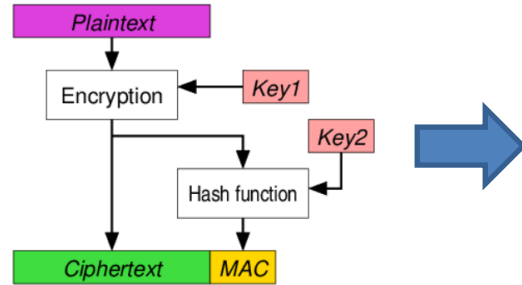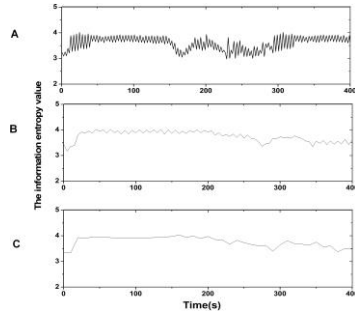# Hardware-In-The-Loop Emulator For In-Vehicle Controller Area Networks
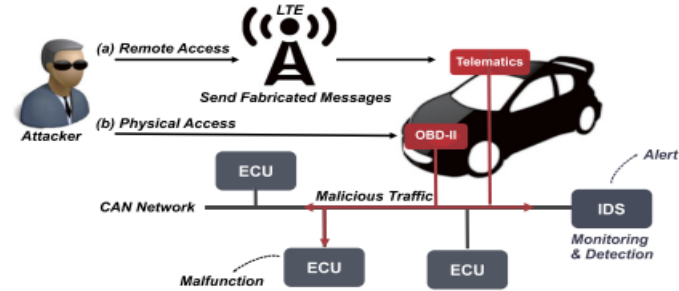
Trinity College Dublin

Date 01/05/2024

Backgrounds

CAN bus attack prevention

**Traditional Detection & Encryption**

IDS & DNN detection

Neural networks have greatly improved attack detection performance,

**But how to deal with** flexible system changes and long development cycle

Method	Precision (%)		Recall (%)		F1-Score (%)	
	Known	New	Known	New	Known	New
OCSVM	35.43	10.83	71.15	35.12	47.30	16.55
IF	43.58	15.62	73.42	31.56	54.69	20.90
OTIDS	**99.82**	70.81	71.68	42.01	83.44	52.73
RNN+Heuristics	98.69	70.25	**99.49**	50.53	**99.09**	58.78
CANTransfer	94.93	**87.97**	95.57	**88.97**	95.25	**88.47**
Gain	-4.89	**17.16**	-3.92	**38.44**	-3.84	**26.69**

System Structure
Structure and features
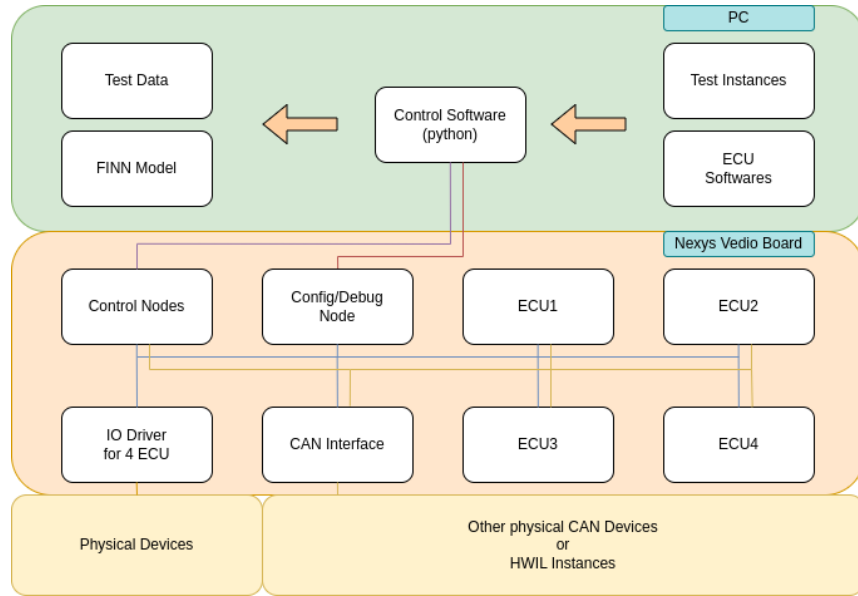
System Structue
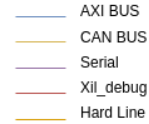
- **Flexible nodes(type, scale)**
- **Physical device access**
- **Automatic testing**
- **Complete tool chain**

Network Change	Test&Data	Model Deployment
Software Define	**Auto Annotation**	**FINN Tool chain**

