SWAN Prosperity Partnership:

LoRaWAN Performance Evaluation and Resilience under jamming attacks

Vaia Kalokidou, Manish Nair & Mark Beach
University of Bristol

Sensor Signal Processing for Defence Programme
Wednesday 14th September 2022

Communications Systems & Networks Group
Smart Internet Lab

University of Bristol

swan-programme@bristol.ac.uk

Summary of Presentation

- SWAN Prosperity Partnership
  - Consortium
  - Research Challenges
- Jamming Attack Analysis
  - Candidate RAT: LoRa
- RF Pen-Testing & Finger Printing
  - Waveform Analysis
  - ML processing to uniquely identify individual sensors
- Conclusions & Next Steps

Secure Wireless Agile Networks

- 5-year collaborative research programme funded, started February 2020
- Project partners:
- Focussing detection & mitigation of on Cyber Attacks at “RF Open Attack Surface”

RF Cyber Crime

Secure Wireless Agile Networks

- 5-year collaborative research programme funded, started February 2020
- Project partners:

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

- Focussing detection & mitigation of on Cyber Attacks at "RF Open Attack Surface"
- Research Challenges:
  - RC1: Threat Synthesis and Assessment
    - Identify vulnerabilities in the RF interfaces

	Threat	Property Violated	Threat Definition
S	Spoofing identity	Authentication	Pretending to be something or someone other than yourself
T	Tempering 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

Roke's RF STRIDE cards

Secure Wireless Agile Networks

- 5-year collaborative research programme funded, started February 2020
- Project partners:

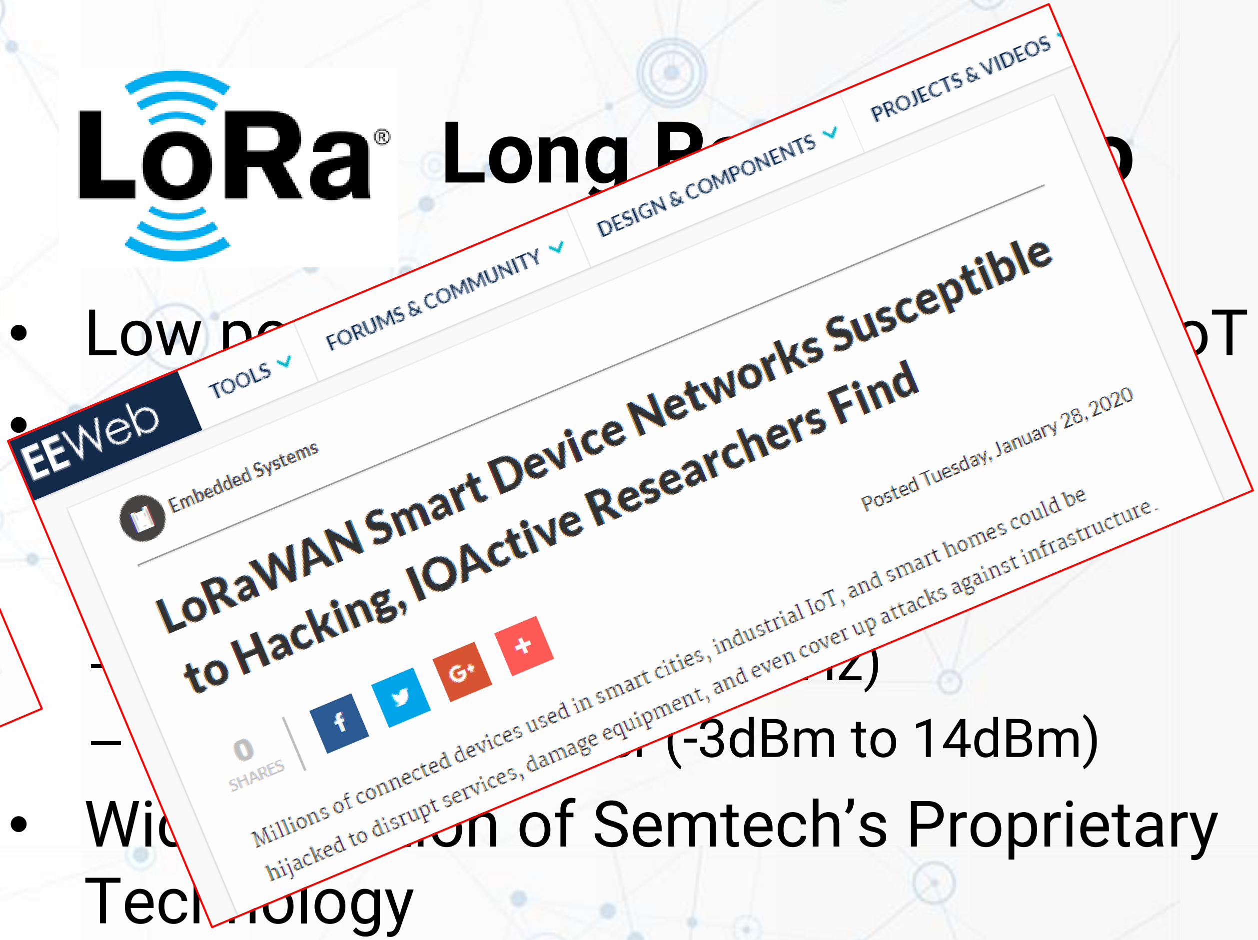
TOSHIBA ROKE GCHQ University of BRISTOL UKRI Engineering and Physical Sciences Research Council

- Focussing detection & mitigation of on Cyber Attacks at “RF Open Attack Surface”
- Research Challenges:
    - RC1: Threat Synthesis and Assessment
        - Identify vulnerabilities in the RF interfaces
    - RC2: RF Cyber Detection & Defence
        - Solutions for detecting attacks at scale

Wireless IoT Devices

Long R...

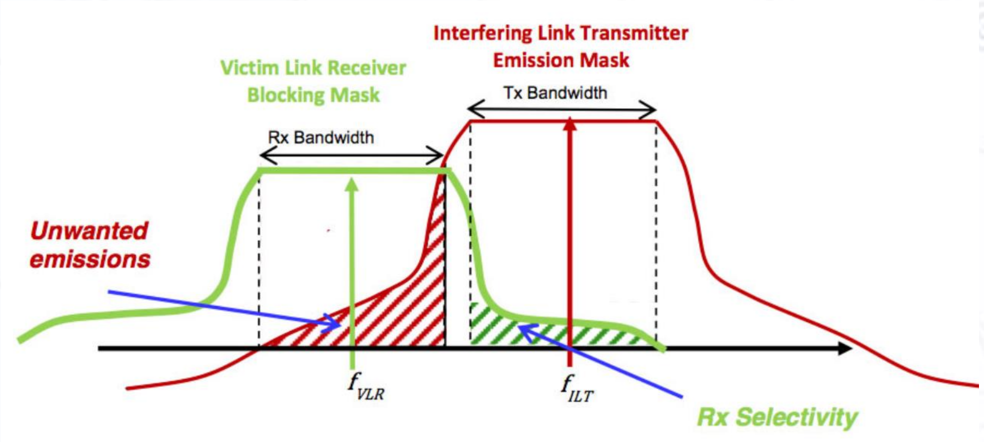
- Low po... ...oT
- ...
  - ...z)
  - ... (-3dBm to 14dBm)
- Wi... ...on of Semtech's Proprietary Tec... ...ology
- SWAN's PHY candidate

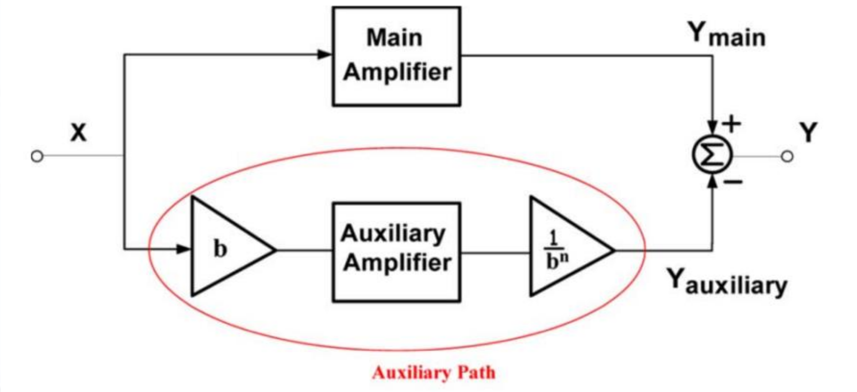


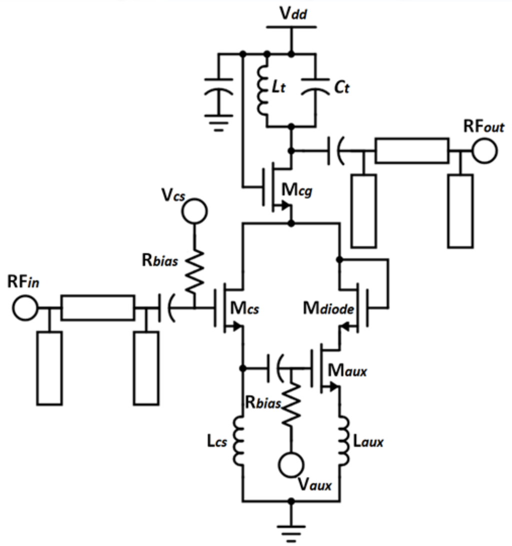
Secure Wireless Agile Networks

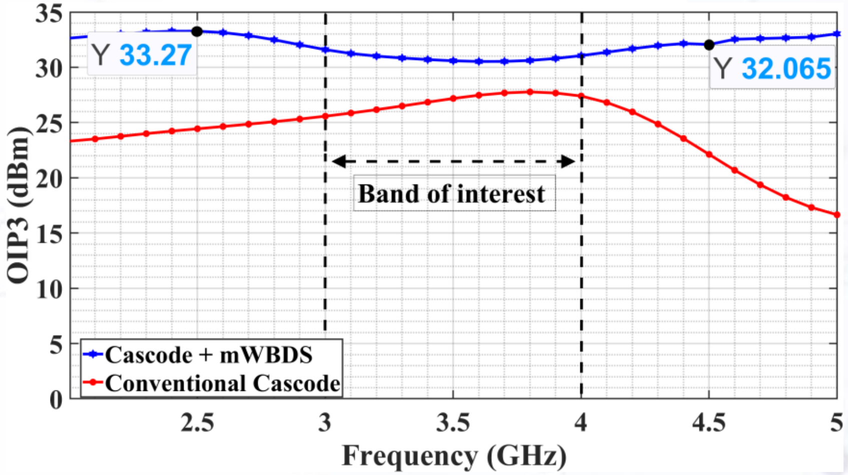
- 5-year collaborative research programme funded, started February 2020
- Project partners:
- Focussing detection & mitigation of on Cyber Attacks at "RF Open Attack Surface"
- Research Challenges:
  - RC1: Threat Synthesis and Assessment
    - Identify vulnerabilities in the RF interfaces
  - RC2: RF Cyber Detection & Defence
    - Solutions for detecting attacks at scale
  - RC3: Cyber Secure Radio Design
    - Resilient & Frequency agile RF transceivers

