sensing system that (most importantly) operates within the bandwidth of the communications system, but with the range resolution close to that of a system operating with around 10 times the bandwidth, is described.

Examples of indoor and outdoor environments with mobile and fixed platforms are presented with comparisons shown for both wideband operation and the 80MHz operation around 2.4GHz.

2. Antenna configurations and environments

- Two different antenna configurations
- Two different outdoor environments and one indoor environment
- Static and moving vehicle-based measurements

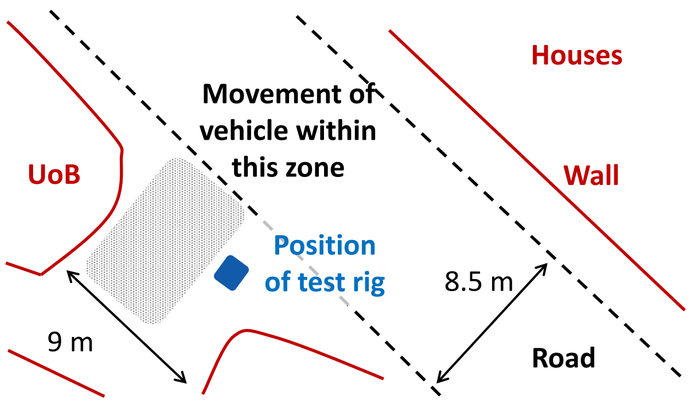


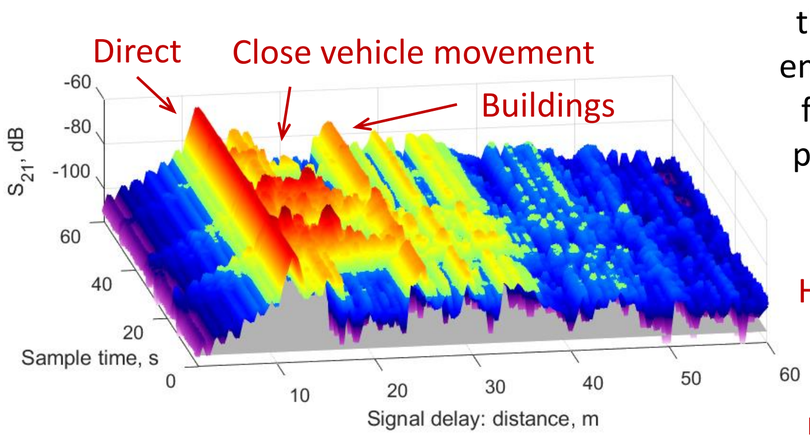
Directional Antennas located 40cm apart for measurements shown on the right

Indoor Laboratory

3. Monitoring vehicle movement

This antenna configuration comprised a directional transmit antenna and monopole receive antenna placed 1.2m apart on the test rig connected to a Vector Network Analyser (VNA)





Coupling in the frequency domain between transmitter and receiver are monitored over time to determine the direct antenna path, local 'fixed' multipath and local movement.

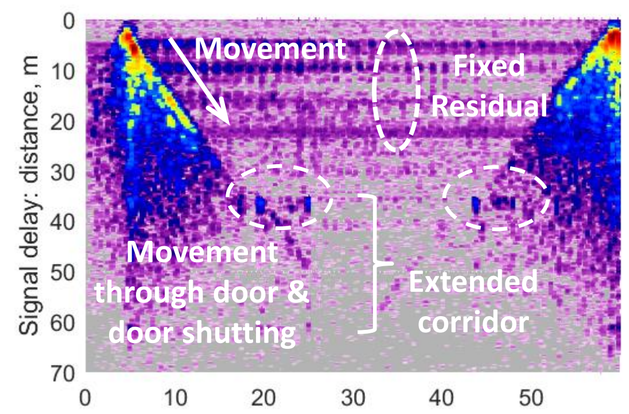
The vehicle movement in the zone by the car park entrance is monitored and frequency-domain data processed (shown as the signal delay distance)

