SECURE WIRELESS AGILE NETWORKS

RF Fingerprinting to Aid Cyber Security in Low Cost Wireless IoT Systems:

16th September 2021

DCMS/SPF event on 6G: Software Defined Radio and RF Sampling

Mark Beach, Academic PI

Manish Nair & Tommaso Cappello

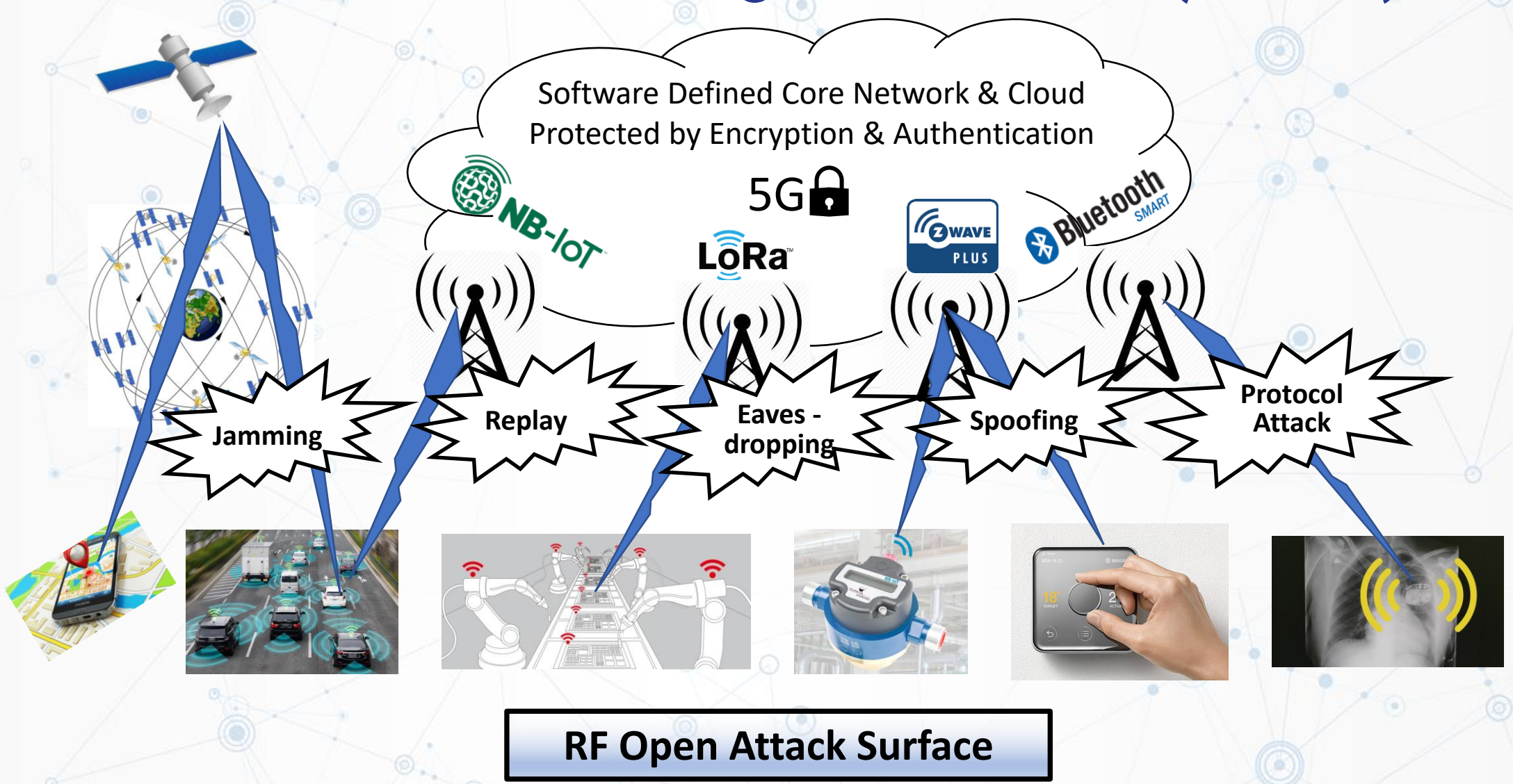
Communications Systems & Networks Group
Smart Internet Lab

University of Bristol

swan-programme@bristol.ac.uk

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

Secure Wireless Agile Networks (SWAN)



RF Open Attack Surface

Secure Wireless Agile Networks (SWAN)

- Joint industrial / academic research programme addressing creation of Secure Wireless Agile Networks (SWAN) that are *resilient to both cyber-attacks and accidental or induced failures*.
- Funded through 3rd Call for UKRI/EPSRC Prosperity Partnerships, £40 million government, industry and university investment *"to transform the way people live, work and travel"* see press release
  - SWAN, with a £6.1M 5 year research programme, is one of six projects funded and started 1st February 2020
  - Toshiba Europe, Roke Manor Research, GCHQ & University of Bristol

    "bringing together a cadre of engineers from industry, government and academia with invaluable commercial insights and in-depth technical skills capable of delivering holistic solutions for a productive, healthy, resilient and connected nation"

Secure Wireless Agile Networks (SWAN)

- Wireless networks that underpin much of modern life are increasingly vulnerable to cyber-attacks and other induced failures.
- SWAN aims to develop secure wireless networks that are resilient to these threats, protecting individuals, businesses and society.
- The Research Programme will:
  - Identify vulnerabilities in the RF interfaces;
  - Development of techniques to detect and mitigate against the effects of cyber-attacks;
  - Create enabling technology for truly Software Defined Radios following “Secure by Design” principles;
  - Creation of more resilient and secure systems.