High Dynamic Range Receivers



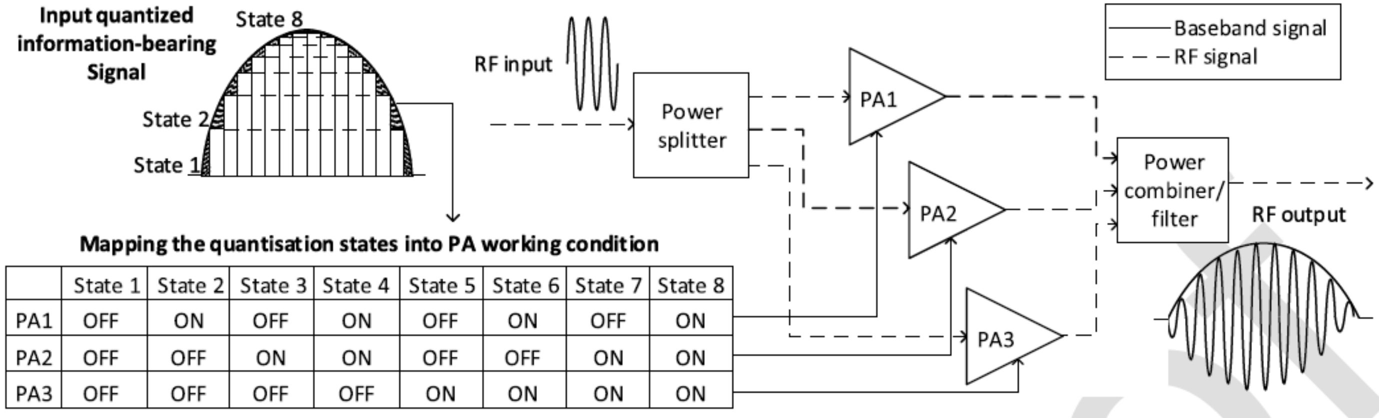




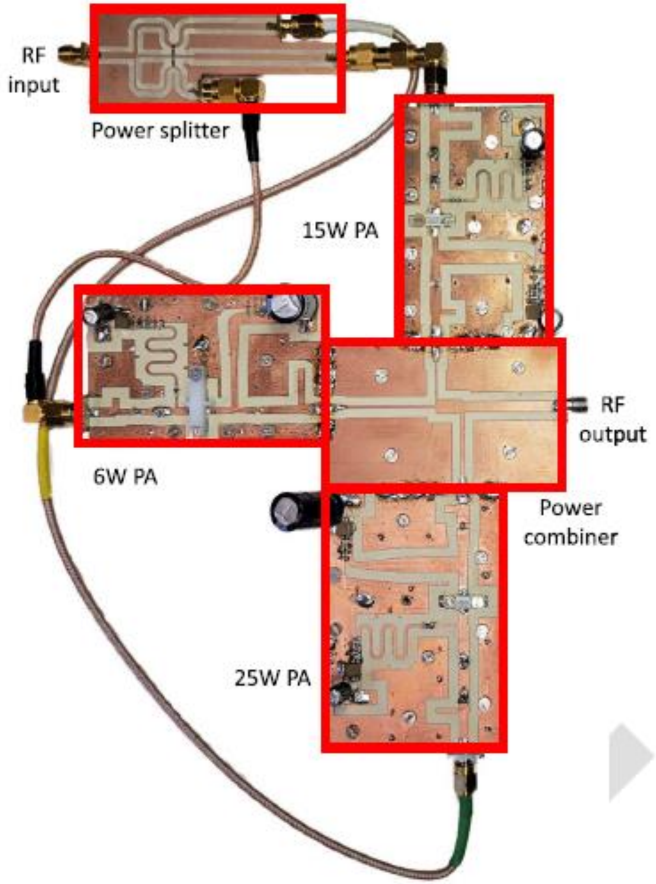


S. Ozan et al "Low-Noise Amplifier with Wideband Feedforward Linearisation for Mid-Band 5G Receivers,"
IEEE Asia Pacific Conference on Circuits and Systems (APCCAS), 2020, pp. 125-128, 10.1109/APCCAS50809.2020.9301695.

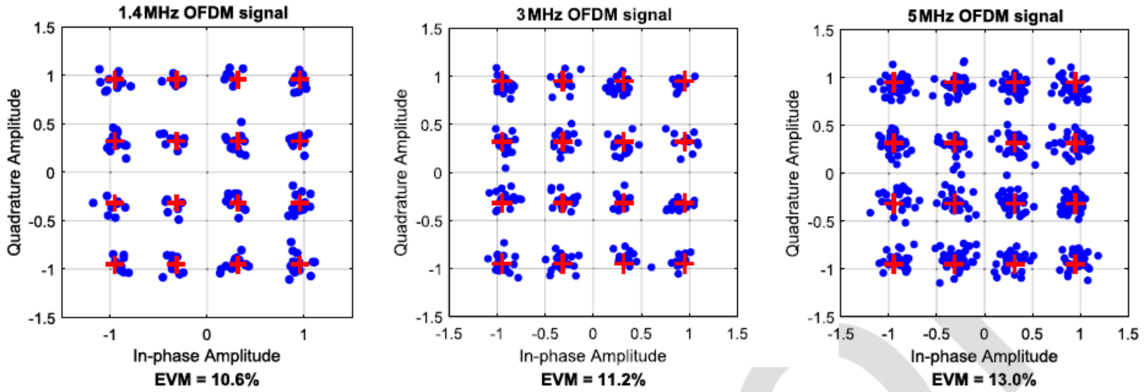
Enabling Technology: Digital RF PA



	State 1	State 2	State 3	State 4	State 5	State 6	State 7	State 8
PA1	OFF	ON	OFF	ON	OFF	ON	OFF	ON
PA2	OFF	OFF	ON	ON	OFF	OFF	ON	ON
PA3	OFF	OFF	OFF	OFF	ON	ON	ON	ON



OFDM Frame Configuration			
Bandwidth	1.4 MHz	3 MHz	5 MHz
Frame Duration	10ms		
FTT Size	128	256	512
Resource Blocks	6	15	25
Data Subcarriers	72	180	300



J. Ma, G. Jindal, M. Nair, T. Cappelo, G.T. Watkins, K.A. Morris & M.A.Beach, *Highly Efficient 3-Bit Digital Power Amplifier for OFDM Waveform Amplification*, IEEE Trans MTT, Aug 2022

Secure Wireless Agile Networks

- 5-year collaborative research programme funded, started February 2020
- Project partners:
- Focussing detection & mitigation of on Cyber Attacks at "RF Open Attack Surface"
- Research Challenges:
  - RC1: Threat Synthesis and Assessment
    - Identify vulnerabilities in the RF interfaces
  - RC2: RF Cyber Detection & Defence
    - Solutions for detecting attacks at scale
  - RC3: Cyber Secure Radio Design
    - Resilient & Frequency agile RF transceivers
  - RC4: Secure Dynamic Spectrum Access
    - Understanding the vulnerabilities of sharing protocols

Wireless IoT Devices

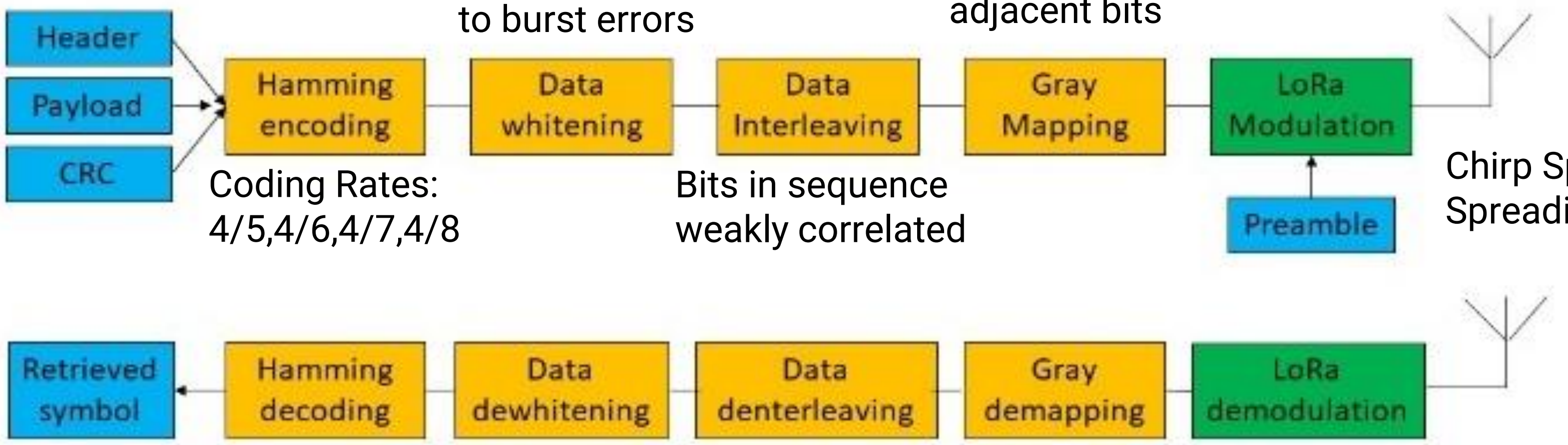
LoRa Long Range Radio

- Low power, low data rate for wireless IoT
- Chirp Spread Spectrum (CSS)
  - ISM bands (868MHz)
  - Variable Spreading Factors (5,6)
  - Channel bandwidths (250kHz)
  - Adjustable Tx power (-3dBm to 14dBm)
- Wide Adoption of Semtech’s Proprietary Technology
- SWAN’s PHY candidate

LoRa PHY and Frame Format

High immunity to burst errors

Reduced errors in adjacent bits



Coding Rates: 4/5,4/6,4/7,4/8

Bits in sequence weakly correlated

Chirp Spread Spectrum
Spreading Factors: 7-12

Variable size
Detects LoRa signal
Modulated (upchirps)

Freq Synchronisation
Modulated (downchirps)

MAC commands and message
Encoded (variable rates),Modulated (upchirps)