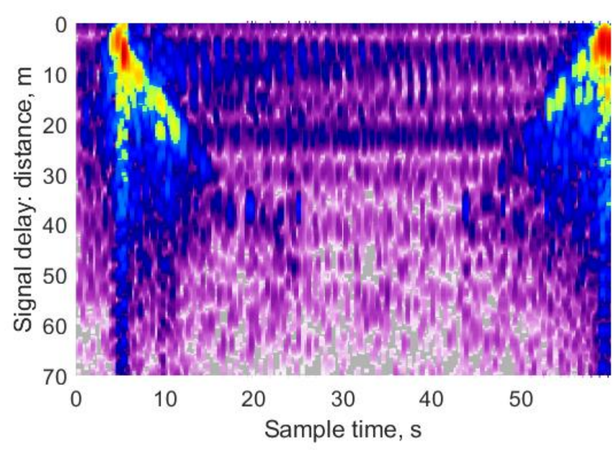
However, low-level details are masked by the high direct coupling and the mathematical processing

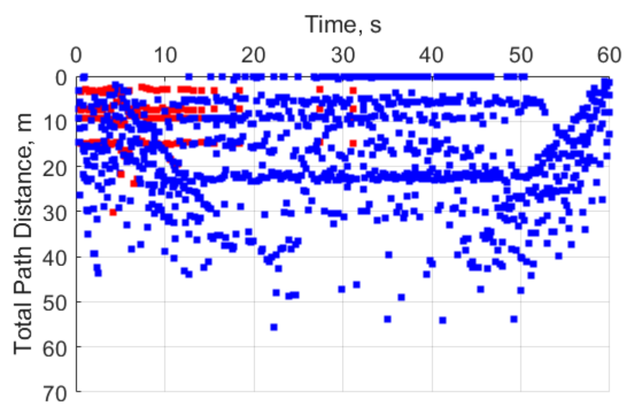
4. Cluttered indoor environment (static antennas)

- Indoor environment and two directional antennas (Tx power of 10dBm)
- Movement from and towards the antennas (including far-end corridor)
- Total delay shown (twice object distance)

This algorithm is processing frame-by-frame variations to monitor the local environment







Wideband operation:
- Most of fixed coupling between Tx and Rx now removed, though some very low-level residual still present
- 16.5m to door (plus cabling) & corridor beyond
- Resolution of 0.38m

Operation with reduced bandwidth

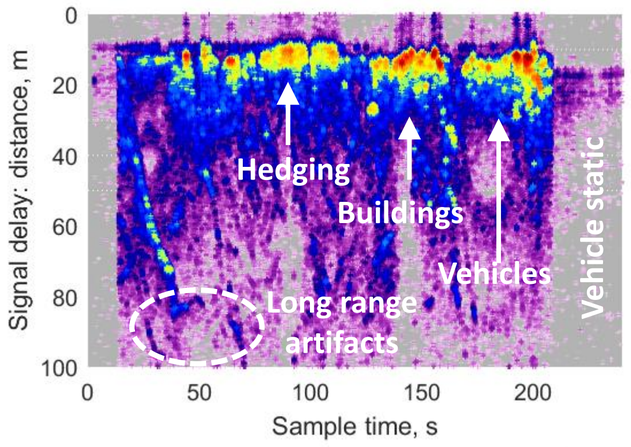
Sampled for only the 80MHz ISM band:
- Resolution now 3.8m
- More difficulty in identifying movement at longer distance

RF data processing to improve resolution with the reduced bandwidth

- Key features resolved to around 0.2m in 30m range
- 'Fixed residual' masking some details but improved earlier processing will remove this

File: dmeas4

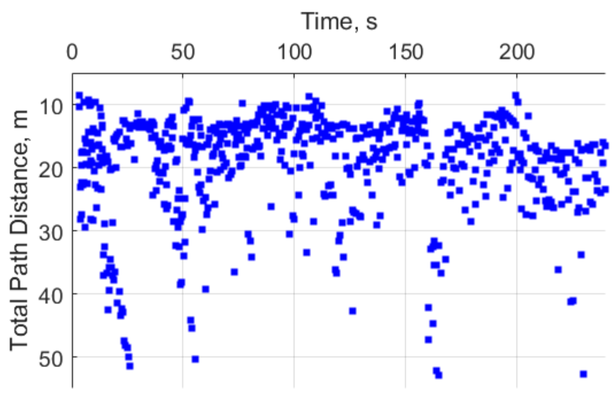
5. Moving vehicle-based outdoor measurements