SWAN's Research Challenges

RC1: Threat Synthesis and Assessment

- Vulnerabilities of wireless to RF cyber attacks have received little attention.
- For critical infrastructure, impact of denial of service and manipulation of data and control need to be understood, as well as understanding the mechanics of such an attack.

Threat	Definition
Spoofing	Pretending to be someone/something other than yourself
Tampering	Modifying something on disk/network/memory/etc.
Repudiation	Claiming not to be responsible for something
Information Disclosure	Providing information to someone unauthorised to access it
Denial of Service	Exhausting resources required to provide service
Elevation of Privilege	Allowing someone to do something they are not authorised to do

ROKE STRIDE cards

SWAN's Research Challenges

RC1: Threat Synthesis and Assessment

- Vulnerabilities of wireless to RF cyber attacks have received little attention.
- For critical infrastructure, impact of denial of service and manipulation of data and control need to be understood, as well as understanding the mechanics of such an attack.

RC2: RF Cyber Detection & Defence

- Power and cost-effective solutions required for large-scale monitoring of potential attacks.
- Resilient waveforms, robust protocols and enhancement spatial processing techniques are required to defend assets.

SWAN's first candidate RAN: LoRaWAN

- Fast adoption of LoRaWAN as a low power, long range wireless IoT technology thanks to the LoRa Alliance®
  - **156** LoRaWAN Network Operators in **171** Countries
  - Multiple use cases, including critical infrastructure

Environment monitoring

Parking management

Safety and security

Street lighting

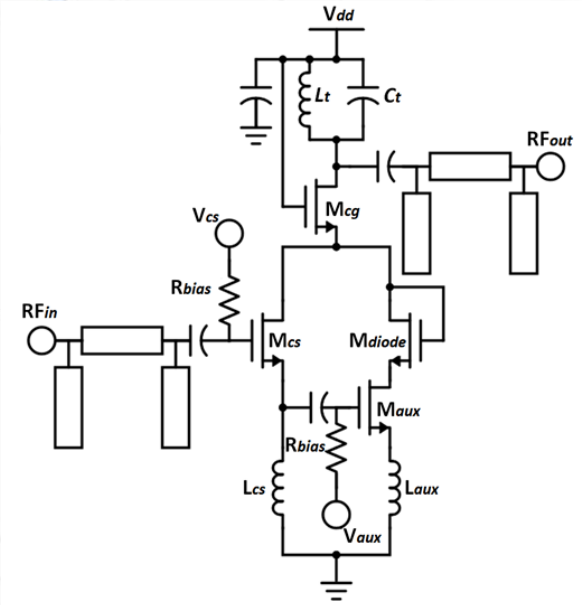
Waste management

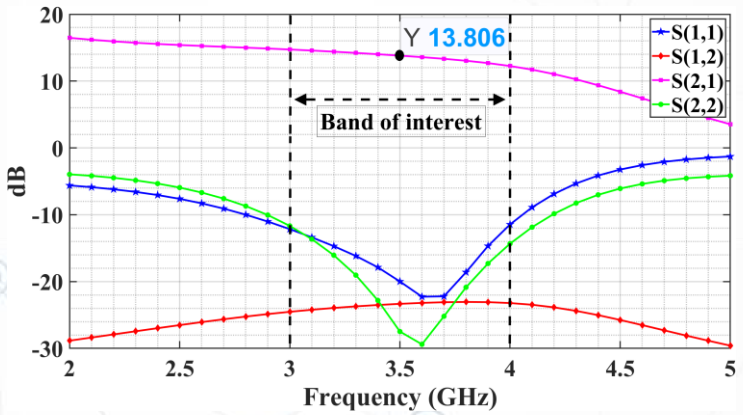
- A number of studies have shown that LoRaWAN may be susceptible to jamming attacks
  - E. Aras, N. Small, G. S. Ramachandran, D. Stéphane, W. Joosen, D. Hughes, (2018), "Selective Jamming of LoRaWAN using Commodity Hardware," *MobiQuitous 2017*, Melbourne, VIC, Australia, November 7–10, 2017, pp. 363–372, https://doi.org/10.1145/3144457.3144478
  - Trend Micro Technical Brief: The current state of LoRaWAN security: https://documents.trendmicro.com/assets/pdf/The%20Current%20State%20of%20LoRaWAN%20Security.pdf