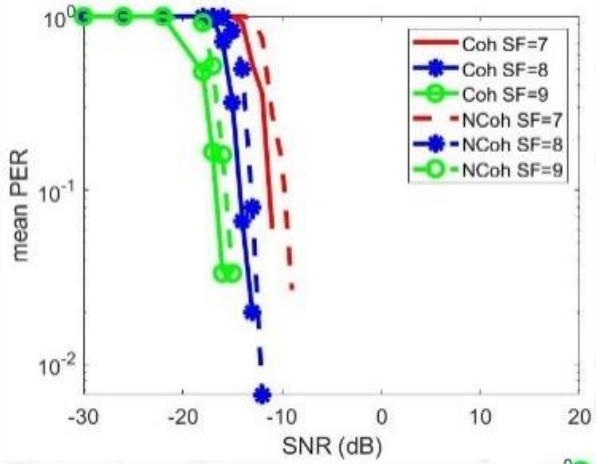
Preamble	SB	SB	Header	Payload	CRC
N symbols	2 symbols	2.25 symbols	M symbols	Max 255 bytes	16 bits

Frame Synchronisation
Modulated (upchirps)

Optional, variable size, Explicit/Implicit
Encoded (4/8), Modulated (upchirps)

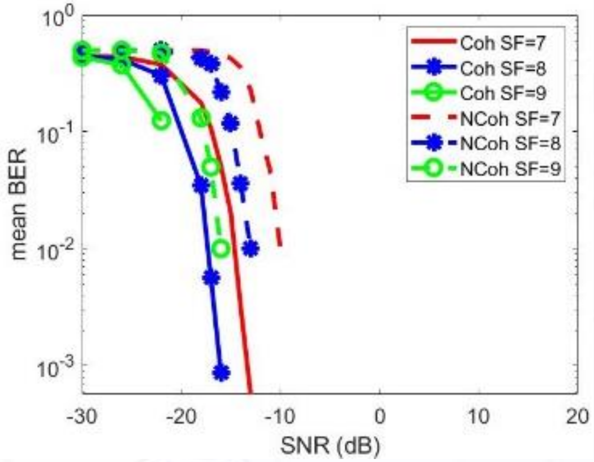
UL, checks for block errors
Encoded (variable rates)
Modulated (upchirps)

LoRa System Performance in AWGN

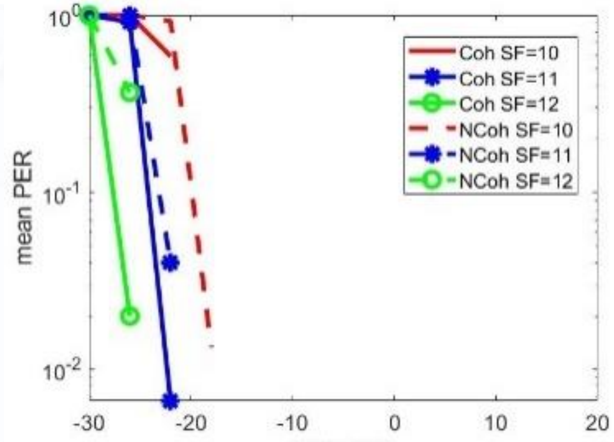


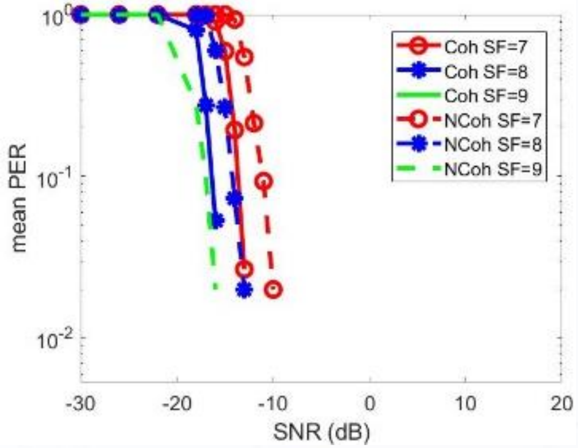
Good agreement with :

B. Al Homssi, et. Al., “*IoT Network Design using Open-Source LoRa Coverage Emulator*”, IEEE Access, vol. 9, pp. 53636-53646, April 2021.



Mean BER & PER
SF=7-9, CR=4

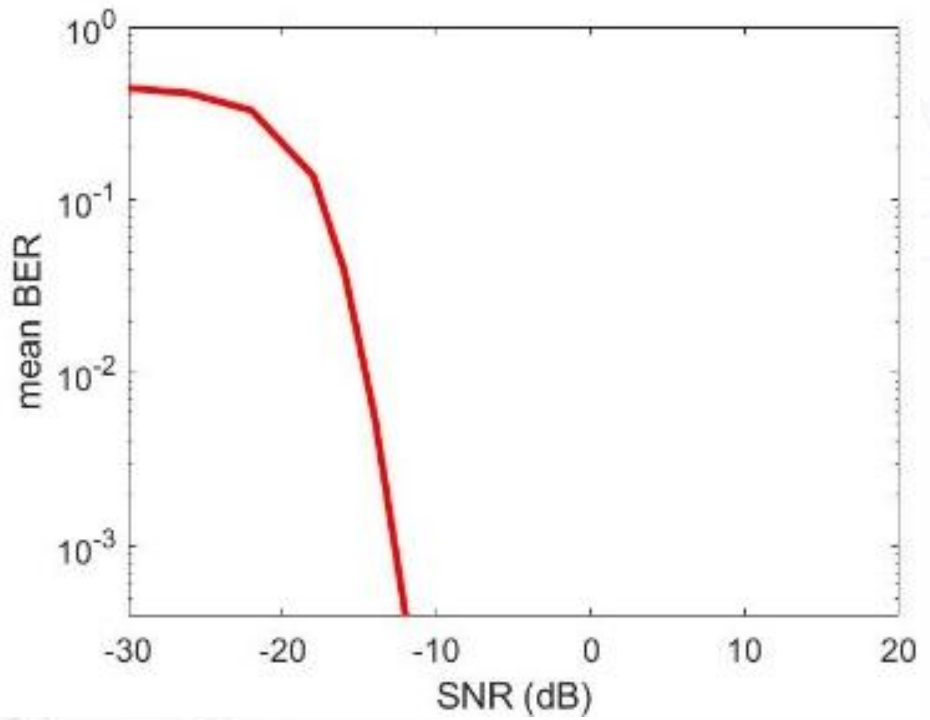




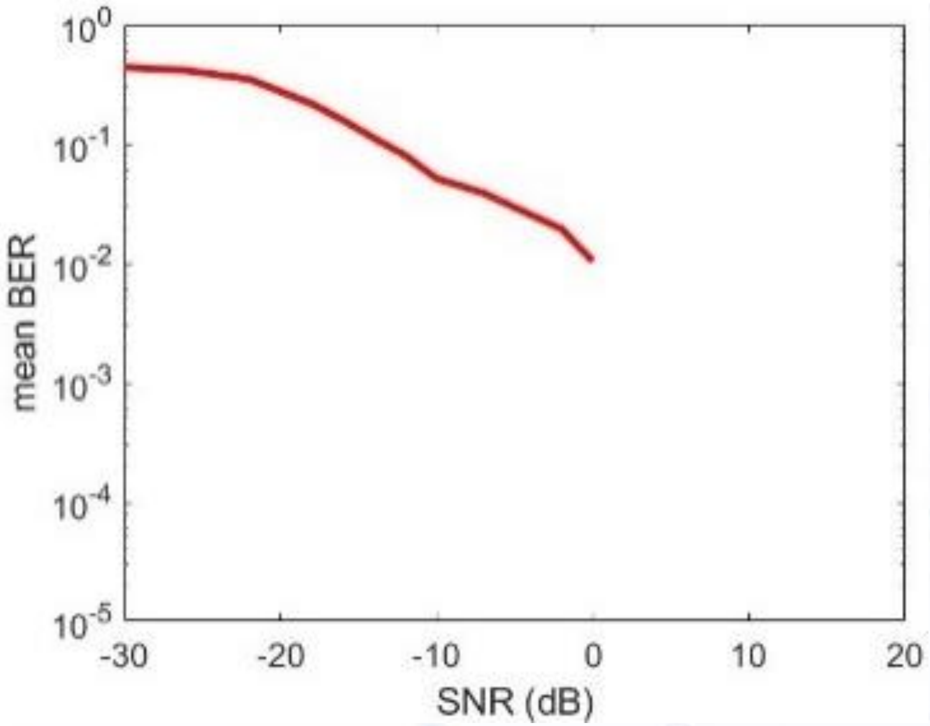
Mean PER for SF=7-12 and CR=1
Both Coherent and Non-Coherent Detection

LoRa Under Attack: Continuous Jamming

- Attacker transmits a continuous sine wave at 868MHz over an AWGN, for SF=7 and CR=1
- Considerable degradation in performance, around 50%.



No Jamming



Continuous Jamming

LoRa Under Attack: Reactive Jamming (1)

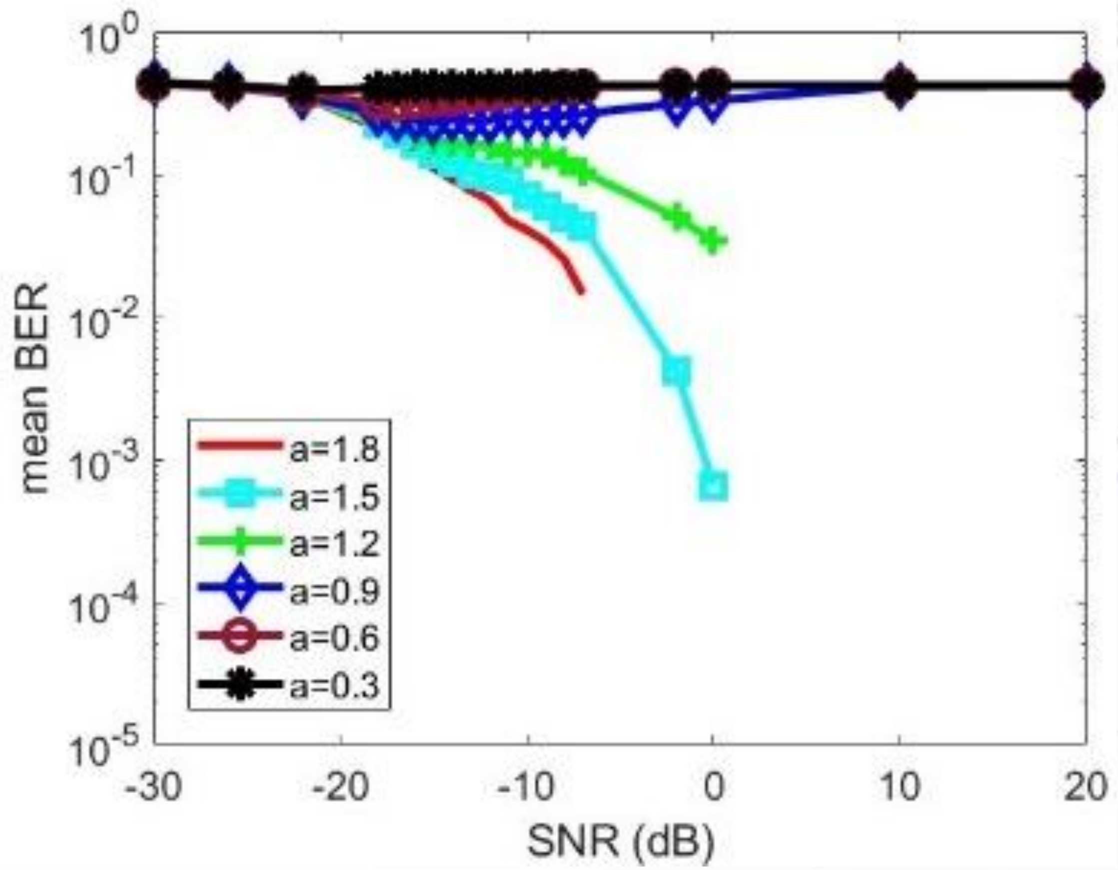
- Considering reactive jamming, the received signal at the gateway is given by:

$$y(t) = s_l(t) + s_a(t) + z(t),$$

where $y(t)$ is the received signal at the gateway, $s_l(t)$ is the CSS modulated LoRa signal transmitted by the legitimate LoRa sensor, $s_a(t)$ is the CSS modulated LoRa signal transmitted by the attacking node, and $z(t)$ represents the AWGN, with $z \in \mathcal{CN}(0, \sigma^2)$

- The ratio of the legitimate node's transmit power over the transmit power of the attacker is denoted by a. For $a < 0.9$ the systems "breaks", i.e. packets cannot be transmitted correctly.

