DLR: DEEP DELAY LOOP RESERVOIR COMPUTING

Silvija Kokalj-Filipovic, Paul Toliver, William Johnson - Perspecta Labs
Raymond Hoare, Joseph Jezak, Joseph St. Onge - Concurrent EDA (sub)

AIE: PHOTONIC EDGE AI COMPACT HARDWARE (PEACH)

Artificial Intelligence

Background:

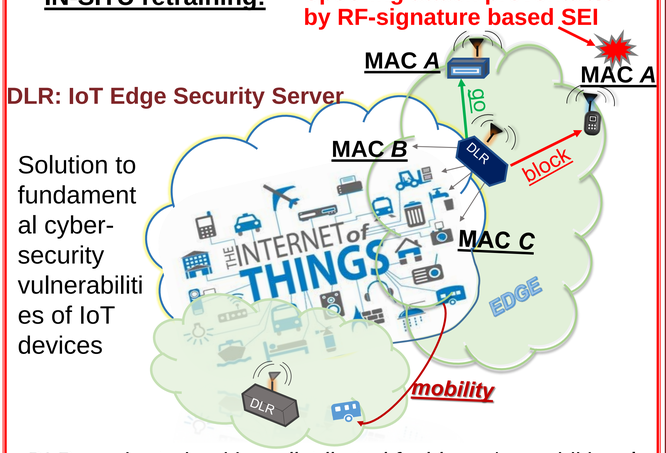
RF fingerprinting for Authentication in Internet of Things (IoT)

- **Specific Emitter Identification (SEI)** exploits fingerprints of emitters to distinguish one RF device from another using AI
- **AI-Based SEI Benefits**:
  - More secure for signal authentication than media access control (MAC) addresses
  - Decreases overhead, saves bandwidth in comms w/ short messages (machine to machine, or tactical gray-zone comms) if MAC address dropped completely
- State-of-the-Art: training AI-based SEI requires big servers; no traditional in-situ, real time training exists
- **DLR** enables mobile edge platforms to use SEI to track and authenticate signals with FAST (3sec) low-SWaP retraining

DLR: ad-hoc tracking of RF devices/ attack detection

IN-SITU retraining!

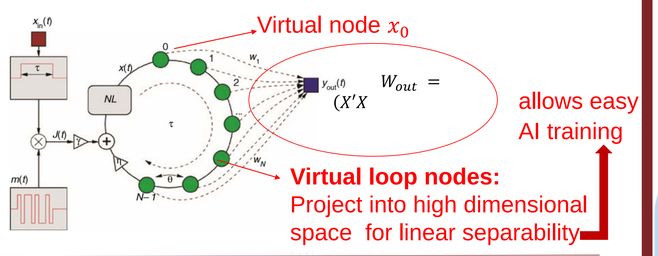
Spoofing attack preventable by RF-signature based SEI

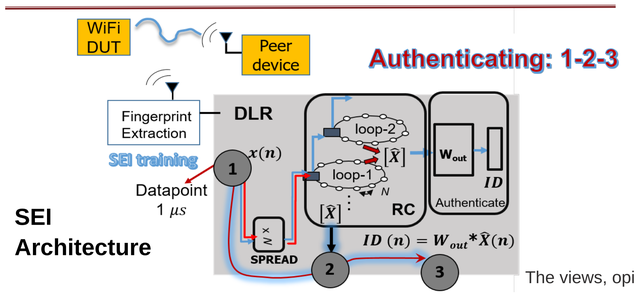


Solution to fundamental cyber-security vulnerabilities of IoT devices

DLR can be trained in a *distributed fashion* w/ no additional power consumption & w/ modest drop in accuracy to authenticate mobile IoT devices across large regions

