ASIA SOUTH PACIFIC DESIGN AUTOMATION CONFERENCE

Colorado State University

TENET: Temporal CNN with Attention for Anomaly Detection in Automotive Cyber-Physical Systems

Sooryaa Vignesh Thiruloga, Vipin Kumar Kukkala, Sudeep Pasricha
Department of Electrical and Computer Engineering
Colorado State University, Fort Collins, CO, USA
{sooryaa, vipin.kukkala, sudeep}@colostate.edu

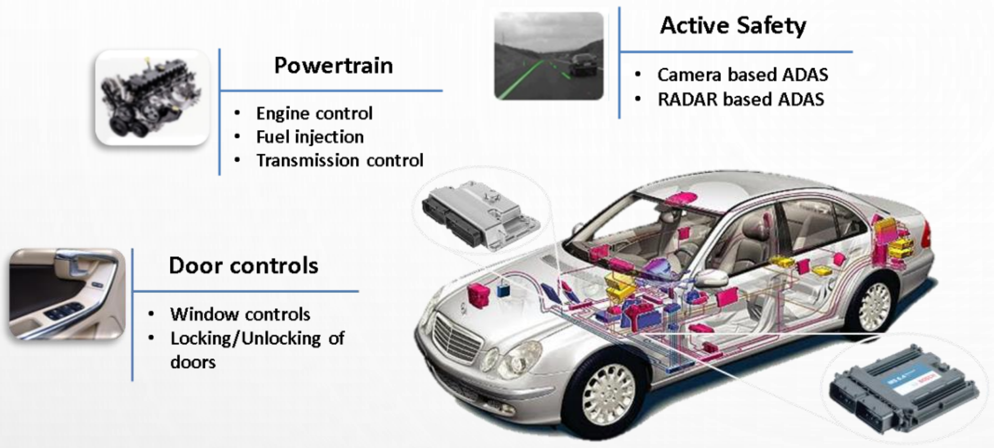
SPONSORS

acm · SIGDA · CEDA (IEEE Council on Electronic Design Automation) · CAS · IEEE · NSF

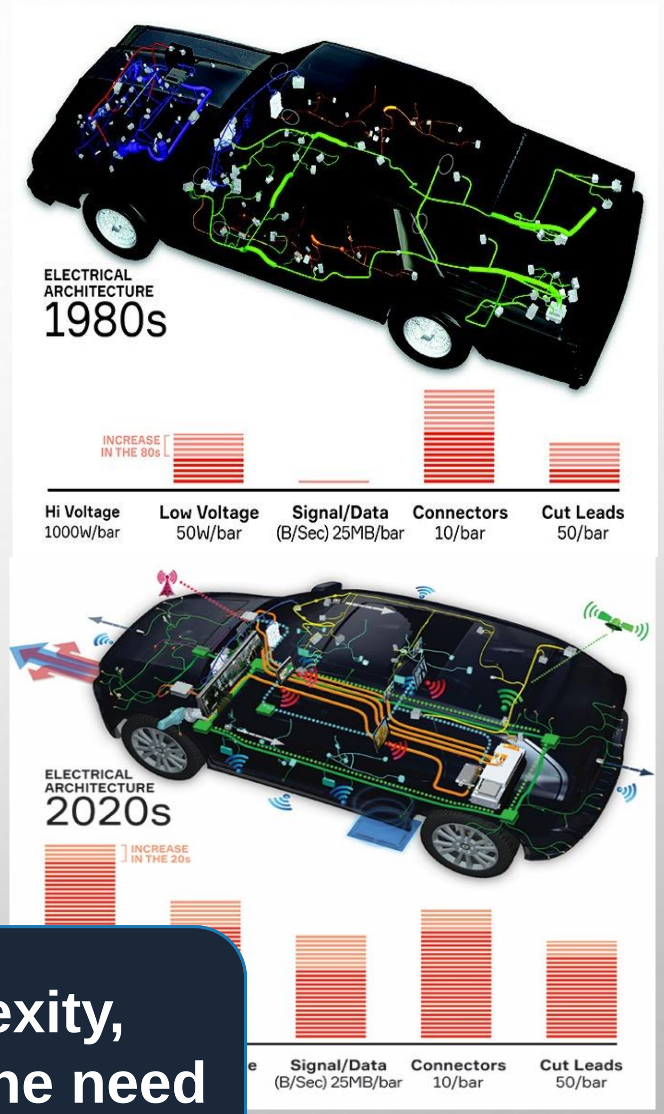
Outline

- Introduction to Automotive Systems
- Prior Work
- Our Contributions
- TENET Framework Overview
- Experimental Results
- Conclusion

Introduction to Automotive Systems



- Electronic control unit (ECU)
  - Engine control, Transmission control, Perception control etc.
- Automotive systems are becoming more complex to achieve autonomy
  - Electrical architecture of vehicles in 1980s vs 2020s.