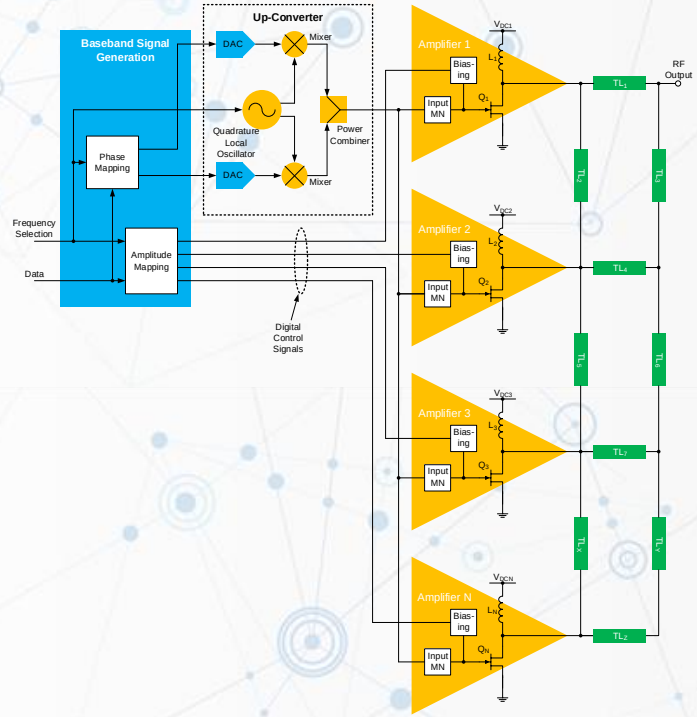
SWAN's Research Challenges

RC3: Cyber Secure Radio Design

- Need for RF architectures which are more resilient to attack and facilitate the detection of an adversary.
- RF transceivers which can offer enhanced frequency agility and thus support dynamic spectrum access (DSA)







SWAN's Research Challenges

RC3: Cyber Secure Radio Design

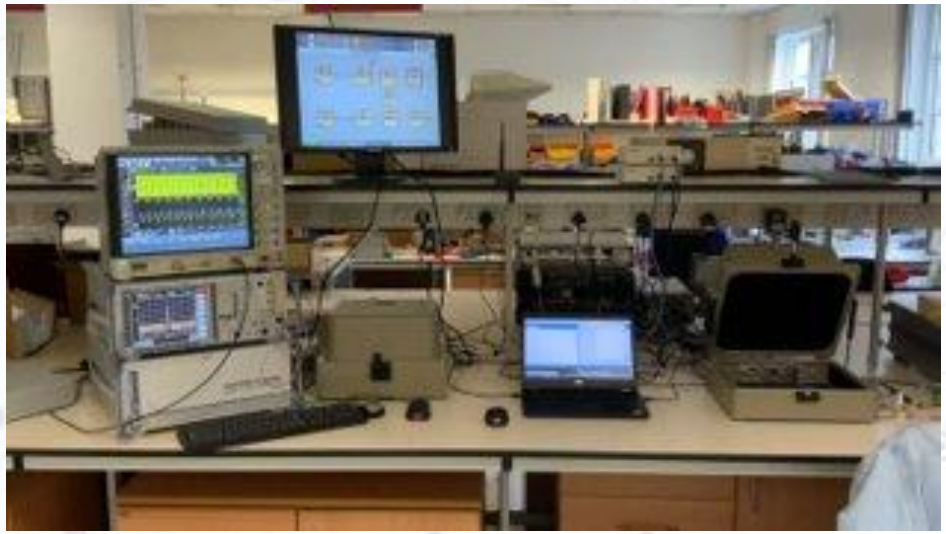
- Need for RF architectures which are more resilient to attack and facilitate the detection of an adversary.
- RF transceivers which can offer enhanced frequency agility and thus support dynamic spectrum access (DSA)

RC4: Secure Dynamic Spectrum Access

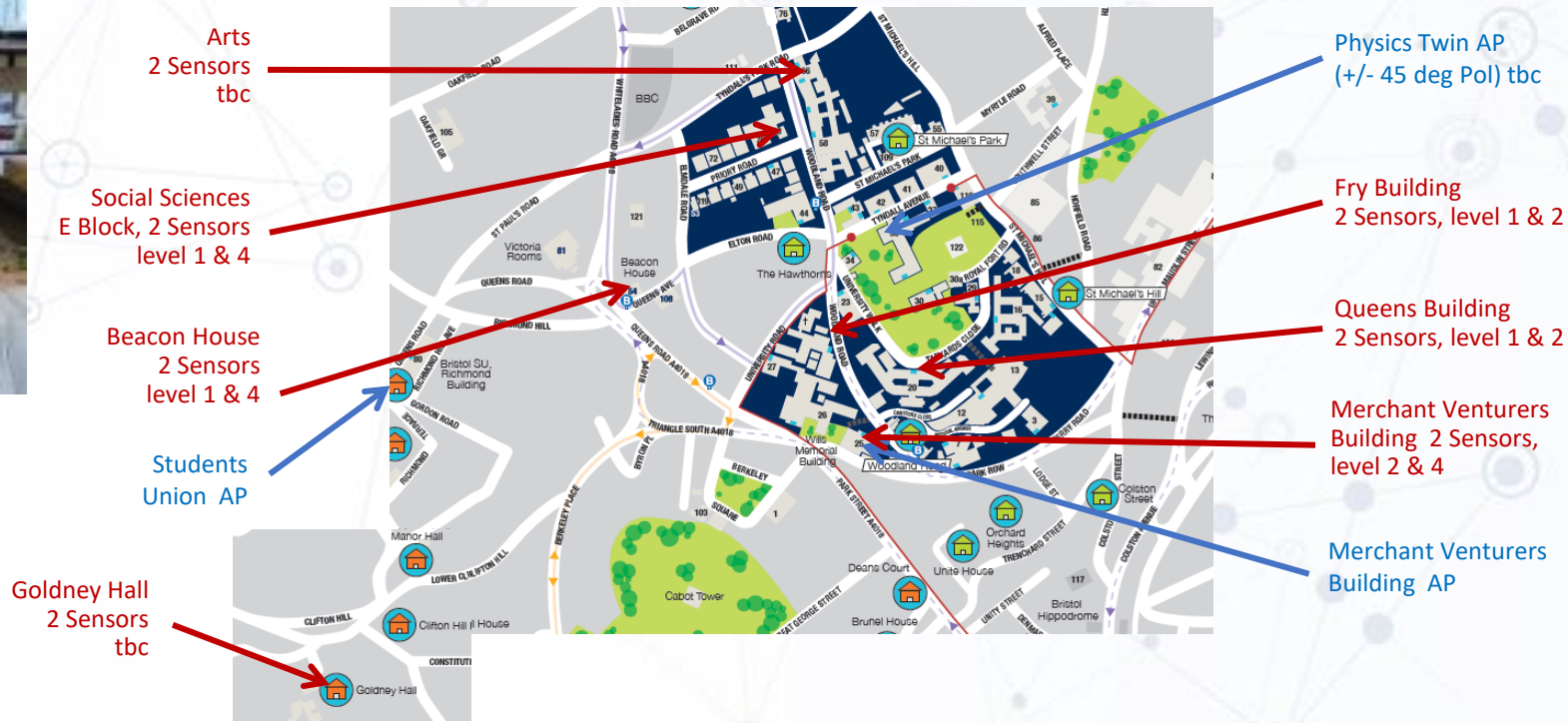
- Understanding the vulnerabilities of sharing protocols is essential if DSA is to be secure
- Need for enhanced RF transceiver technology to support a change from fixed spectrum allocation.