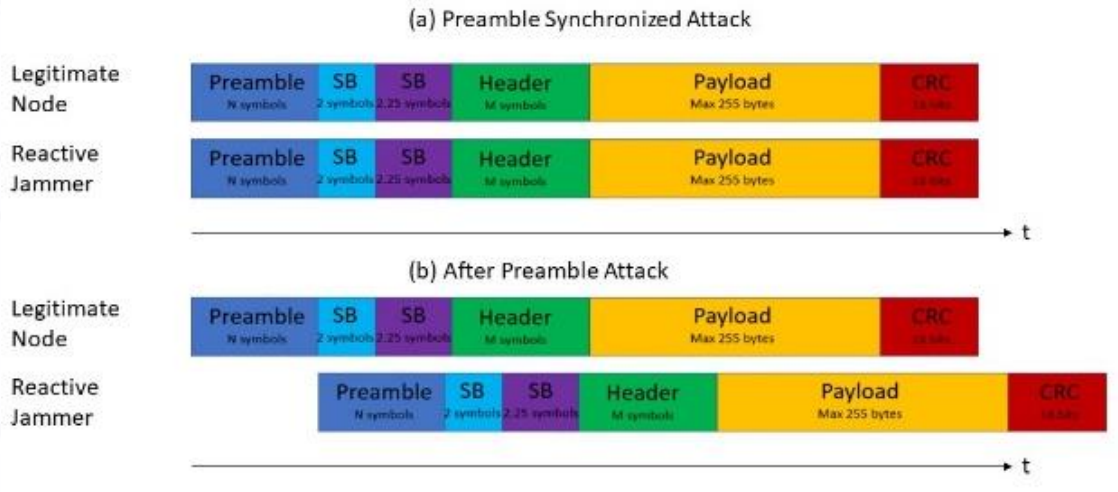
Mean BER for SF=7 and CR=1



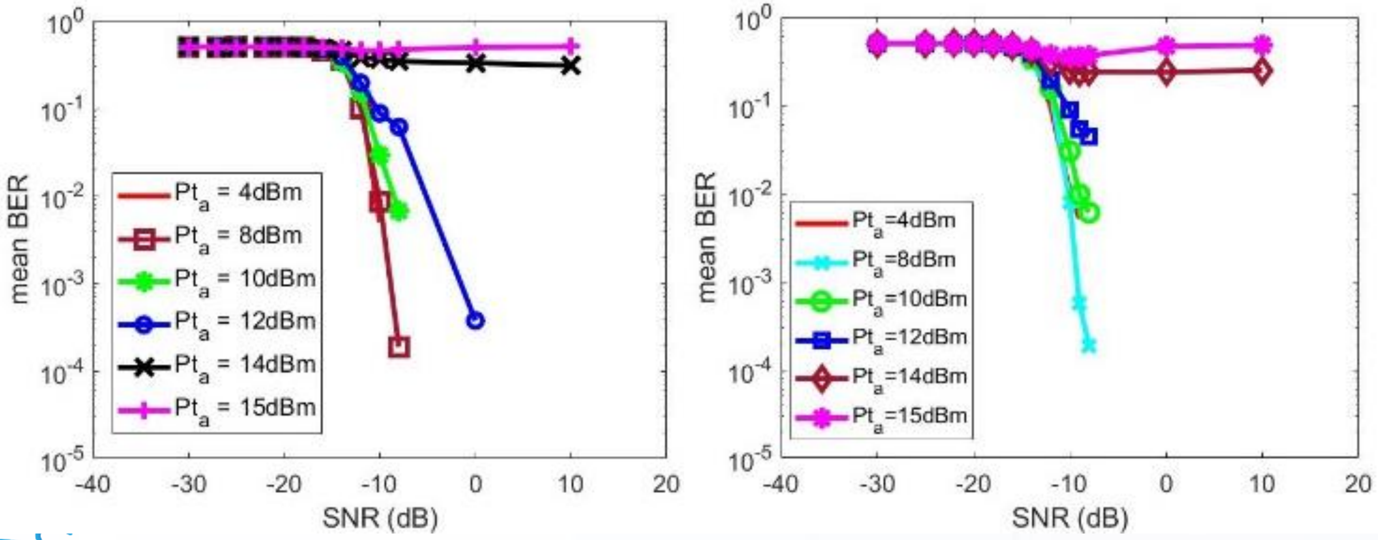
LoRa Under Attack: Reactive Jamming (2)

- Considering a reactive jamming attack performed:
  - a) in total frame synchronisation between the attacker and the legitimate node
  - b) right after the end of the preamble transmission from the legitimate node's end
- Attacker's transmit power varies from 4 to 15 dBm
- Legitimate node's transmit power = 12 dBm

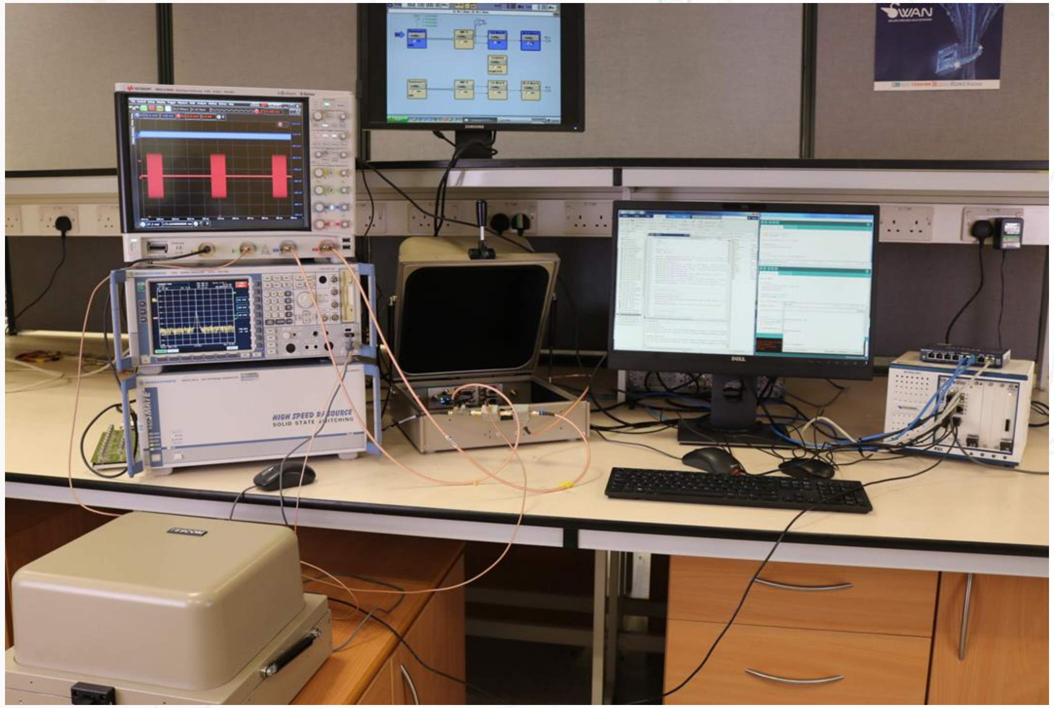
- When the attacker transmits at 13dBm or lower, a fairly good BER can be achieved.
- No major difference, on the performance, is observed if there is no total synchronisation between the transmissions of the attacking and the legitimate node.