Wideband response:
- Most obstacles within 10m of moving vehicle
- Longer range visible (~50m distance) when no local clutter
- Fixed residual levels visible with vehicle static

File: rmeas3

80MHz processed data:
- Key propagation features identifiable to around 0.2m
- Can now apply image processing techniques to improve the visualisation quality of the data



6. Conclusions

- Can identify fixed environment features and movements within the environment to at least 30m range with only 10dBm power level
- Reduced bandwidth processing is used to identify propagation paths within field of view of the Tx and Rx antennas
- Further RF and image processing will remove 'spurious' clutter
- Current work uses a VNA and future work will be developed on RFSoC technology making the system more compact and versatile.

This research was supported through the UKRI/EPSRC Prosperity Partnership in Secure Wireless Agile Networks (EP/T005572/1).

Communication Systems & Networks Research Group
Merchant Venturers Building, Woodland Road, Bristol, BS8 1TR

@PartnershipSWAN

https://www.swan-partnership.ac.uk/

swan-programme@bristol.ac.uk

Engineering and Physical Sciences Research Council · TOSHIBA · University of BRISTOL · ROKE · GCHQ

SECURE WIRELESS AGILE NETWORKS

Magnus Sandell, SWAN Business Lead

Factory IoT

- Manufacturing IoT data collection and utilisation
- The connected factory
- Sensitive to delays and interruptions
- Needs to be protected on all communication layers

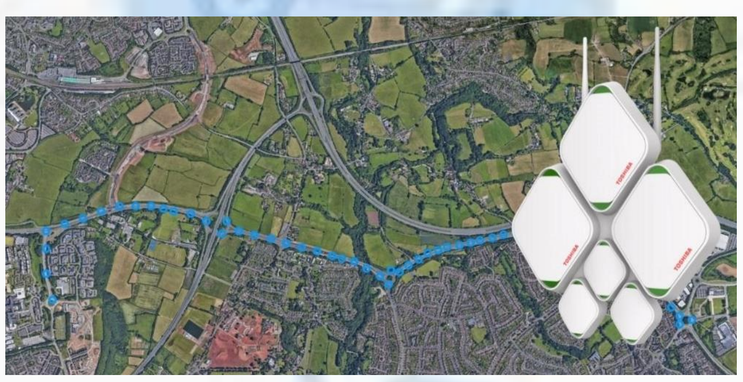
- **Benefits from SWAN:**
  - Spoofing and jamming

Autonomous Warehouses

- Reduced time spent looking for goods
- Reduced risk of injuries and fatigue of workers
- Optimised shelf position and route selection
- IoT network needs to be protected

- **Benefits from SWAN:**
  - RF fingerprinting and authentication

Wireless Sensor Networks



- UMBRELLA is one of the largest, world-leading open programmable Industrial Internet of Things (IIoT) networks covering parts of South Gloucestershire.
- A unique platform which connects several testbeds, bridging the gap between the physical and laboratory worlds, and evolving ideas past the boundaries of the lab and closer to market.
- But as an open platform, its wireless interface is susceptible to interference (intentional or otherwise)