See Simon Wilson, 1st Workshop on 6G: Technology Enablers for Spectrum & Power Efficiency Wireless Access, 26th May 2021 (hosted by Uni of Bristol)

SWAN's Test Beds

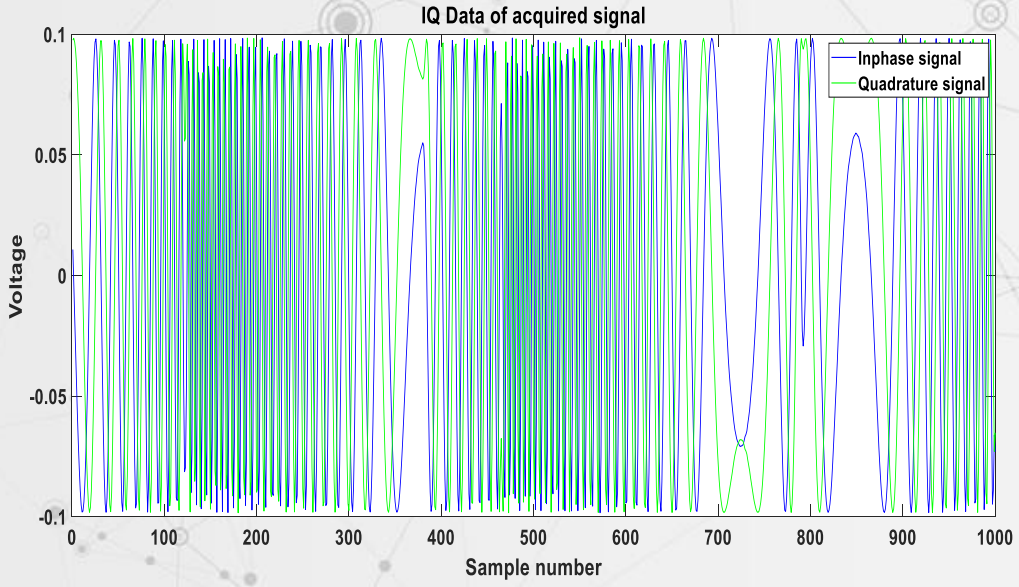


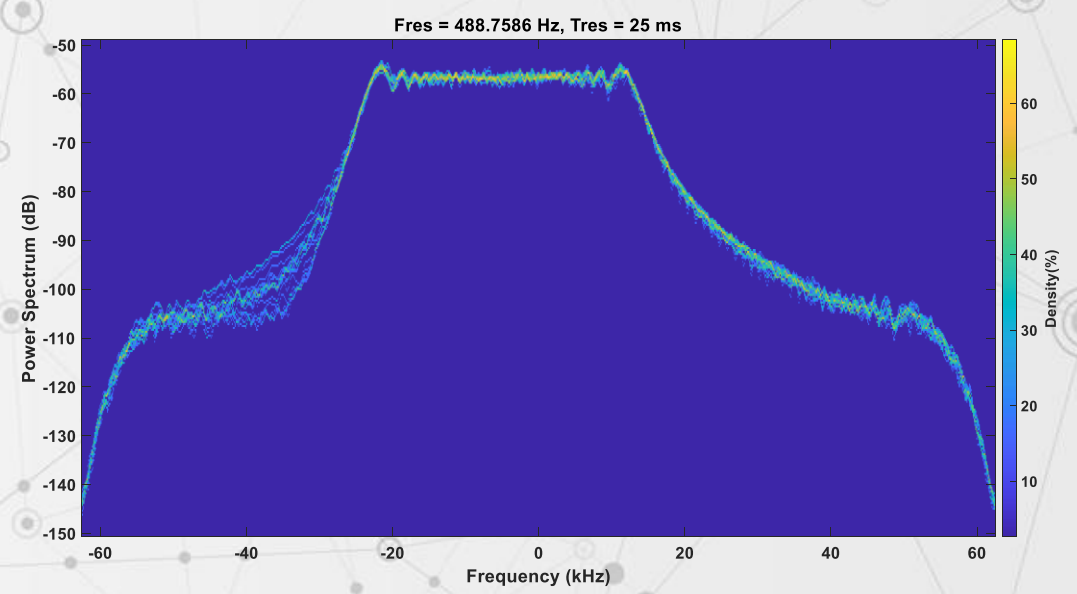
RF Penetration Testing:
Inc: IQ Capture