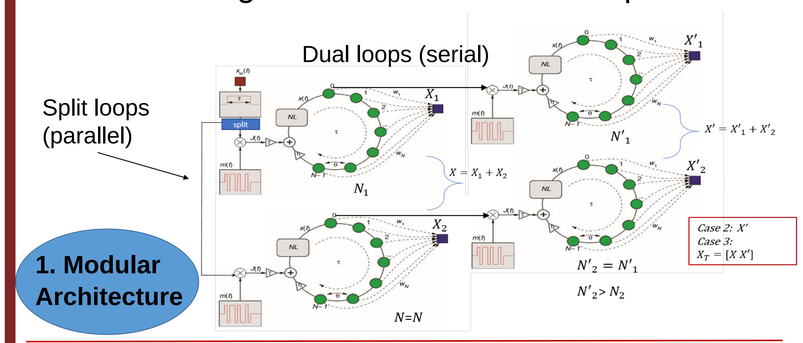
Loop Reservoir: 1 neuron replaces N neurons for traditional recurrent neural nets (RNN) – AI with less resources!





Approach:

Flexible Loop Based Architectures for IoT Devices – Digital or Photonic Loop

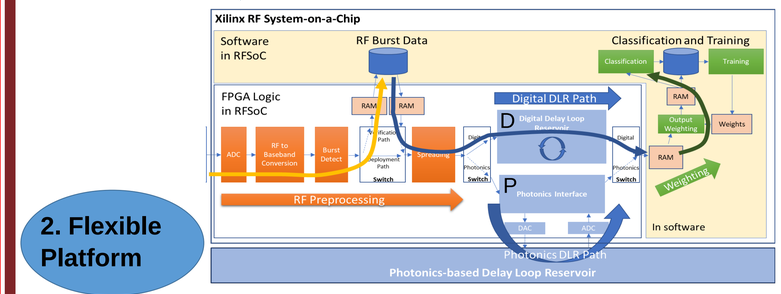


RFSoC based platform with a switch between digital (D) and photonic (P) loop

Platform Features

1. Live Capture and Storage of Emitted Signals
2. Real-time or Offline training

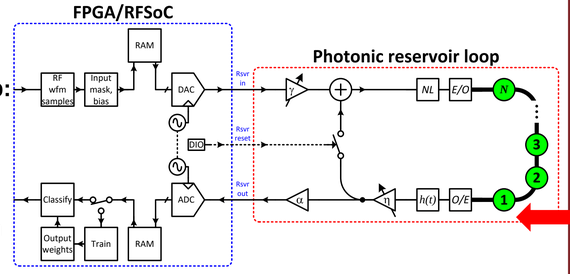
- DLR can be sourced with either live captured data (real-time training and classification) or from previously captured files (repeatable performance verification)



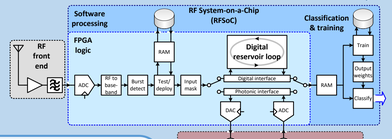
Mixed Digital+Photonic Hardware

Photonic delay loop:

- *N virtual nodes*
- Sinusoidal neuron
- Filter for node coupling
- Wavelength division multiplexing

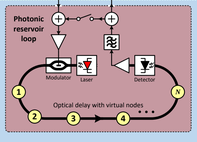


PEACH lab prototype

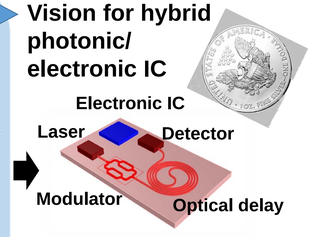


2 selectable DLR implementations:

- FPGA-based
- Photonics-based



Vision for hybrid photonic/ electronic IC

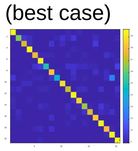


Capacity scaling through *wavelength, time, and spatial multiplexing*

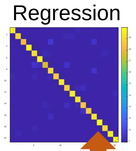
Results

SEI of 20 WiFi devices: Comparison with SoA (State-of-the-Art) Deep Neural Nets - Residual (ResNet) & Recurrent (RNN) - expressed by FOMs

Ridge Regression (best case)