[Source: https://www.aptiv.com/insights/article/evolution-of-vehicle-architecture]

With increasing automotive CPS complexity, attack surface also increases, motivating the need for powerful new Anomaly Detection solutions

Anomaly Detection Approaches

- **Traditional methods**
  - Firewalls fail to provide protection from complex attacks
  - Rule based approaches fail to detect novel attack patterns
- **AI based anomaly detection system (ADS)**
  - AI based ADSs are effective in learning complex patterns
  - Detect both known and novel attacks
  - Abundance of in-vehicle data
  - Increasing computation capabilities of ECU

AI based ADS provides a viable solution for anomaly detection

Relevant Prior Work

- **[M. Weber et al., 2018]**
  - Proposed a recurrent r … o learn the normal operating behavior of t … ts inputs
  - Fails to detect complex … cks

Detect novel / complex attacks

Low memory footprint

- **[M. O. Ezeme et al., 201**
  - Proposed a LSTM bas … ention mechanism along with a Kernel De … nomaly detection
  - Memory intensive and … d

Low detection latency

High reliability

- **[V. Kukkala et al., 2020**
  - Proposed a gated recu … r model
  - Uses a static thresholding technique, will miss attacks below the threshold value

Our Contributions

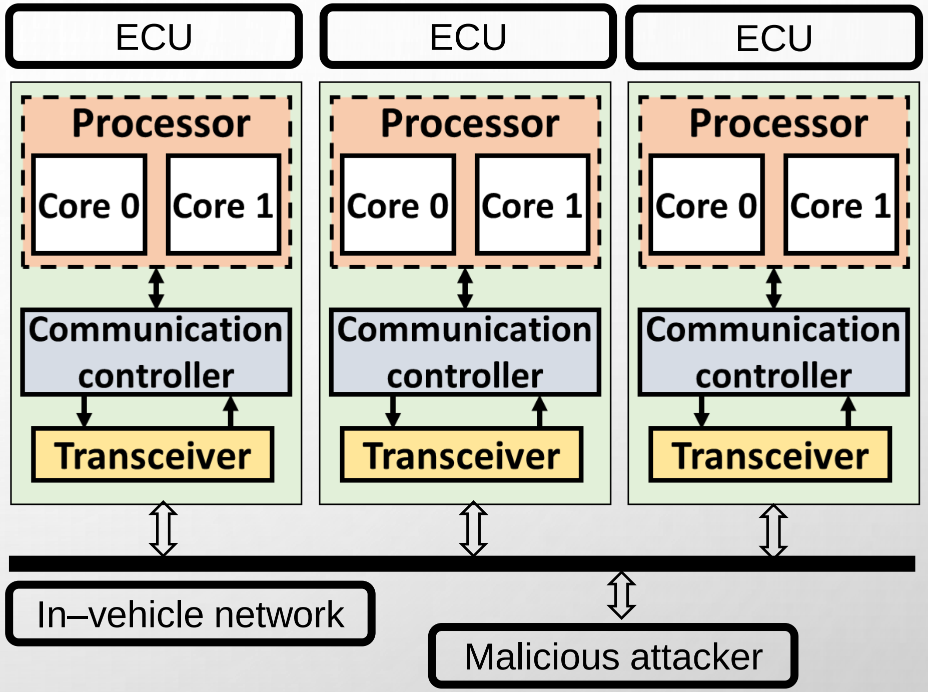
- **Proposed *TENET* framework for anomaly detection**
  - Temporal convolutional neural attention (TCNA)
    - A novel architecture to learn very long term dependencies between messages
  - Divergence score metric
  - Decision tree based detector to detect variety of attacks

- **Compared *TENET* framework with a spectrum of architectures**
  - A RNN based replicator neural network (M. Weber et al., 2018)
  - A LSTM based autoencoder model with attention (M. O. Ezeme et al., 2018)
  - A GRU based autoencoder (V. Kukkala et al., 2020)