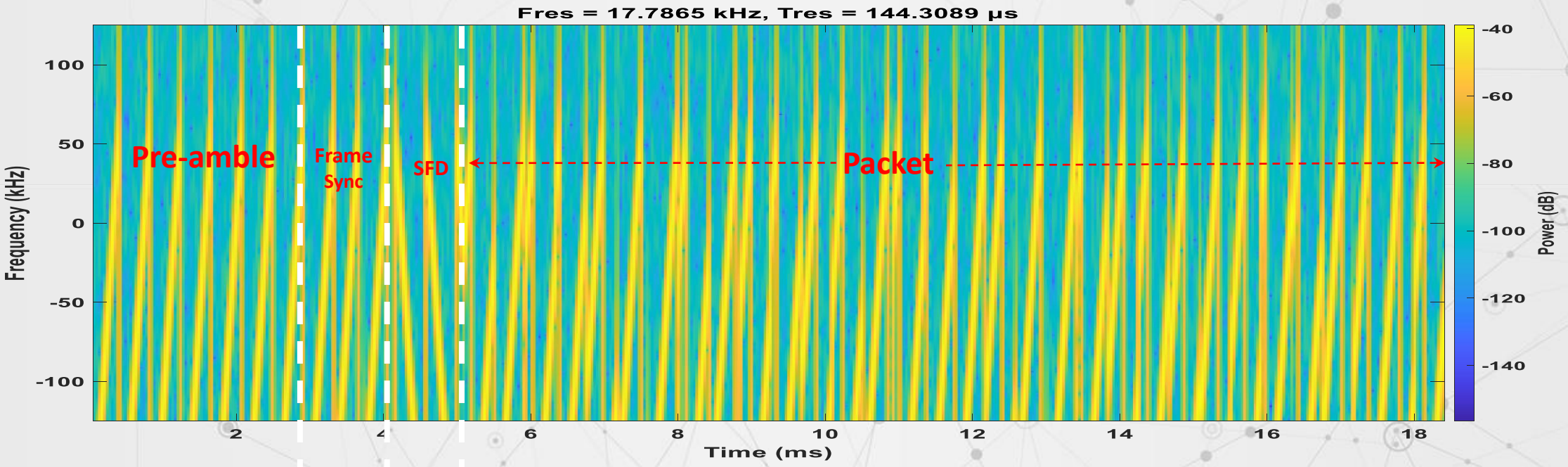


Clifton Campus LoRaWAN
AP & Sensor deployments

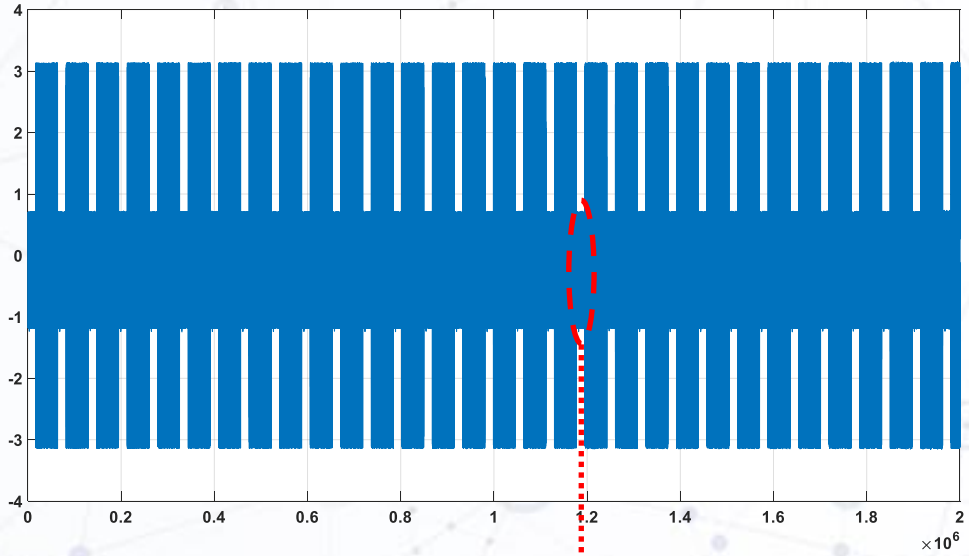
Over the Air LoRa waveforms

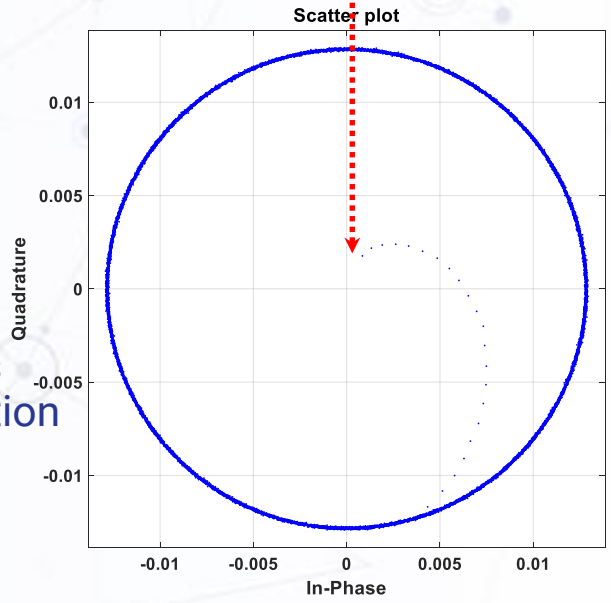




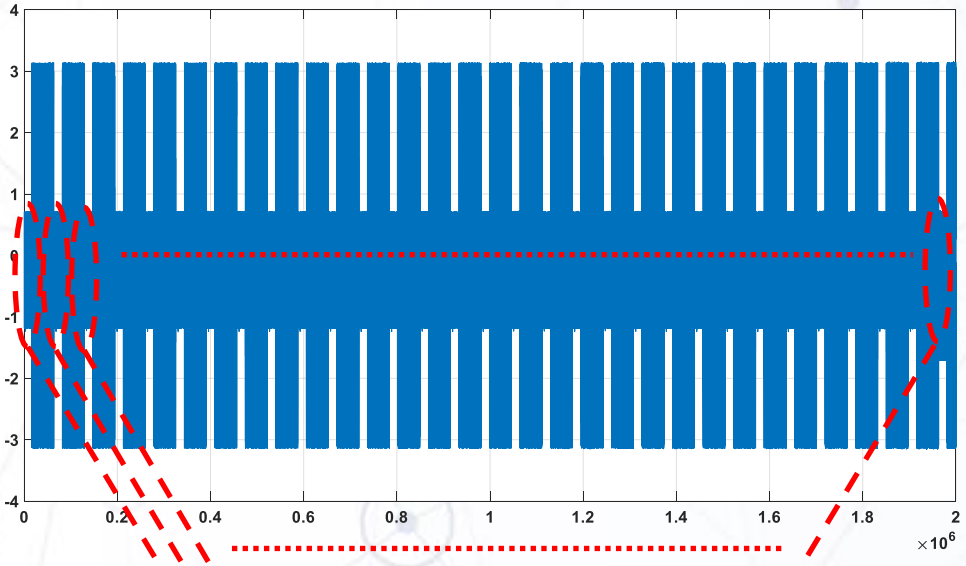


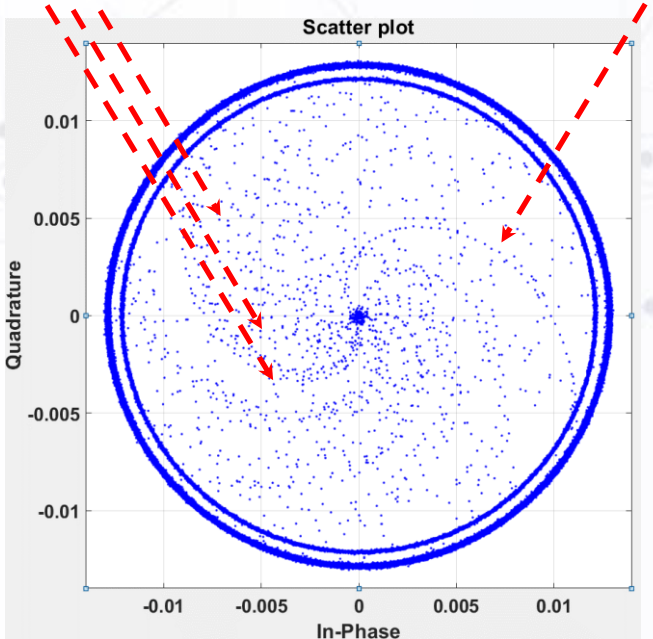
I/Q Data