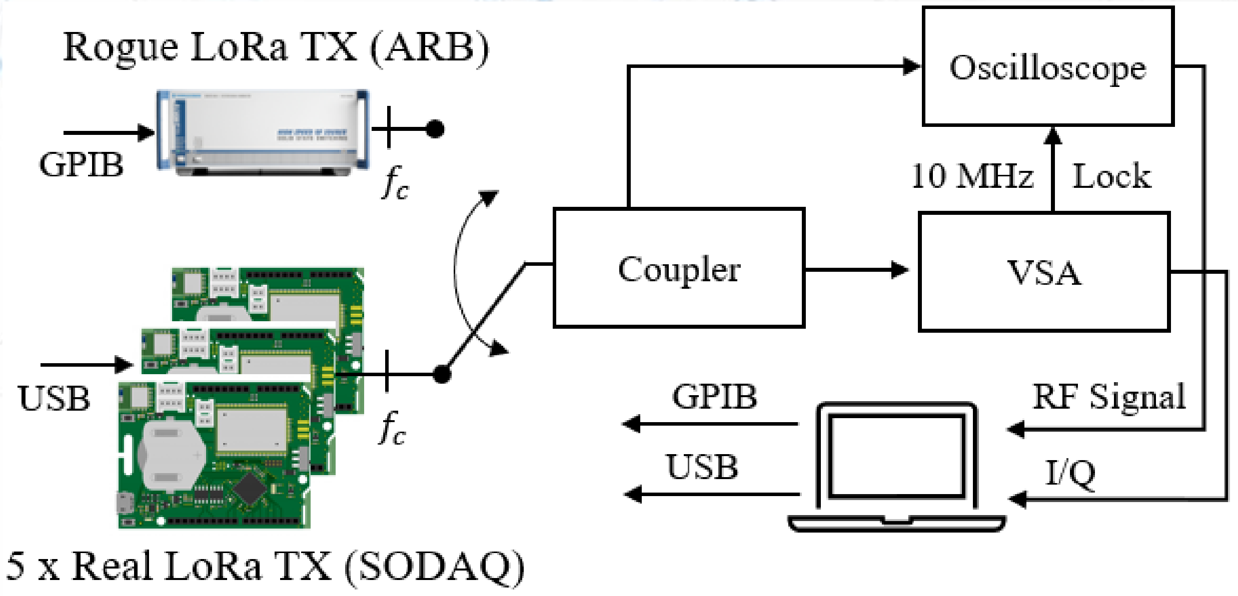


Mean BER for SF=7 and CR=1 for (a)left and (b)right



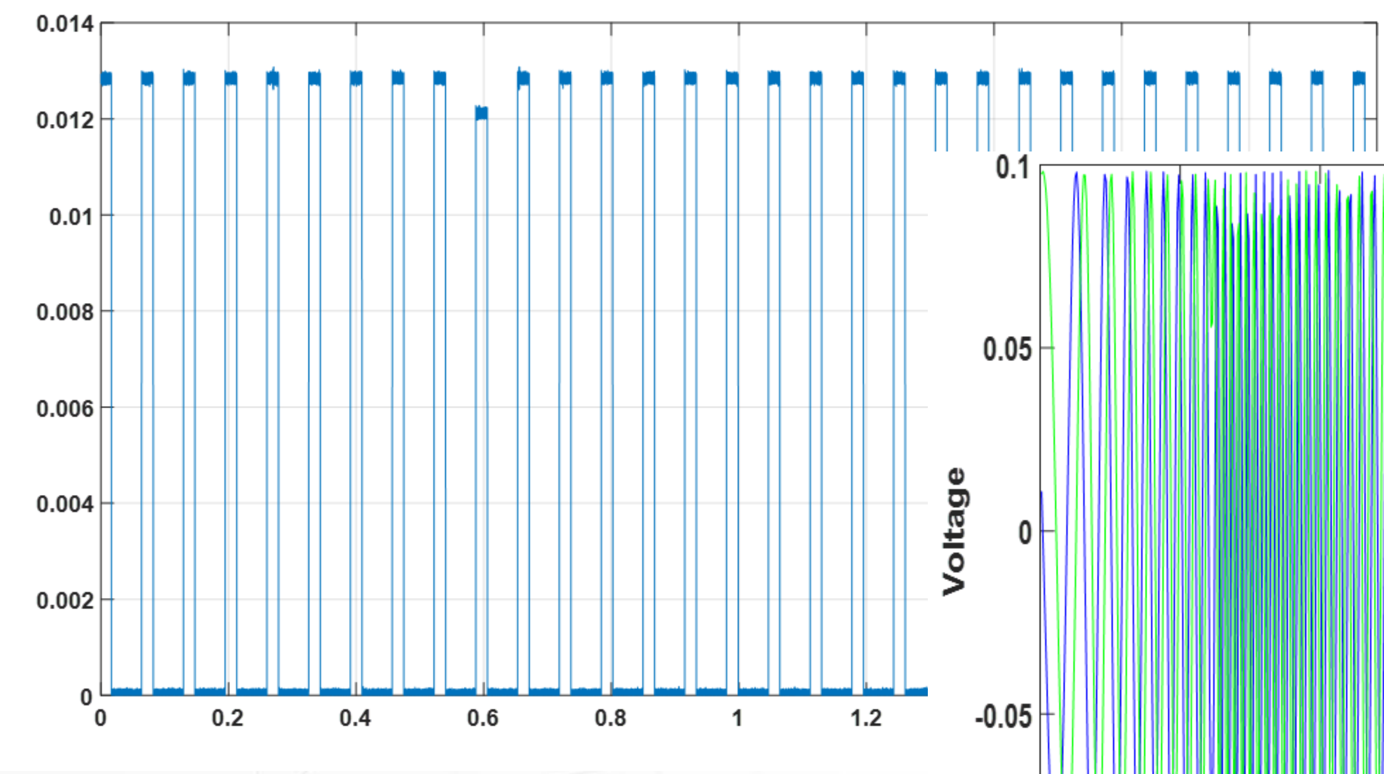
RF Penetration Testbed

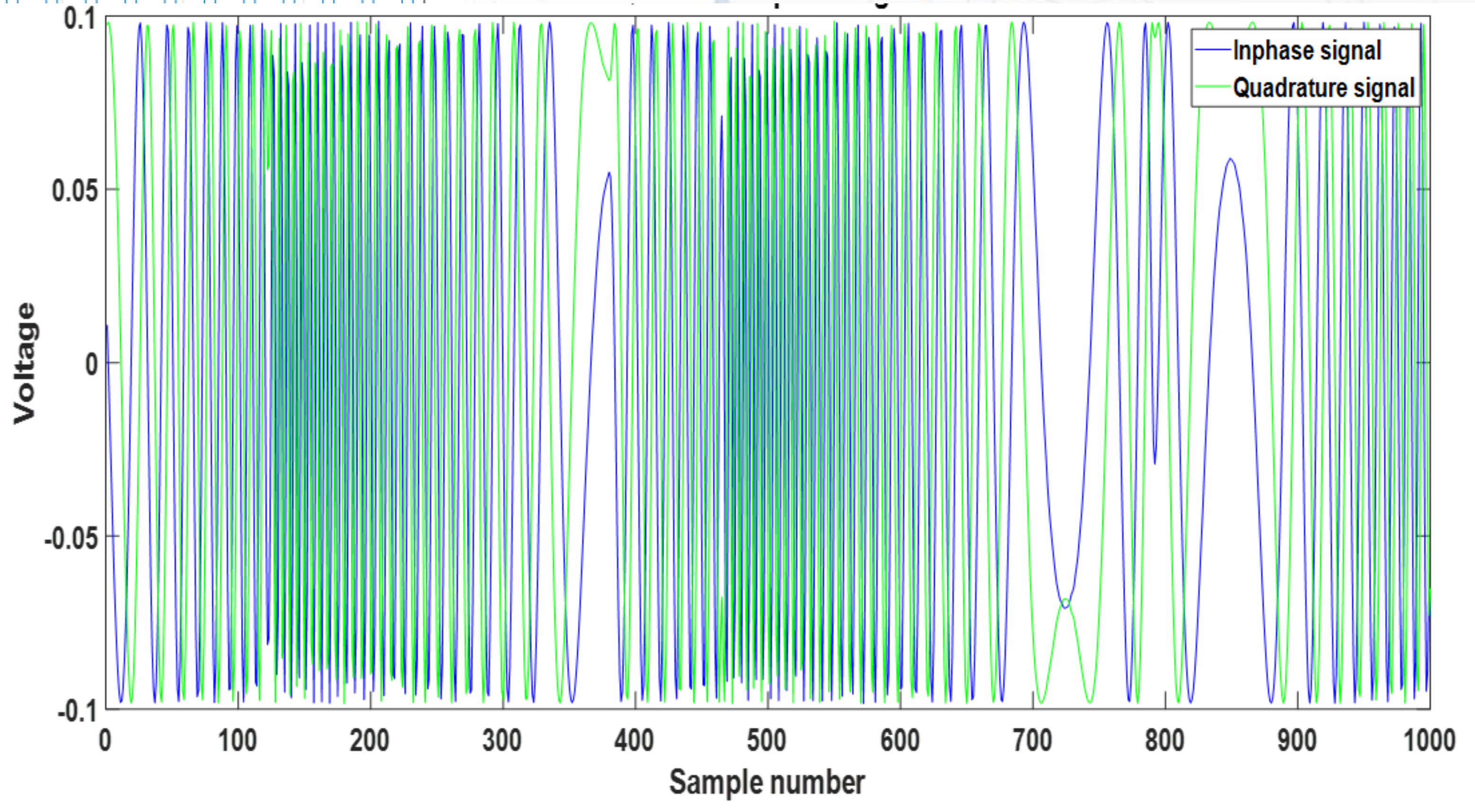




- Conductive Jamming Sensitivity Testing
  - Async & Sync waveforms
- Operational Link RF waveform capture