- **Extensive analysis on memory and latency overhead**

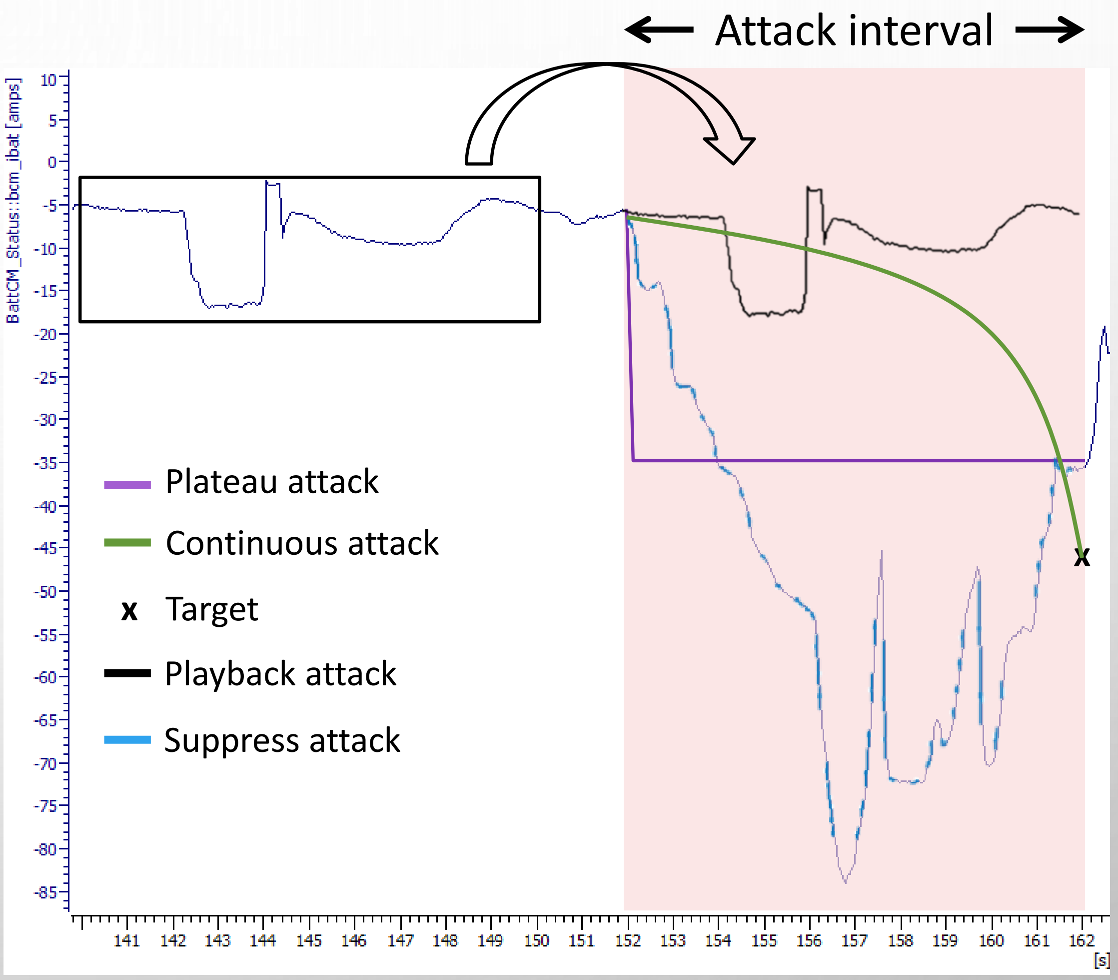
System Model

- **Multiple ECUs are connected using in-vehicle network**
- **Distributed ADS approach**
  - Real-time and anomaly detection applications are co-located
- **Assume attacker can gain access to the in-vehicle network using the most common attack vectors**
  - Example: Infotainment system, ADAS system, OBD-II port, etc.
- **Protocol agnostic, can be applied to Flexray, Ethernet or CAN**
- **Controller Area Network (CAN)**



Attack Model

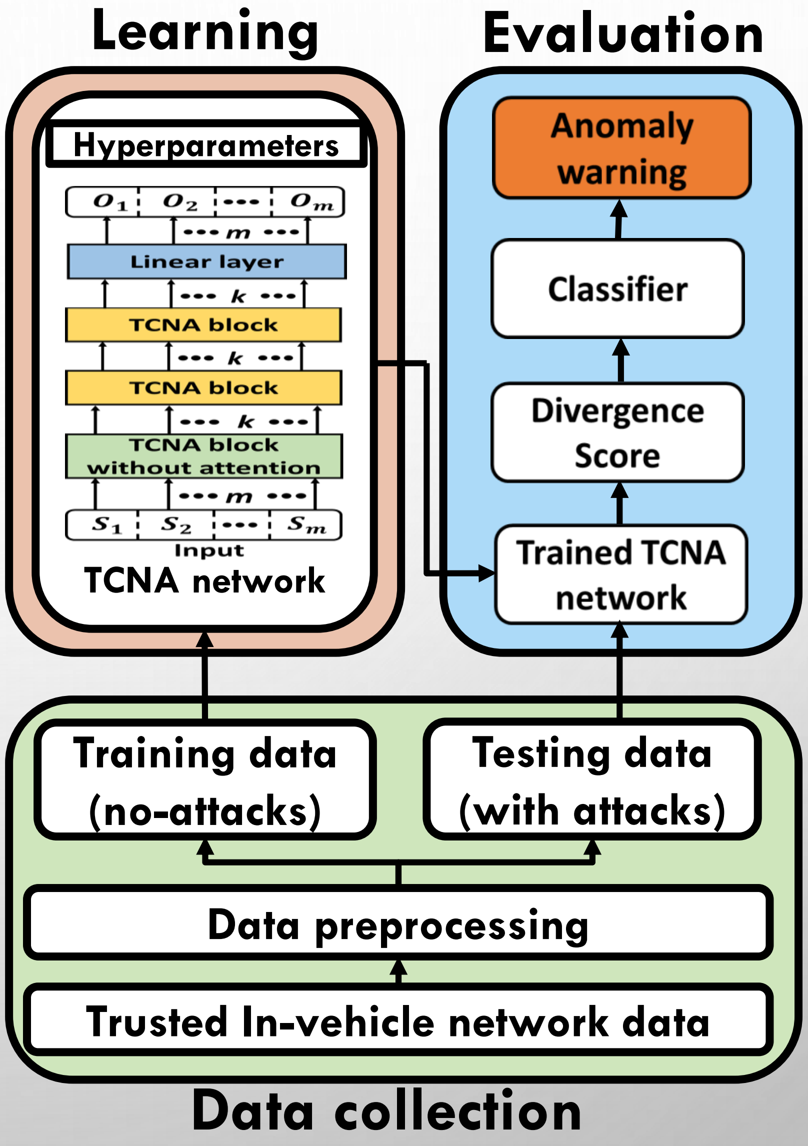
- **Attacks evaluated against**
  - **Plateau attack**: Sets a constant value for a signal.
  - **Continuous attack**: Slowly overwrites the signal value over a period.
  - **Playback attack:** Replays a normal sequence of transmission from the past.
  - **Suppress attack**: No message transmission allowed.