Accelerate Deployment

Software Platform

Functions and features
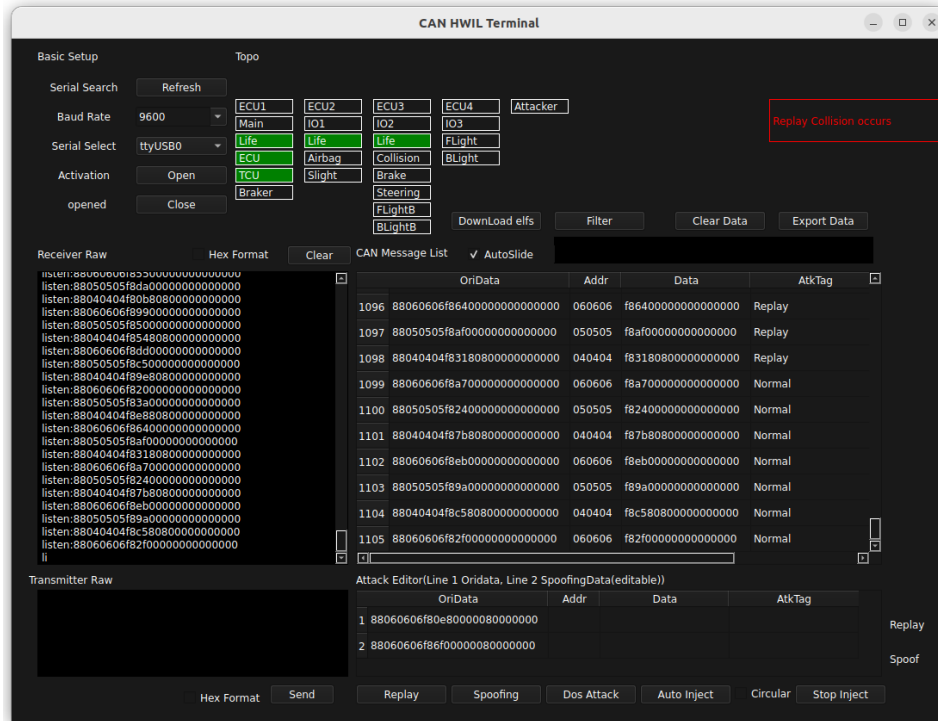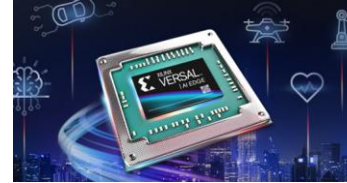
Complete Solution

Empower the Automotive safety
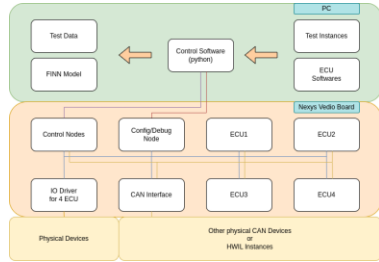
Flexible
HWIL Emulator
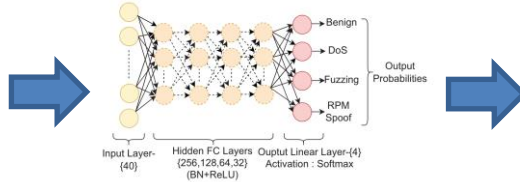
High-Performance
QNN Accelerators

Deployable
Stitched IP for Edge

Flexibly Changeable System Structure

Complete CAN bus Test & Detection Solution → Empower → **Automotive Safety**

Brevitas **FINN**

Attack	Model	Precision	Recall	F1	FNR
DoS	GIDS [30]	-	99.9	-	-
	DCNN [13]	100	99.89	99.95	0.13
	MLIDS [36]	99.9	100	99.9	-
	G-IDCS [28]	99.81	98.86	99.33	-
	TAN-IDS [29]	100	100	100	-
	HyDL-IDS [33]	100	100	100	0
	NovelADS [32]	99.97	99.91	99.94	-
	TCAN-IDS [31]	100	99.97	99.98	-
	iForest [35]	-	-	-	-
	GRU [34]	99.93	99.91	99.92	-
	CQMLP-IDS	99.92	99.88	99.90	0.11
Fuzzing	GIDS [30]	-	98.7	-	-
	DCNN [13]	99.95	99.65	99.80	0.5
	MLIDS [36]	99.9	99.9	99.9	-
	G-IDCS [28]	99.71	99	99.35	-
	TAN-IDS [29]	99.99	99.99	99.99	-
	HyDL-IDS [33]	99.98	99.88	99.93	-
	NovelADS [32]	99.99	100	100	-
	TCAN-IDS [31]	99.99	99.89	99.22	-
	iForest [35]	95.07	99.93	97.44	-
	GRU [34]	99.32	99.13	99.22	-
	CQMLP-IDS	99.93	99.69	99.81	0.27
RPM-Spoof	GIDS [30]	-	99.6	-	-
	DCNN [13]	99.99	99.94	99.96	0.05
	MLIDS [36]	100	100	100	-
	G-IDCS [28]	99.85	98.69	99.27	-
	TAN-IDS [29]	99.99	99.93	99.96	-
	HyDL-IDS [33]	100	100	100	0
	NovelADS [32]	99.9	99.9	99.9	-
	TCAN-IDS [31]	99.9	99.9	99.9	-
	iForest [35]	98.9	99.9	99.4	-
	CQMLP-IDS	99.96	100	99.98	0

Model Performance

Thank You