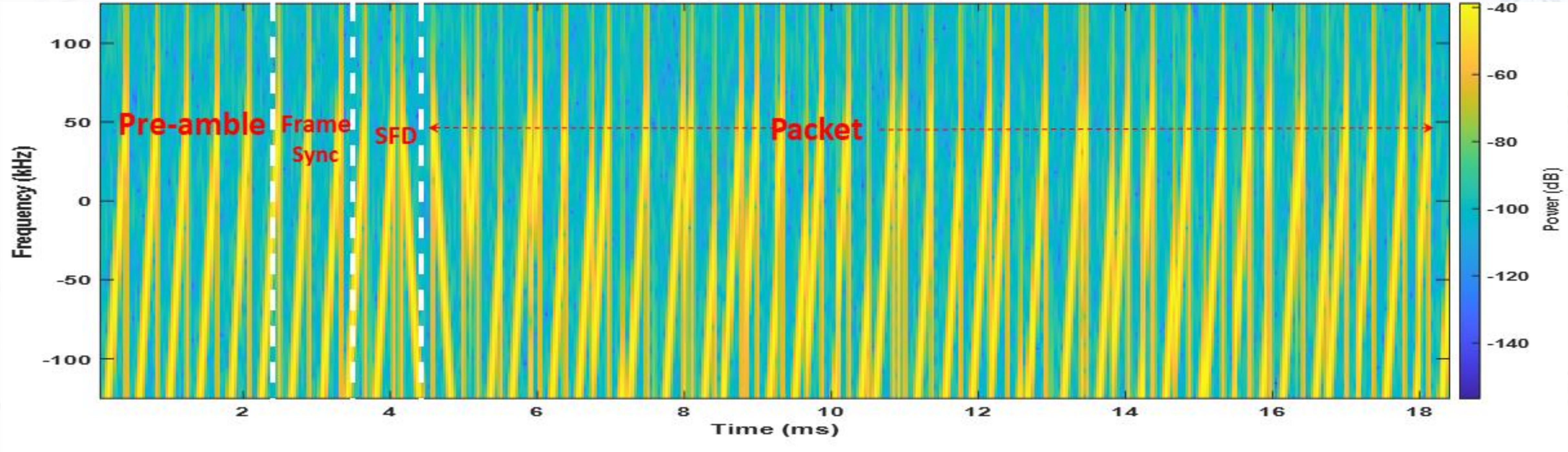
RF Capture and IQ Extraction



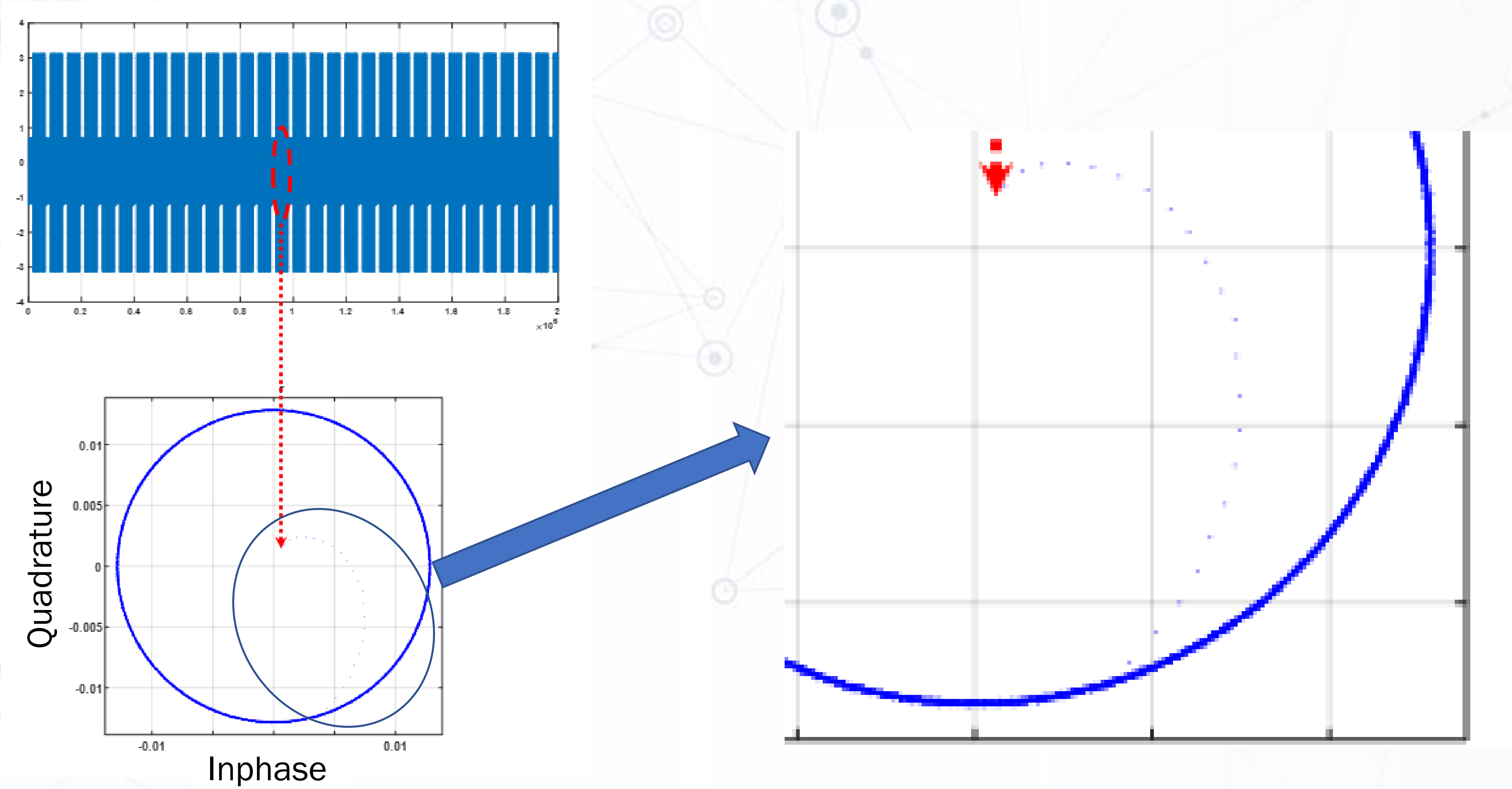


SECURE WIRELESS AGILE NETWORKS

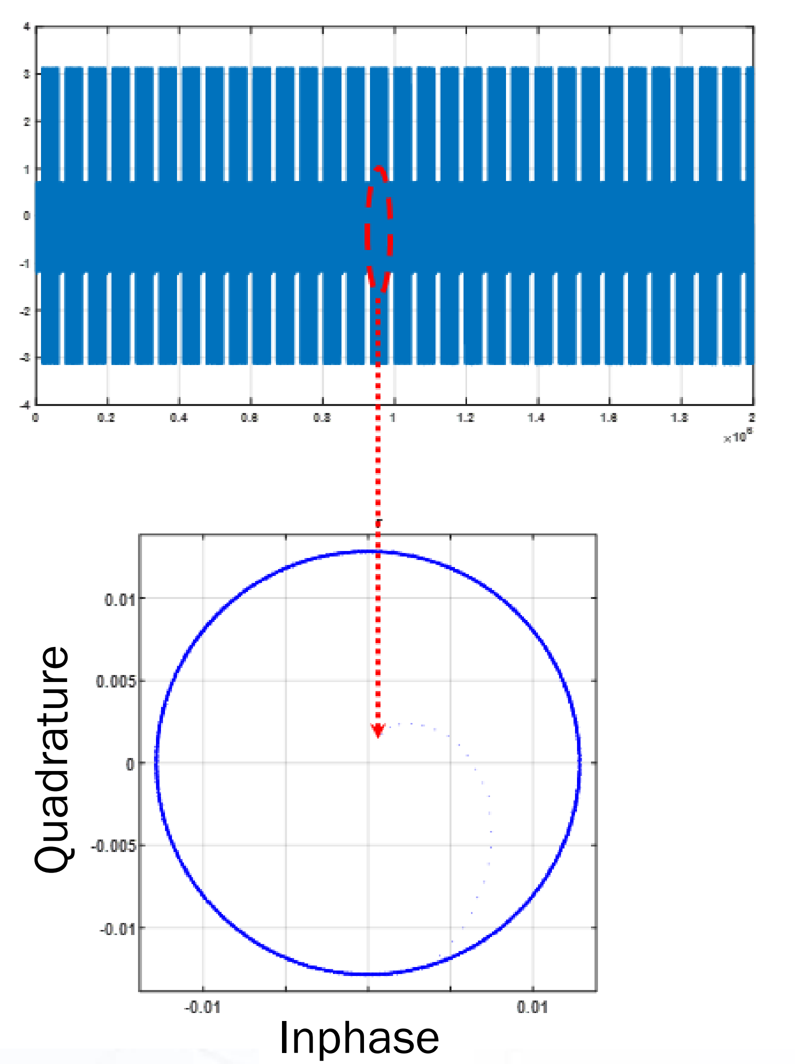
Frequency Domain Analysis

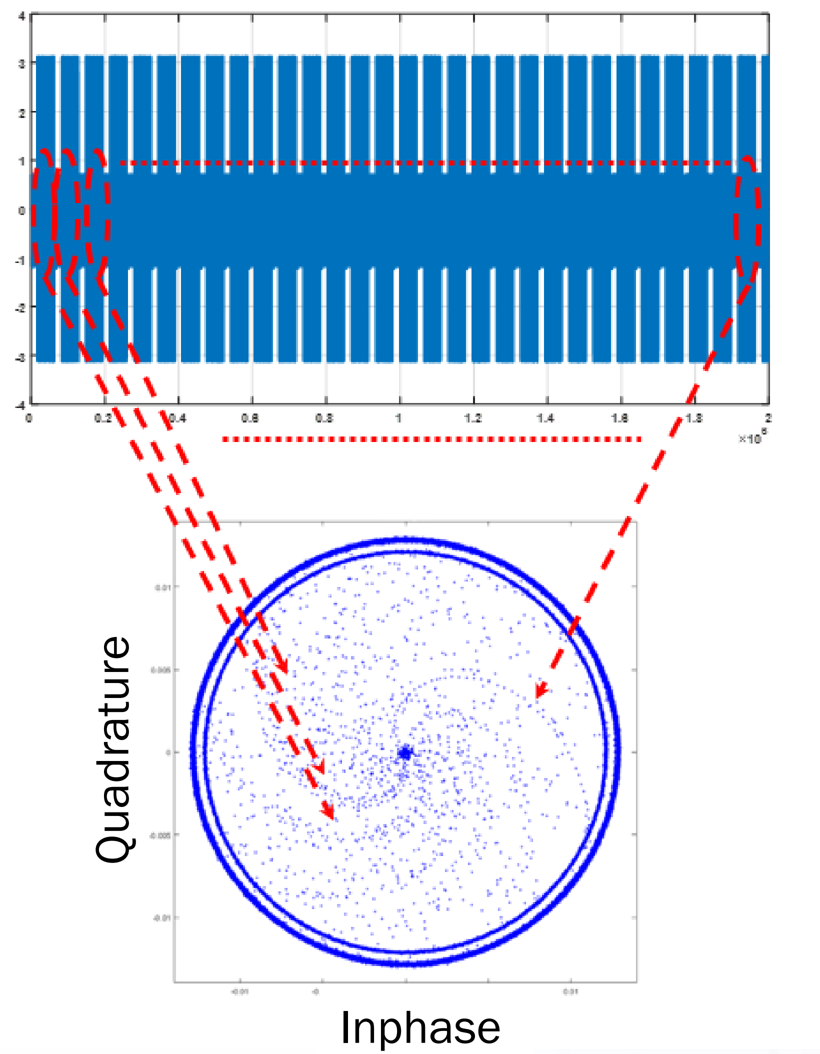


Time Domain Chirp Analysis



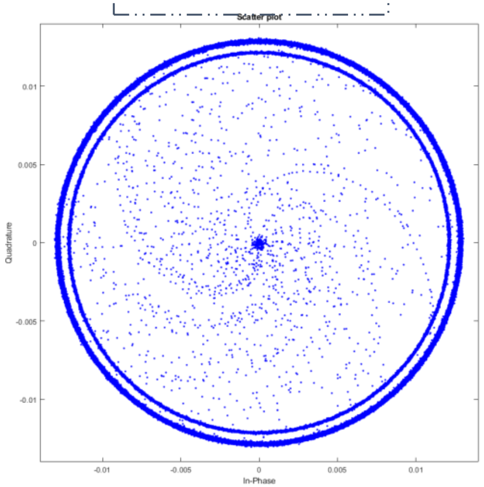
Time Domain Chirp Analysis



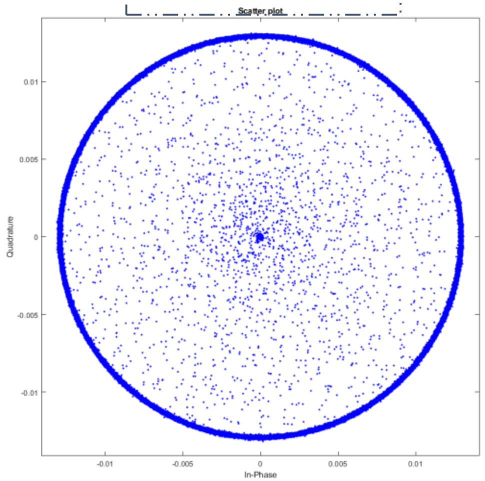


Multi-sensor Time Domain

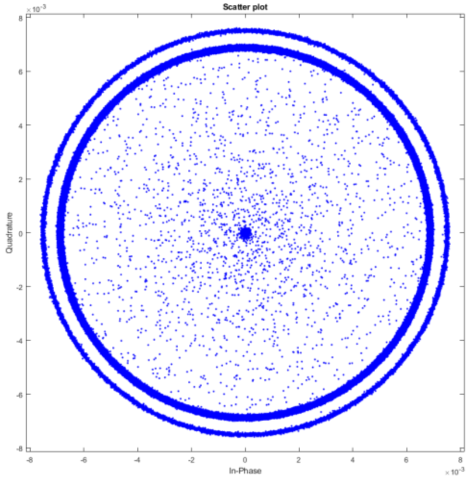
SODAQ-A