TENET Framework Overview

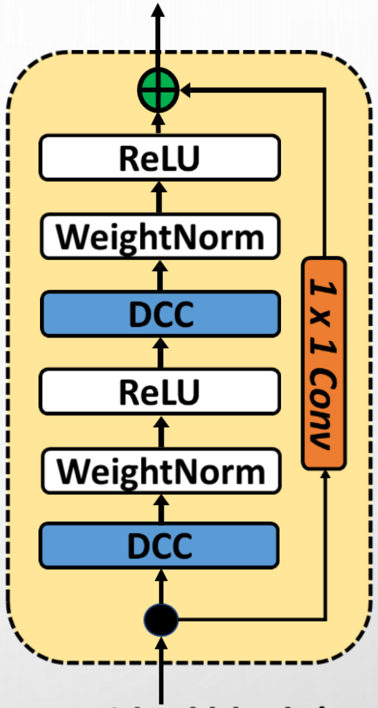
Three phases of *TENET* framework

- Data collection
- Model learning
- Model evaluation

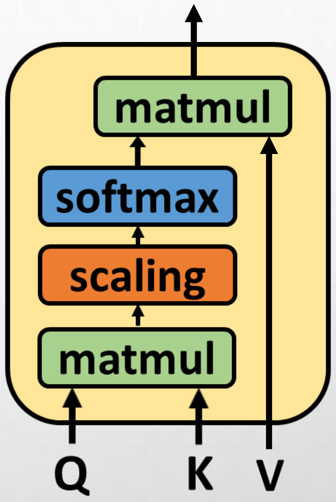


TCNA Network Building Block

- **TCNA block is combination of a temporal residual block (TRB) and self attention mechanism**
- **Temporal Residual Block (TRB)**
  - TRB consists of two dilated causal convolution (DCC) layers, two weight normalization and two ReLU activation layers
  - The skip connection efficiently backpropagate gradients
- **Self Attention mechanism**
  - Helps identify important feature maps from the output of TRB and scale appropriately



TCN Residual block (TRB)

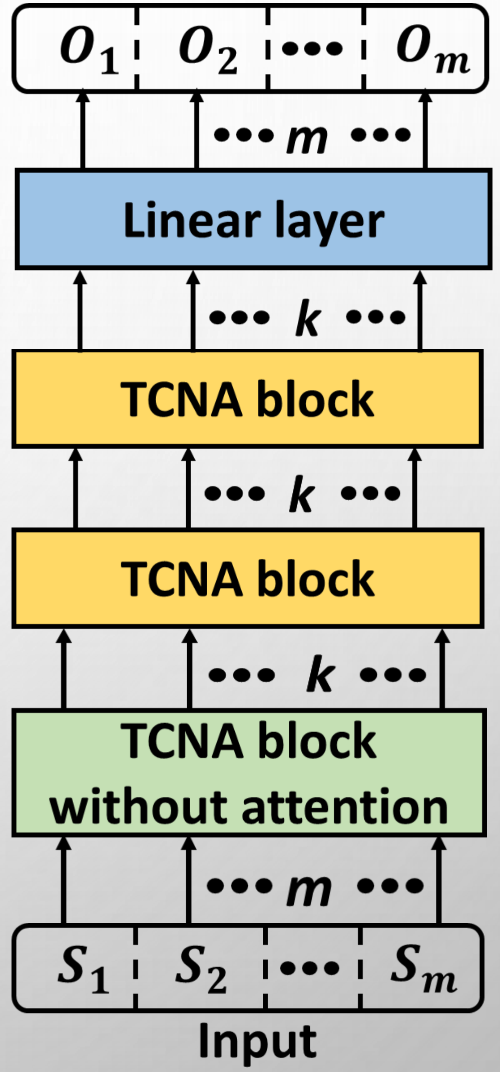


Attention mechanism

Q - Query
K - Key
V - Value

TCNA Network Architecture

- **TCNA Network Architecture**
  - Inputs pass through the first TCNA block without attention mechanism
  - Feature maps generated by the first TCNA block traverses through stacked TCNA block with attention
  - The output from final TCNA block is then passed through a dense layer to output predicted signal values
- **TCNA Training**
  - TCNA training is unsupervised
  - Rolling window approach
  - Mean squared error (MSE) based prediction error is back propagated to update weight parameters