- Constant amplitude
- Continuous phase rotation



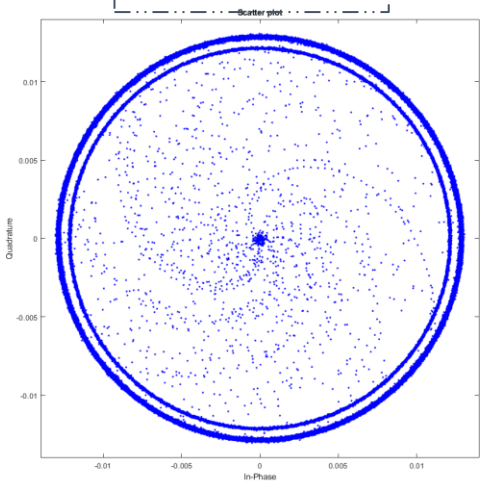


- Constellation rotation due to CFO

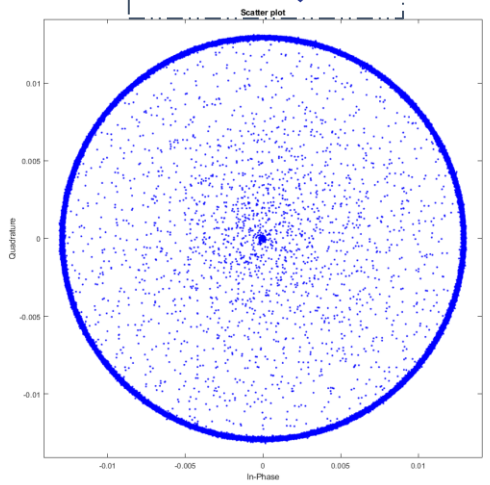
SECURE WIRELESS AGILE NETWORKS

Fingerprinting LoRa: Neutral Network (NN) Clustering of Differential Constellation Trace Figures