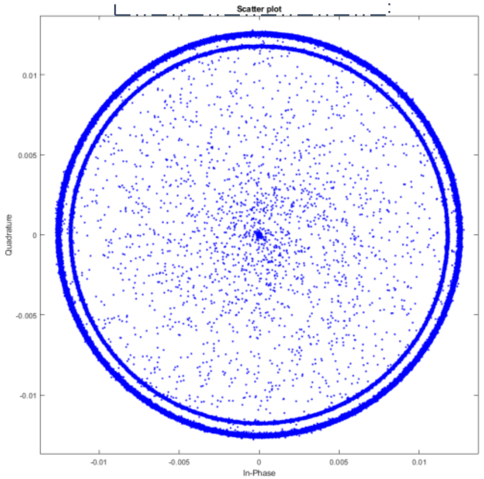
SODAQ-B



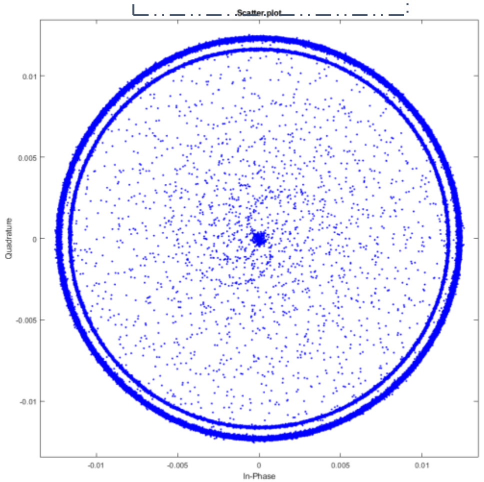
SODAQ-C



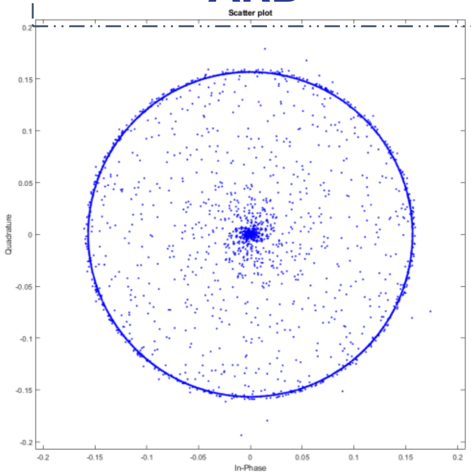
SODAQ-D



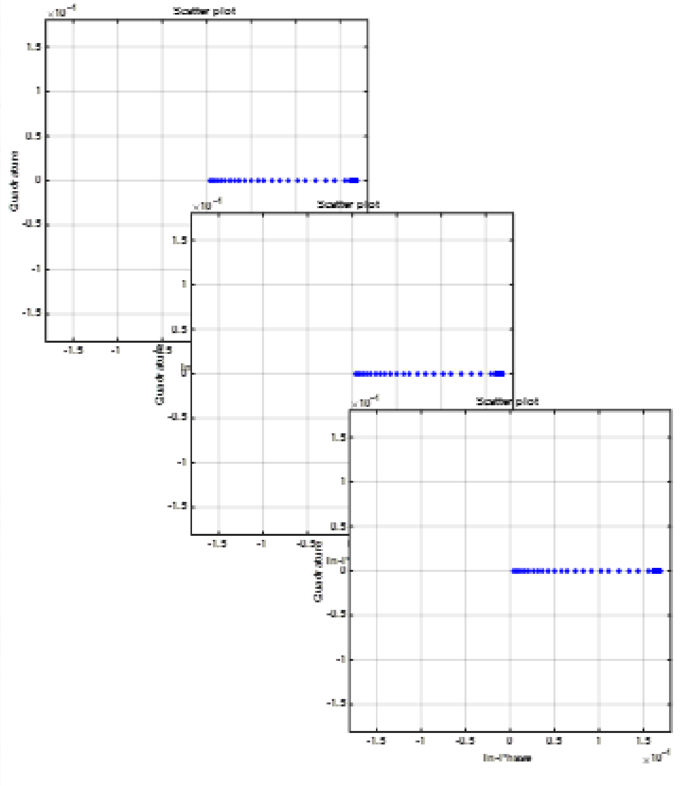
SODAQ-E

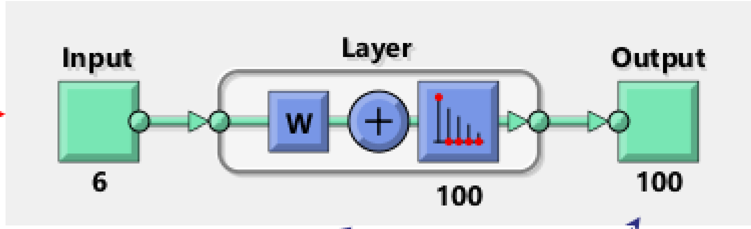


ARB



Neural Network Analysis



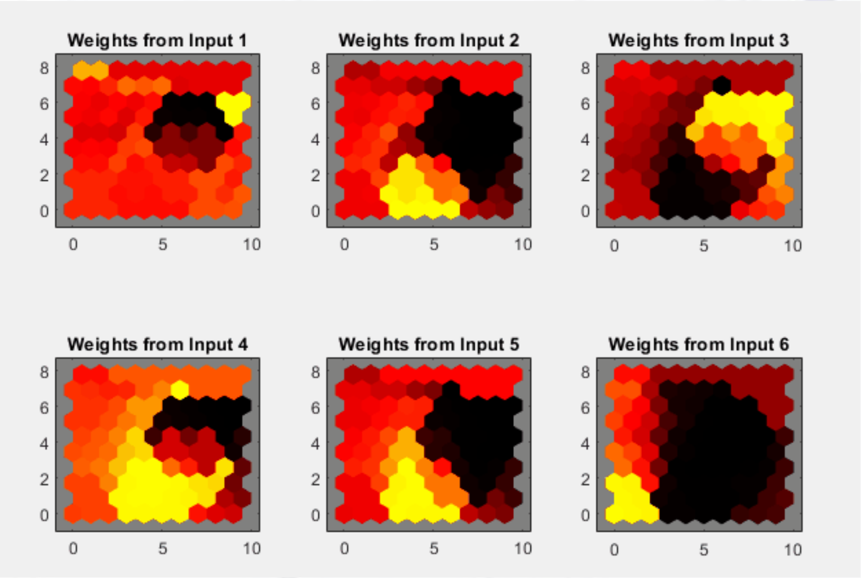


$6x[1x16270]^H$
High Dimensional
Input Matrix

[6x10]
Input
Weight
Matrix

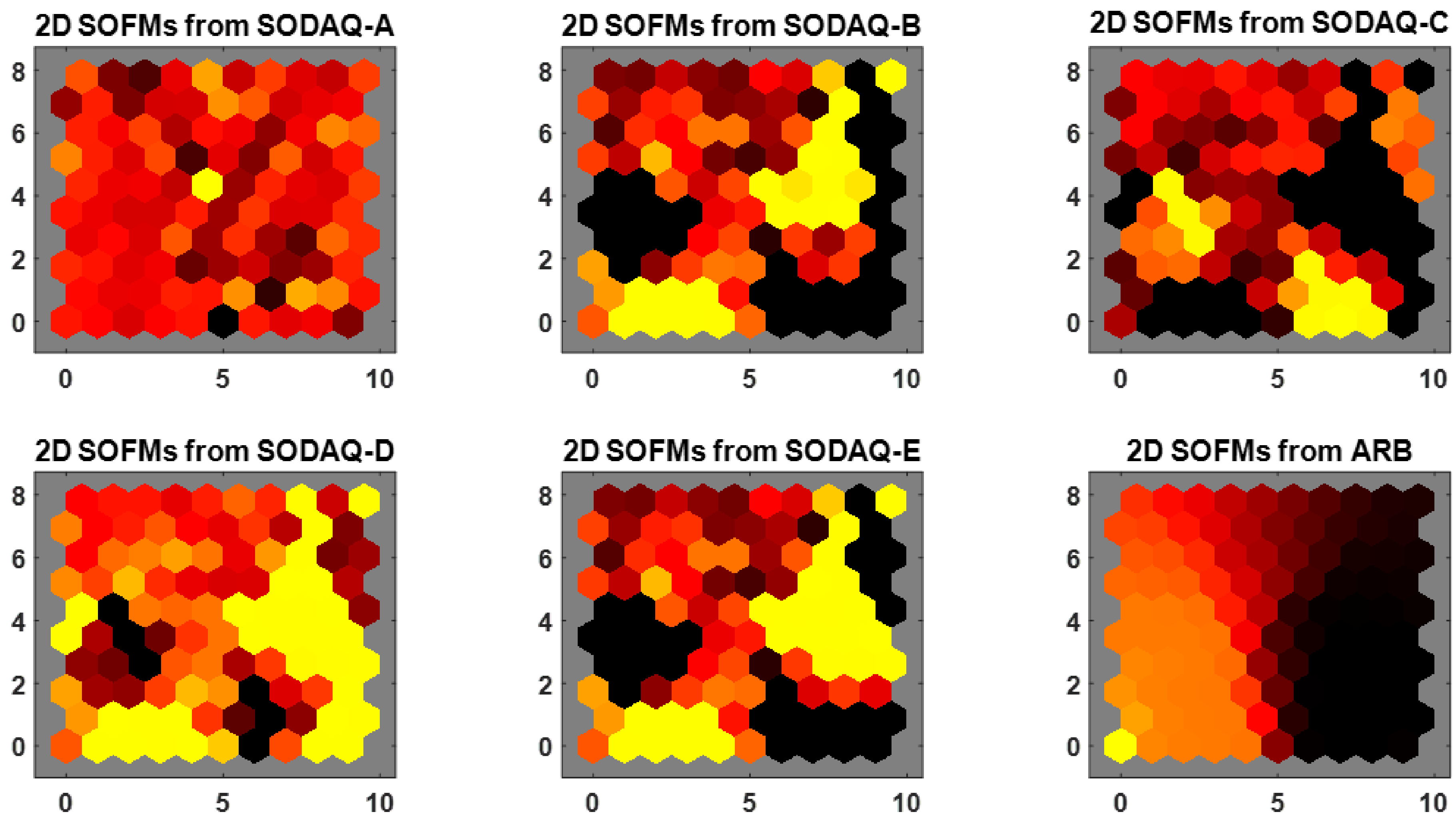
$[6x\{10x1^H, \cdots, 10x1^H\}]^H$
$=6x[10X10]$
Kohonen
(NN) Layer Matrix