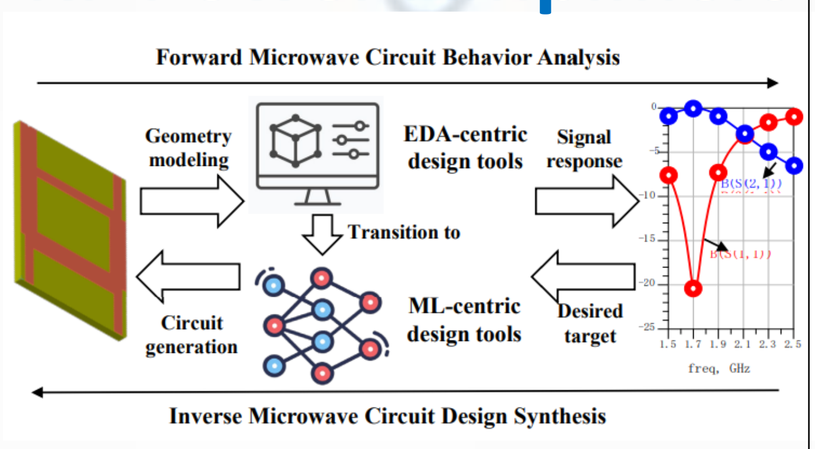
- **Benefits from SWAN:**
  - Intrusion detection and fidelity

Autonomous Hunting Drone

- A drone which autonomously captures target drones with its net guns
- Eliminates dangerous drones physically, safely towing them to a safe location
- Need to be robust against attacks on its control signals and sensors
- The Physical Layer communication needs to be protected

- **Benefits from SWAN:**
  - Jamming detection and avoidance

RF Power Amplifiers



- Novel Digital Power Amplifier architecture under development
  1. Characteristics can be "tuned" to frequency bands of interest
  2. Offers improved frequency agility
  3. Maintains energy efficiency

- Researching techniques to enhance resilience of RF frontends (receivers) against intentional and nonintentional jamming

- **Benefits from SWAN** :
  - RF agility for spectrum management

This research was supported through the UKRI/EPSRC Prosperity Partnership in Secure Wireless Agile Networks (EP/T005572/1).

Communication Systems & Networks Research Group
Merchant Venturers Building, Woodland Road, Bristol, BS8 1TR

@PartnershipSWAN
https://www.swan-partnership.ac.uk/
linkedin.com/company/swan-prosperity-partnership
swan-programme@bristol.ac.uk

Engineering and Physical Sciences Research Council
TOSHIBA
University of BRISTOL
ROKE
GCHQ

SECURE WIRELESS AGILE NETWORKS

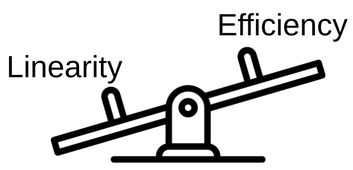
WP4: RF Transmitter and Receiver Development

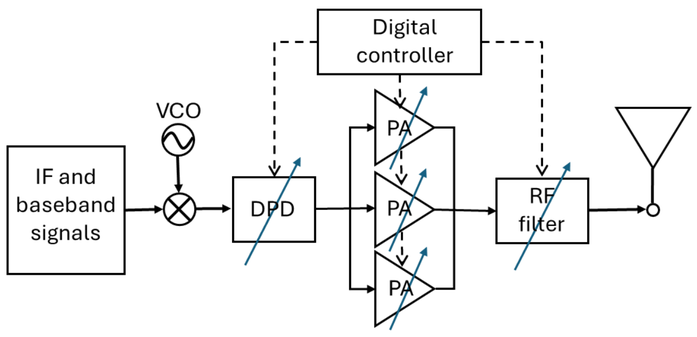
Dr. Jiteng Ma

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. Developing agile and intelligent RF front-end is essential to enhance the security of the wireless communication system.

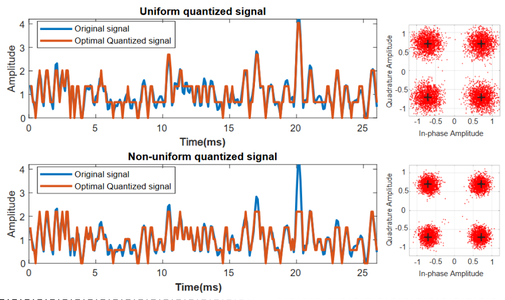
Digitally-controlled transmitters

Digitally controlled RF power amplifiers (PA) ensure high performance through adaptive power management, fast switching, and efficient signal processing while enhancing secure communication by enabling encryption, jamming resistance, and precise modulation control.