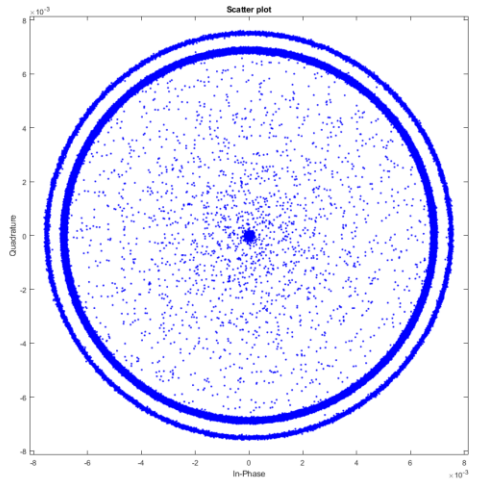
SODAQ-A



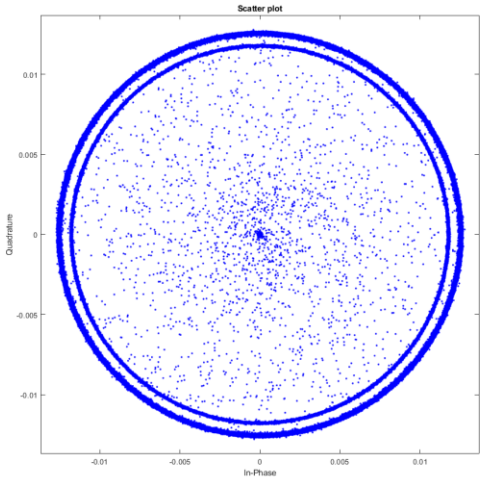
SODAQ-B



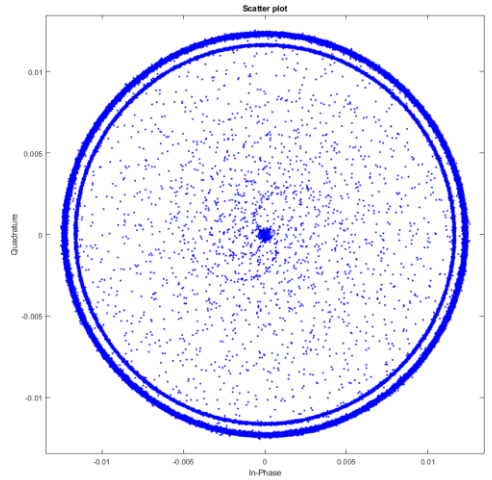
SODAQ-C



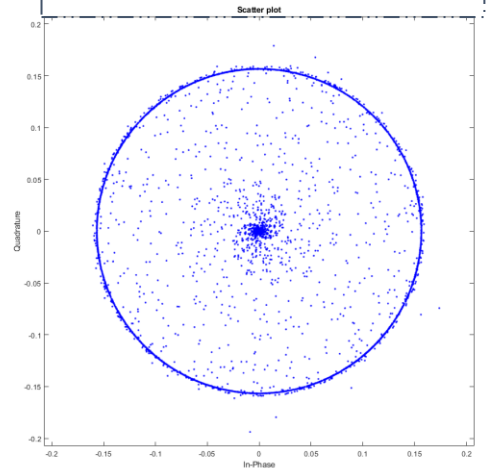
SODAQ-D



SODAQ-E

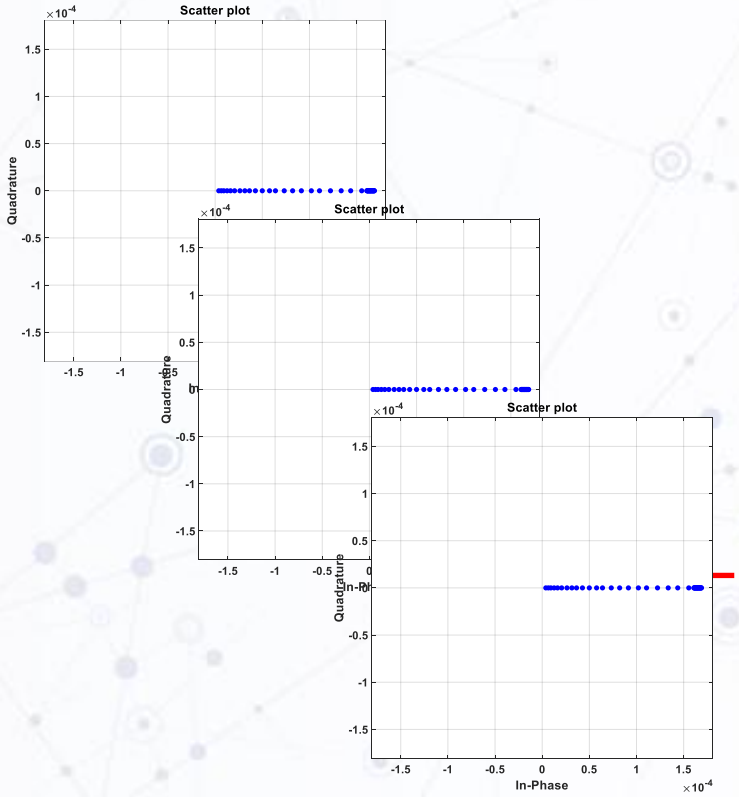


ARB

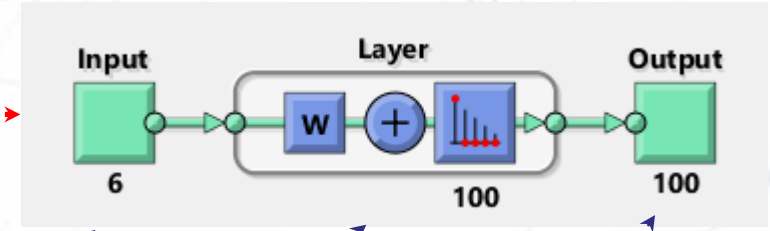


SECURE WIRELESS AGILE NETWORKS

Fingerprinting LoRa: NN Clustering of Differential Constellation



IQData[st:end].*conj(IQData[st:end])



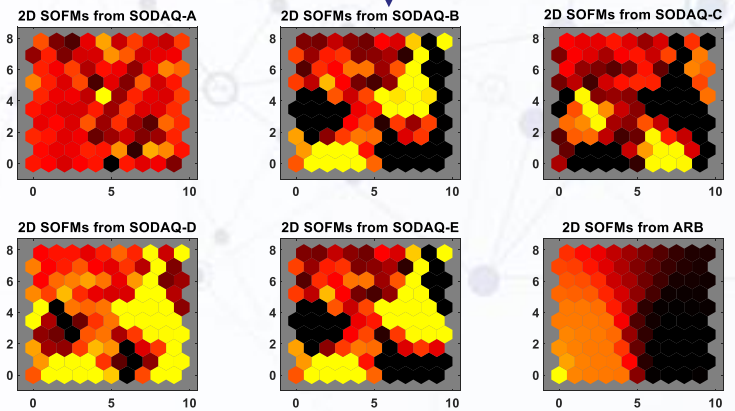
$6x[1x16270]^H$
High Dimensional Input Matrix

[6x10] Input Weight Matrix

$[6x\{10x1^H, \cdots, 10x1^H\}]^H$
$=6x[10X10]$
Kohonen (NN) Layer Matrix

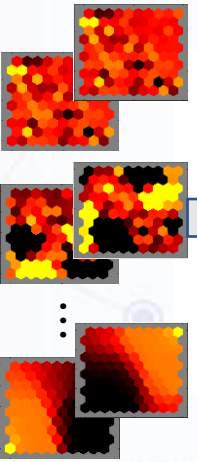
Trace Figures: 2D Self-Organizing Feature Map

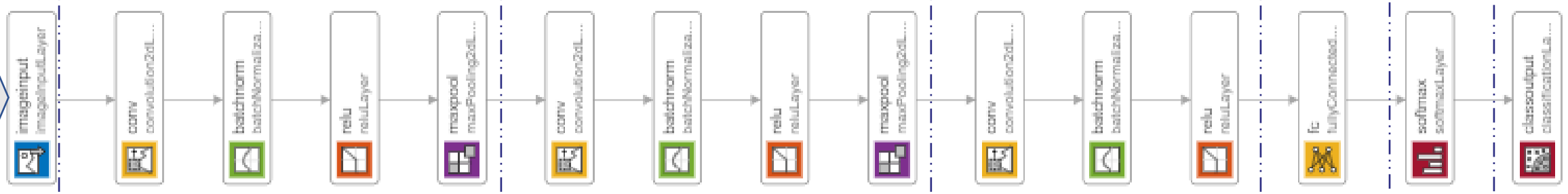
$6x[10X10]$
Low Dimensional Output Layer Matrix: 2D SOFMs



SWAN
SECURE WIRELESS AGILE NETWORKS

Fingerprinting LoRa: Classification based on CNN





371x314x3 input layer

[3,8]x32: Filter Size
[2,2]: Stride

1st convolution layer

Batch Normalisation layer