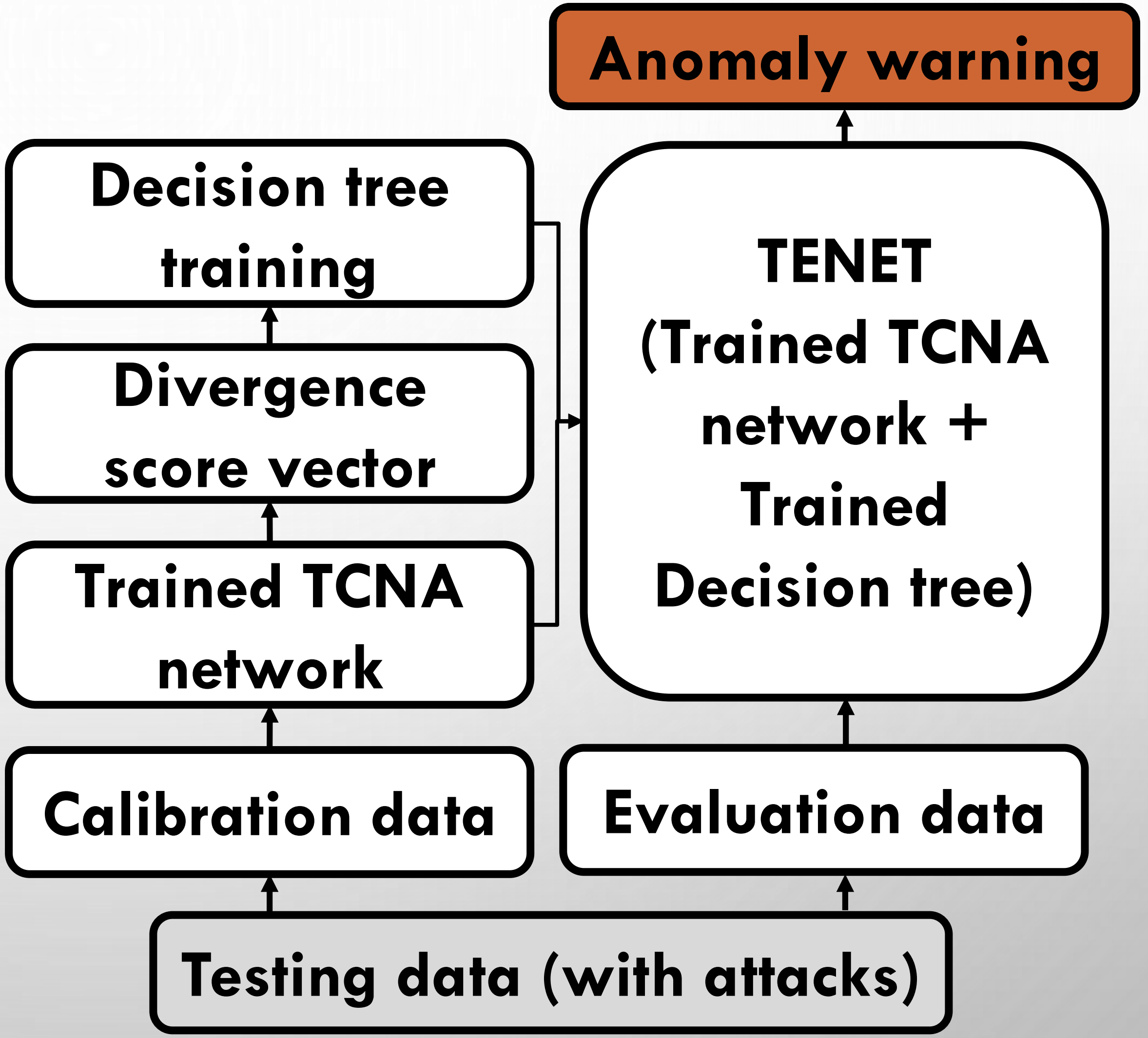


TENET Evaluation Phase

- **Testing data split**
- **Divergence score vector**
  - Computes signal level deviations between predicted and observed signals

$$DS_i^m(t) = \left(\hat{S}_i^m(t) - S_i^m(t+1)\right) \ \forall \ i \ \in [1, N_m], m \ \in [1, M] \quad ..(1)$$

- **Decision tree for classification**
  - Lightweight classifier with high detection accuracy
- **Anomaly warning**

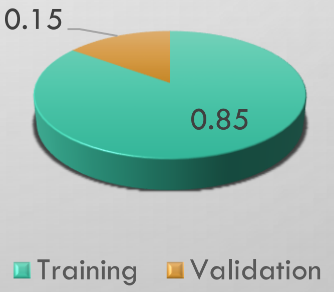


Simulation Setup

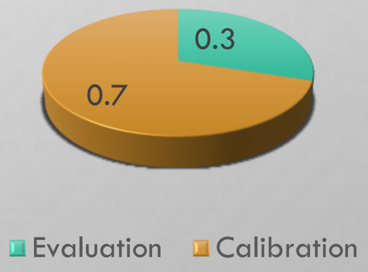
- **Sensitivity analysis on receptive field length**
- **Compared with best-known prior works**
  - RN: [M. Weber et al., 2018]
  - HAbAD: [M. O. Ezeme et al., 2018]
  - INDRA: [V. Kukkala et al., 2020]
- **Memory overhead and latency analysis**
- **Comparison metrics**
  - Detection accuracy, False negative rate (FNR), Receiver operating characteristic curve with area under the curve (ROC-AUC), Mathews Correlation Coefficient (MCC)
- **Dataset**
  - Developed from real world in vehicle network data
  - Hyperparameter list for TENET
  - Train and Test split