DLR: RC + Ridge Regression

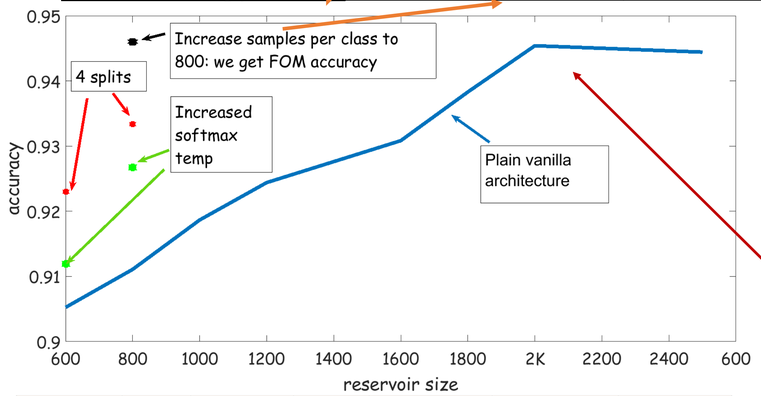


Figures of Merit (FOMs)	
Spatial Reduction FOM $= \frac{M_{RNN}}{M_{DLR}} \approx 20$	M_x = memory reqs
H/W Compl. Red. FOM $= \frac{C_{RNN}}{C_{DLR}} \approx 100$	C_x = complexity (# of MACs)
Latency Red. FOM $= \frac{\Delta_{RNN}}{\Delta_{DLR}} \approx 1200$	Δ_x = latency(s)

§: may improve further

DLR achieved accuracy of the most complex SoA NNs w/ total H/W reduction factor of >2K in the training phase

	S/W implement.	Accuracy %	# of params (memory M)	Complexity C	Latency Δ
	ResNet	94.5	214K x 20	$>5*10^{11}$ x 100	
	LSTM RNN	91	210K x 20	$5*10^{11}$ x 100	> 1h x 1200
	PEACH DLR	**>94.5**	Q*N=12K	$5*10^{9}$	~ 3s §



Using architectural combinations of loops we match the accuracy of a large network while staying in the low SWaP

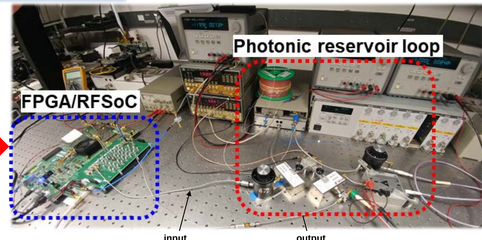
Proof that projection into higher dimensional space helps learning

DLR Architecture N=600, b=600	2 splits	2 splits plus increased temperature	4 splits	4 splits plus increased temperature	8 splits plus increased temperature	Combined multiple loops (2 layers 4 splits)
Accuracy	0.905 ↗	0.912 ↗	0.923 ↗	0.928 ↗	0.915 ↘	0.912 ↘
Power	$C*10^9$	$C*10^9$	$C*10^9$	$C*10^9$	$C*10^9$	$C*10^9$

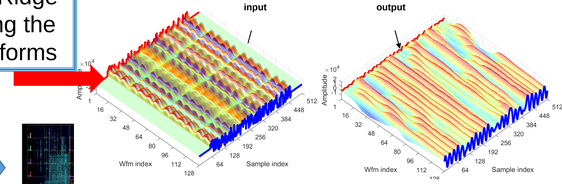
Comment: < 50 samples in 1 loop fails to capture temporal memory of the signature

Same reservoir size, different loop architectures move average accuracy up and down 3%

The results above have been achieved on the FPGA implementation of the loop (fully digital DLR)
The **calibration of the photonic loop** to match these results is currently under way (mixed signal DLR)



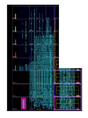
Efficient realization of RF capture, preprocessing, Ridge training allow for accelerated feedback in calibrating the photonic loop on the level of SEI accuracy & waveforms



Reservoir waveforms

Acceleration of Discovery and Training

MATLAB → Python → Python w/C Kernels → Concurrent EDA's Synthesis Tools →



hours → 35 minutes → 3 seconds 325-900 faster

Classification << ms

Demo ready!

This research was developed with funding from the Defense Advanced Research Projects Agency (DARPA).
The views, opinions and/or findings expressed are those of the author and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government.
Distribution Statement A – Approved for Public Release, Distribution Unlimited