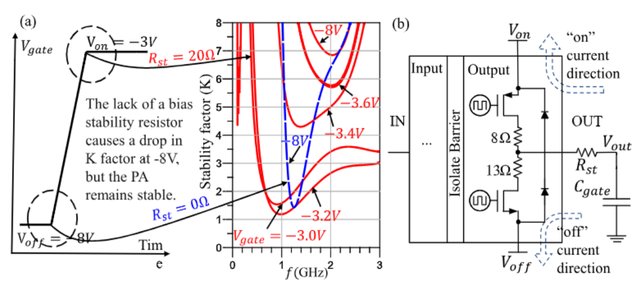




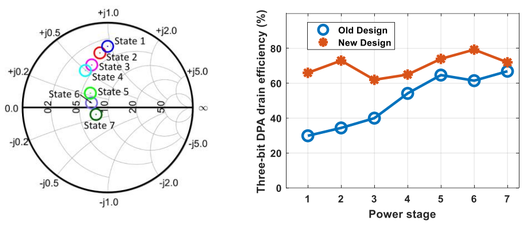
The amplifying linearity can be enhanced by properly quantize the modulated signal.



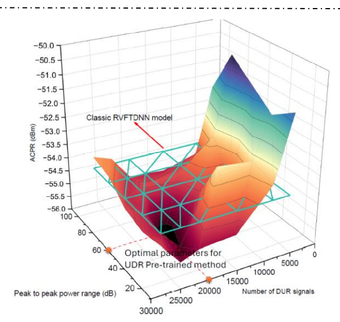
We developed a fast gate-switching PA achieving rise and fall times of 750ps and 950ps.



We developed 3-bit DPA to achieve very high backoff efficiency.

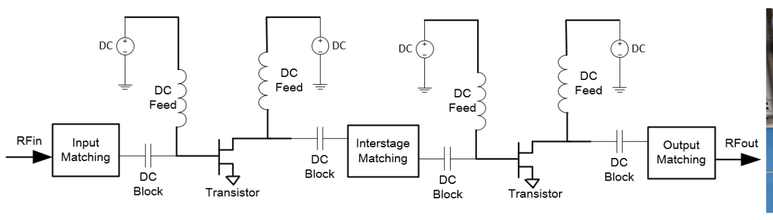


We developed a pre-training ML method for digital pre-distortion (DPD) using self-defined random data to enhance PA nonlinear estimation and adaptability across operating conditions.

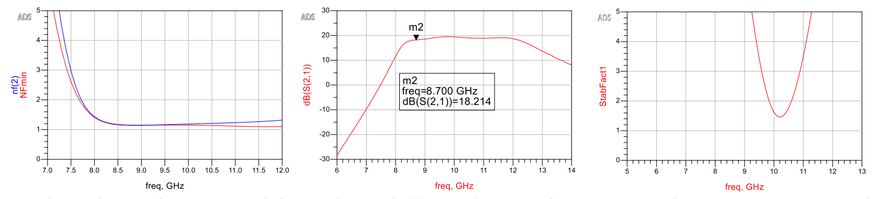


Reconfigurable receivers

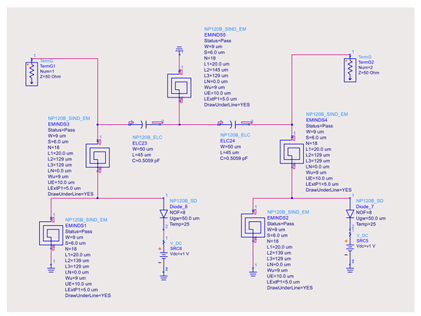
Traditional low-noise amplifiers (LNAs) struggle to deliver the required performance due to limitations in noise figure, robustness, and efficiency. Gallium Nitride (GaN)-based monolithic microwave integrated circuits (MMICs) provide a groundbreaking solution by leveraging high electron mobility to achieve LNA superior performance.