Hyperparameters	
Epochs	200
Loss function	MSE
Optimizer	ADAM
Learning rate	1e-4
Batch size	256
Kernel size	2
TRB Layers	3

Training data



Testing data



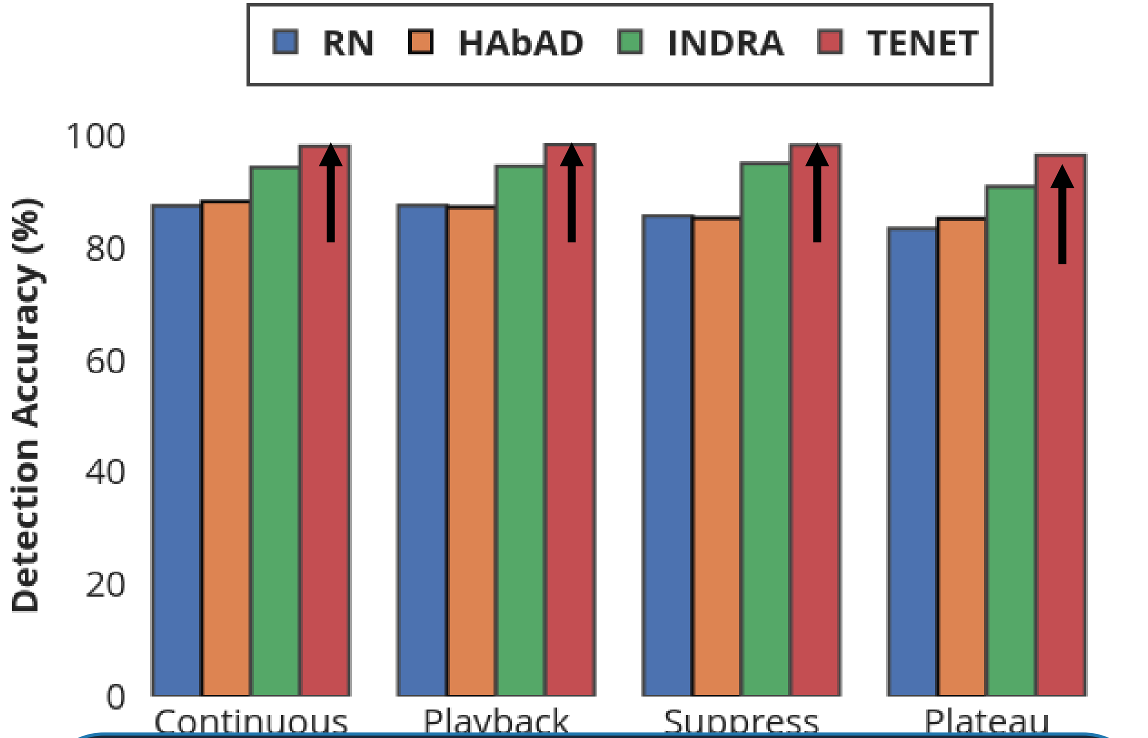
TENET Receptive Field Length Analysis

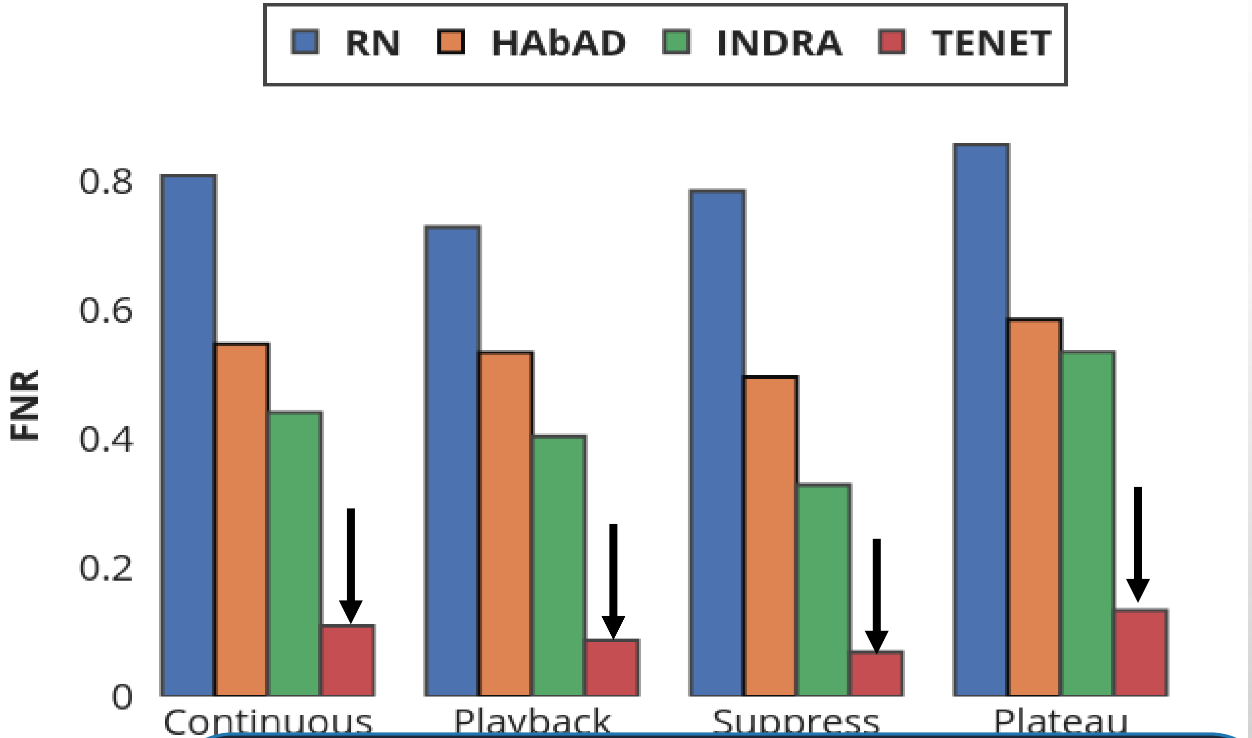
	Receptive field lengths			
	16	**32**	**64**	128
Average training loss	4.1e-4	3e-4	**2.5e-4**	6.8e-4
Average validation loss	5.5e-4	4.3e-4	**2.9e-4**	9.3e-4

- **Receptive filed length analysis**