[5,5]: Pool Size
[1,1]: Stride

[3,8]x32: Filter Size
[2,2]: Stride

2nd convolution layer

Batch Normalisation layer

[5,5]: Pool Size
[1,1]: Stride

[3,8]x32: Filter Size
[2,2]: Stride

3rd convolution layer

Batch Normalisation layer

[5,5]: Pool Size
[2,2]: Stride

Fully Connected Layer

Size: 6

Softmax Layer

$\hat{j} = \arg\max_j \sum_{i=1}^{n_k} \mathbb{E}[p_{ij}]$

$Cost(f) = \sum Loss(f)$: ASGD

Classifi-cation Layer

- *Expected to be* invariant to MAC ID Spoofing: due to multiple 2D SOFMs from multiple training epochs

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

SWAN Quarterly Newsletter

Issue 1 - Autumn 2020

Sign up to our Quarterly Newsletter to receive regular updates on the latest SWAN news and research activities:

https://bit.ly/332RR5z

SECURE WIRELESS AGILE NETWORKS

swan-programme@bristol.ac.uk

www.swan-partnership.ac.uk
www.bris.ac.uk/smart | www.bris.ac.uk/csn

@PartnershipSWAN
@bristol_smart | @BristolCSN

linkedin.com/company/swan-prosperity-partnership