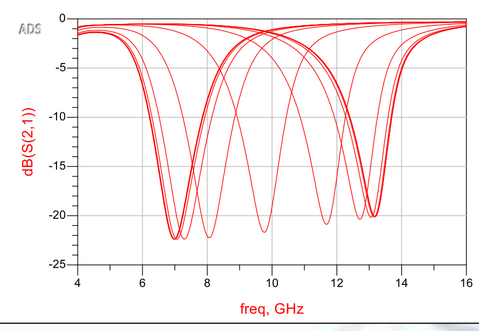


We developed multiple LNAs at L-band, S-band, and X-band using WIN Semiconductors GaN MMIC 120nm and 240nm processes. These designs outperform most state-of-the-art LNAs developed using other processes.



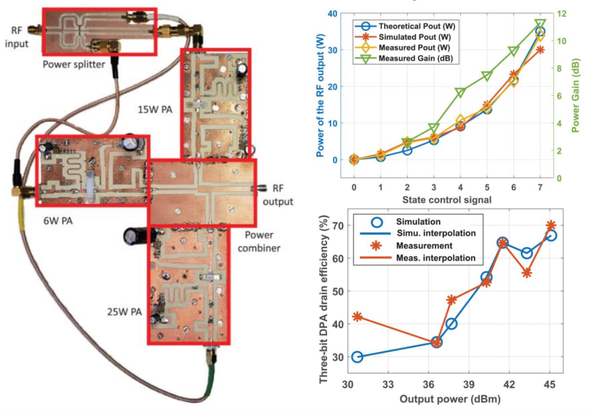
We developed a tuneable X-band filter that enhances cyber-secure RF design by enabling fast, accurate frequency agility with high selectivity to suppress out-of-band and broadband interference.



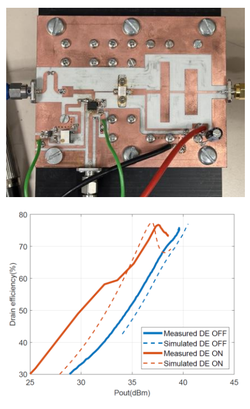


Selected designs on PCB and MMIC

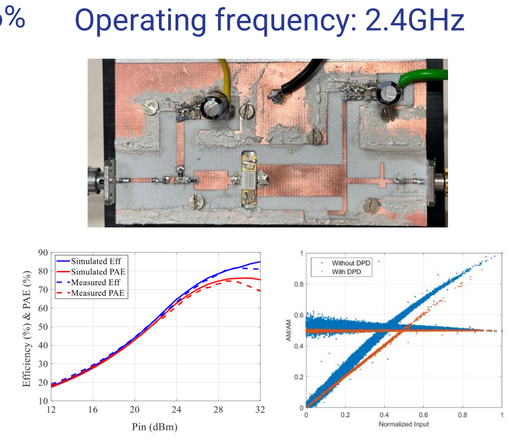
3-bit digital PA:
Peak PAE: 64.3%
Peak output power: 45.2dBm
7.5dB backoff efficiency: 47.3%



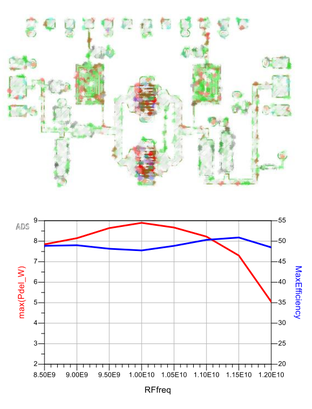
Gate switching PA:
Peak efficiency: 76%
Peak output power: 39.5dBm
3dB backoff efficiency: 76%



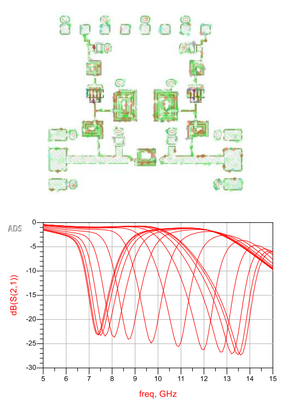
Inverse Class-E PA:
Peak efficiency: 82%
Peak output power: 41dBm
Operating frequency: 2.4GHz