  - Helps to understand if long receptive lengths can better learn the normal system behavior
  - Receptive field represents size of inputs influencing the output at a particular timestep
  - Relatively poor ... ture map produced from ... esentation of the relationship be...

A receptive length of 64 effectively represents the input time series data

Comparison with Prior Works





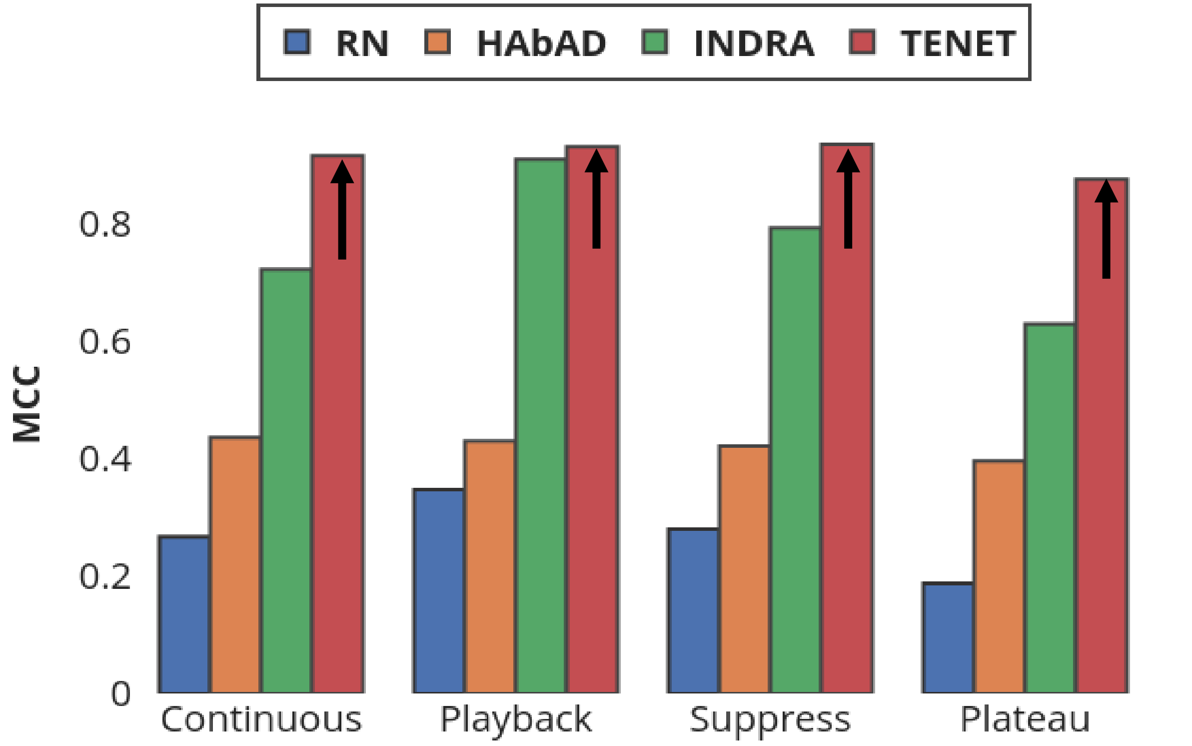
***TENET* achieved an average of 3.32% improvement in detection accuracy**