2D Self-Organising Feature Maps (SOFM)

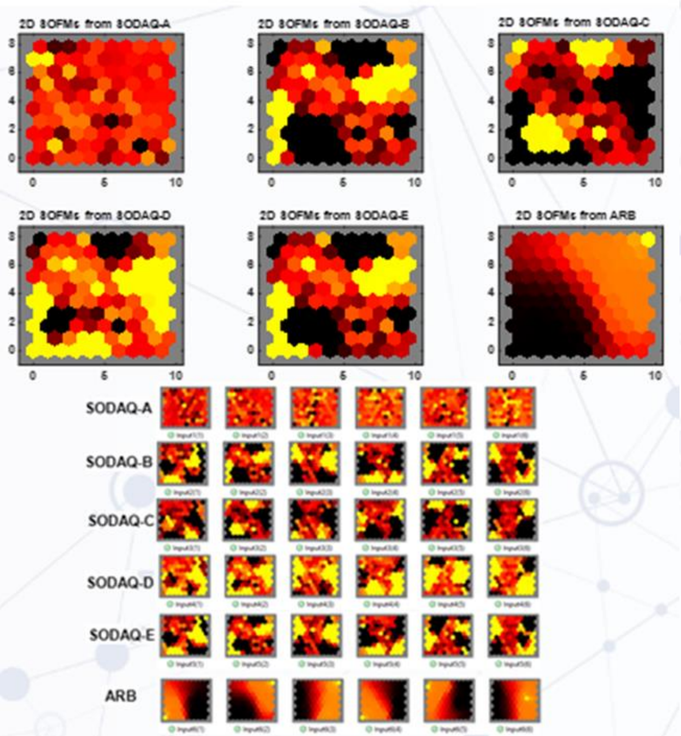


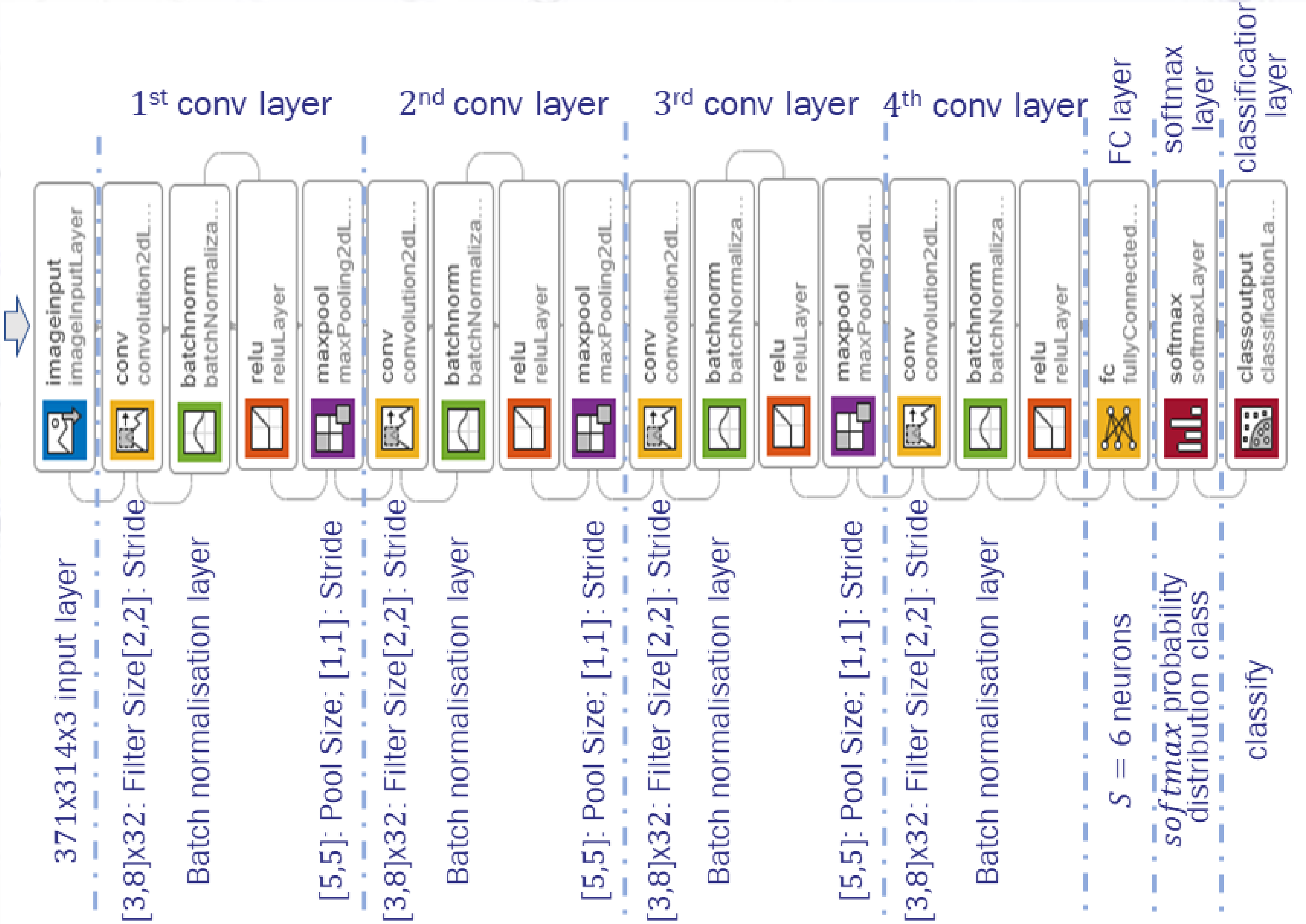
$6x[10X10]$
Low Dimensional Output Layer

Self Organising Feature Maps

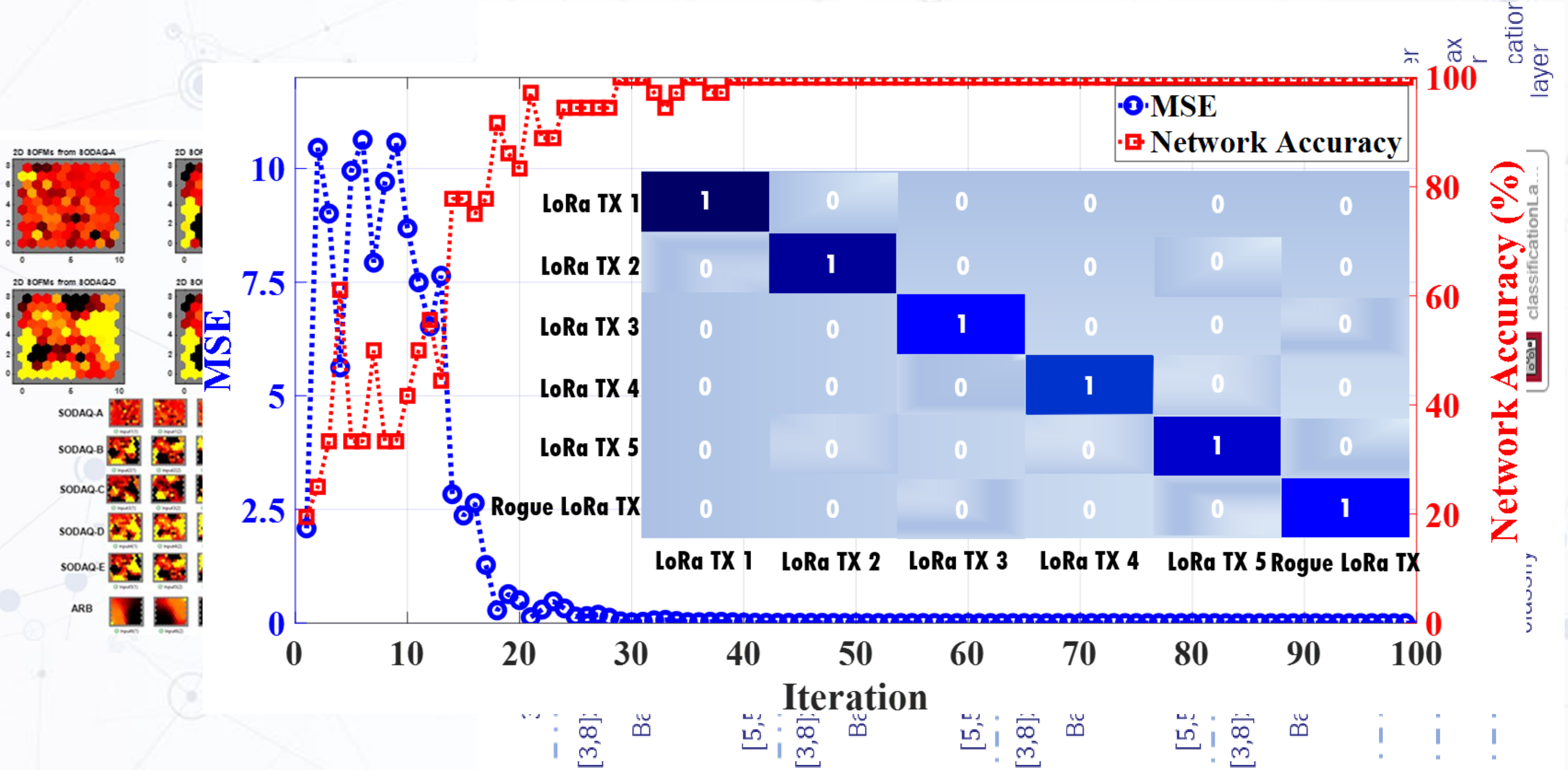


Convolutional Neural Network





Unique Device Identification



Take Aways:

- **Low cost IoT within critical infrastructures requires protection from adversaries**
  - Async jamming can reduce performance by circa 50%
  - Reactive jamming: Impact only when tx power greater than subject device
- **SWAN has proposed a robust RF fingerprinting methodology for LoRa**
  - Extracts classifiable features from real-world devices with apparently correlated electrical features
  - Unsupervised ML generates self-organizing maps [SOMs] and convolutional neutral networks [CNN] then provide the necessary orthogonal separation

Next Steps:

- **Inclusion (and separation) of the composite antenna and propagating channel**
- **Deployment within Bristol's external LoRa testbed**
- **Extension to 4G & 5G Smart phones and modems**

IMS
Connecting Minds. Exchanging Ideas.

EXPLORE THE PEAKS OF MICROWAVE ENGINEERING
DENVER2022

Sign-up here:

swan-programme@bristol.ac.uk

www.swan-partnership.ac.uk

@PartnershipSWAN