Inverse-class F MMIC PA:
Peak efficiency: 43%-52%
Peak output power: 40.6dBm
Bandwidth: 8.5GHz to 11.5GHz



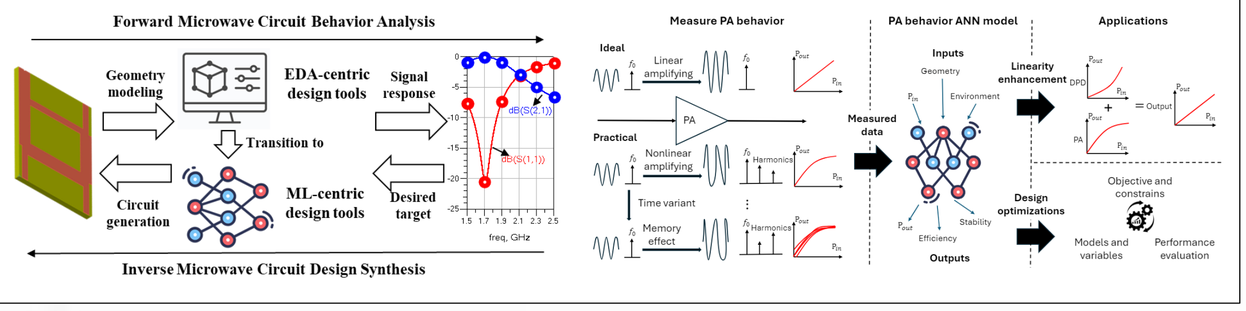
Tuneable MMIC notch filter
Range: 8GHz to 12GHz
2dB bandwidth:
Insertion loss: less than 1dB



What artificial intelligence (AI) can do

AI/machine learning (ML) can be used to design passive circuits such as RF filter, matching network, and coupler.

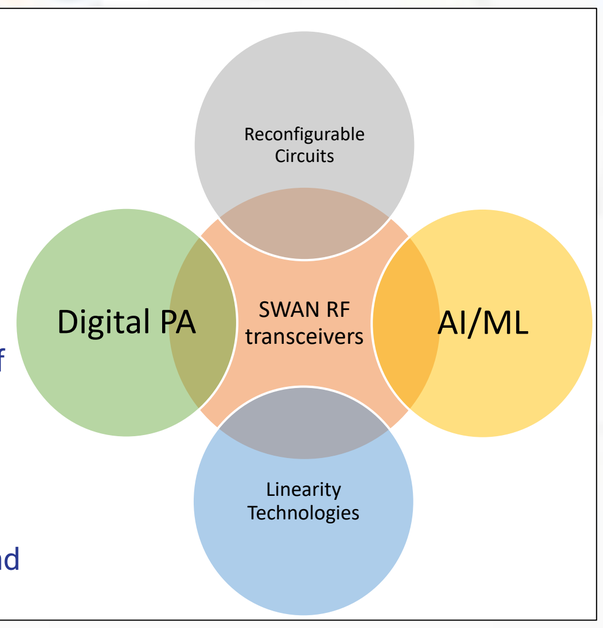
AI/ML can be used to model the behaviour of active devices and optimize the PA linearity based on the input signal (predistortion) or circuit design.



Conclusion

Proper RF transceivers to align with SWAN targets should include the following characters:

- Enhance the analogue RF PA using digital techniques.
- High-performance GaN LNA to enhance the linearity implications of the receiving signals
- Reconfigurable filter is important to reject the jamming signals.
- AI/ ML can make significant contributions to the performance and intelligence of the RF transceivers



This research was supported through the UKRI/EPSRC Prosperity Partnership in Secure Wireless Agile Networks (EP/T005572/1).

Communication Systems & Networks Research Group
Merchant Venturers Building, Woodland Road, Bristol, BS8 1TR

@PartnershipSWAN
https://www.swan-partnership.ac.uk/
linkedin.com/company/swan-prosperity-partnership
swan-programme@bristol.ac.uk

Engineering and Physical Sciences Research Council
TOSHIBA
University of BRISTOL
ROKE
GCHQ