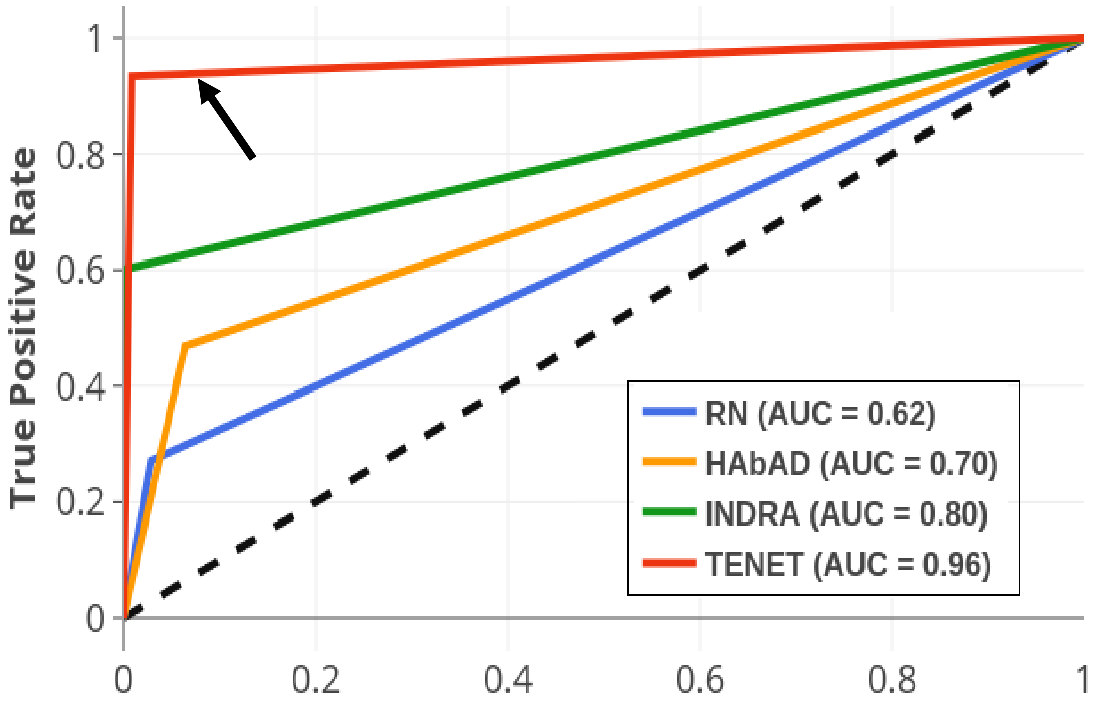
***TENET* achieved an average of 32.70% reduction in FNR metric**

RN

ention-based
et al., 2018]

Comparison with Prior Works

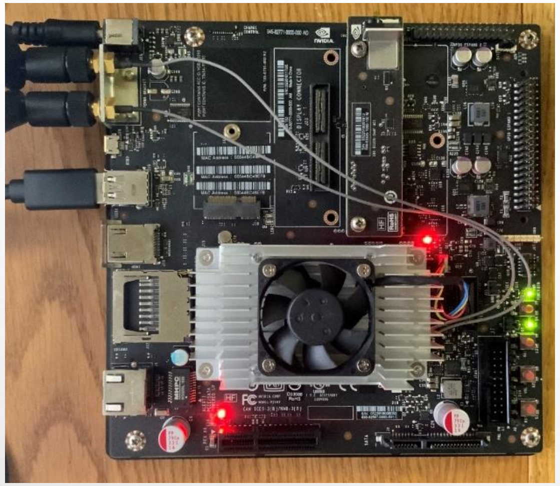




***TENET* achieved an average of 19.14% improvement in MCC metric**

***TENET* best performed with an AUC of 0.96**

Memory and Latency Analysis



ADS Framework	Memory footprint (KB)	Model parameters	Inference time (μs)
TENET	59.62	6064	**250.24**
RN [17]	**7.2**	**1300**	412.50
INDRA [23]	453.8	112900	482.10
HAbAD [24]	261.63	64484	1370.10

- **Model footprint, model parameters and latency**
  - Tested on Nvidia Jetson TX2 with dual-core ARM cortex-A57 CPUs
  - Compared to RN, *TENET* has
    - 69.47% lower F
    - 64.3% higher M
    - 37.25% higher
    - 9.48% higher c

TENET **has relatively minimal inference time and memory overhead**

Conclusion

- **Proposed TCNA network**
  - Novel TCNA network to learn normal system behavior during learning phase
  - Divergence score metric to quantify the deviation from expected behavior
  - Decision tree based classifier to detect attacks at runtime
- **Presented receptive field length analysis**
- ***TENET* performance analysis**
  - Compared against various recurrent architectures with and without attention
- **Performed memory and latency analysis**
- ***TENET* outperforms all compared works in all attack scenarios and metrics while having relatively low memory and detection latency**

Thank you

Questions?